[redacted]

#### *1.2.2.8 Public Disclosure*

[redacted]

#### *1.2.2.9 Incident Reporting*

[redacted]

### 1.2.3 Consequences of Rules Violations

[redacted]

# INFORMATION SECURITY POLICY (ISP)

# 2 Section II: Identify

This section provides Information Security policy for managing cybersecurity risk to systems, assets, data, and capabilities. It includes the following categories:

- Asset Management (ID.AM);
- Business Environment (ID.BE);
- Governance (ID.GV);
- Risk Assessment (ID.RA); andRisk Management (ID.RM);

## 2.1 Asset Management

[redacted]

### 2.1.1 Platform Boundary

[redacted]

### 2.1.2 Authorized Hardware and Software

[redacted]

[redacted]

#### *2.1.2.1 Remediation*

[redacted]

### 2.1.3 Information System Boundary

[redacted]

[redacted]

### 2.1.4 IT Systems and Inventory

[redacted]

### 2.1.5 Information System Interconnections and Information Flow

[redacted]

[redacted]

### 2.1.6 Security Categorization and Prioritization

[redacted]

[redacted]

### 2.1.7 CyberSecurity Roles and Responsibilities

[redacted]

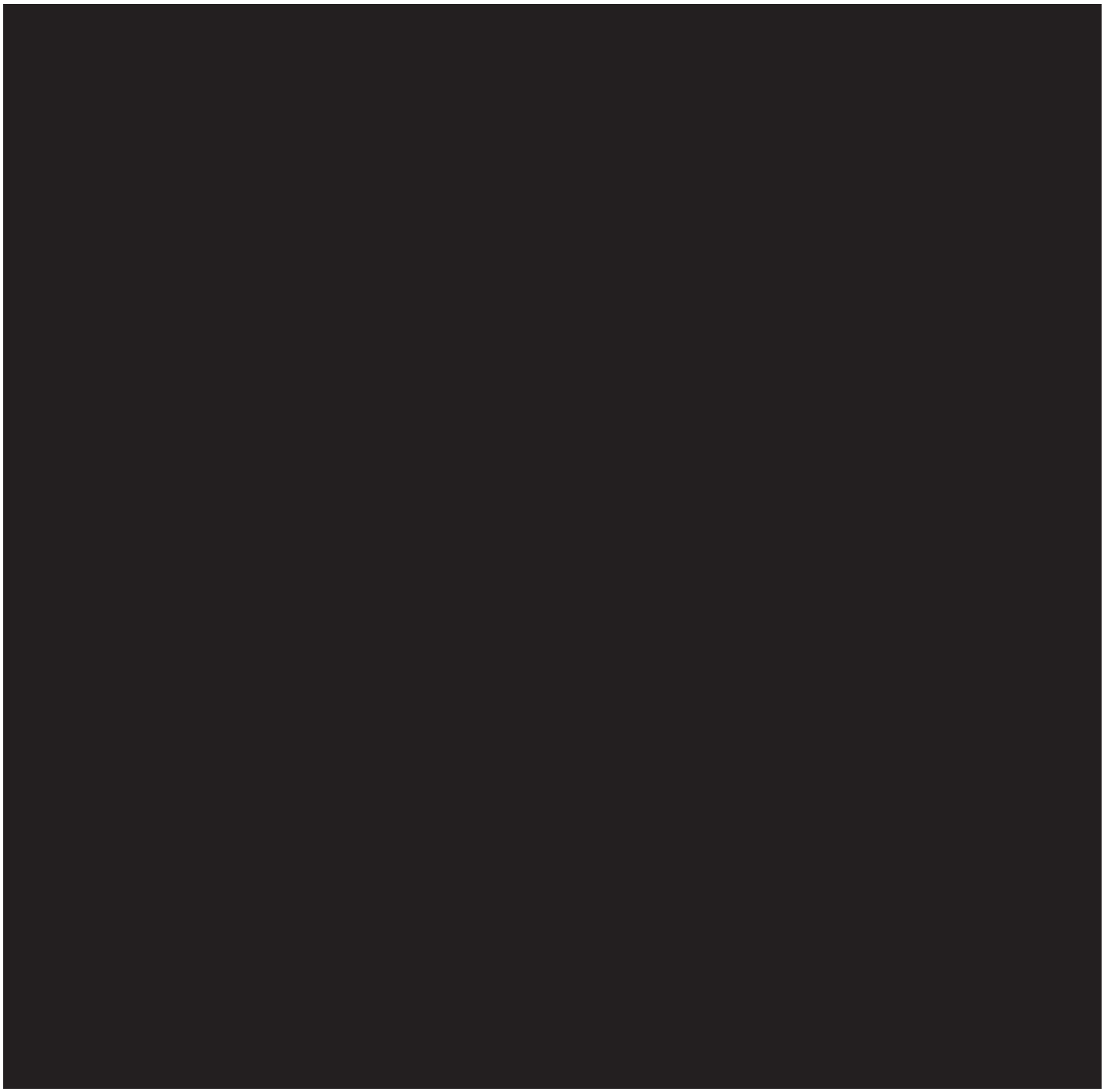
[redacted]

## 2.2 Business Environment

[redacted]

### 2.2.1 Contingency Planning

#### *2.2.1.1 Information System Contingency Planning*



#### *2.2.1.2 Contingency Planning Policy*

[redacted]

## 2.3 Governance

### 2.3.1 Information Security Policy

[redacted]

### 2.3.2 Security Organization Structure

[redacted]

### 2.3.3 Laws and Regulations

SSA is subject to statutory requirements to protect the sensitive information it collects and maintains on individuals. SSA establishes administrative controls to prevent fraud, waste, and abuse. These statutory requirements are contained in the following documents:

[redacted]

[redacted]

## 2.4 Risk Assessment

### 2.4.1 Security Assessment and Authorization (SA&A)

[redacted]

#### *2.4.1.1 The SSA Risk Management Framework (RMF) Process*

[redacted]

[redacted]

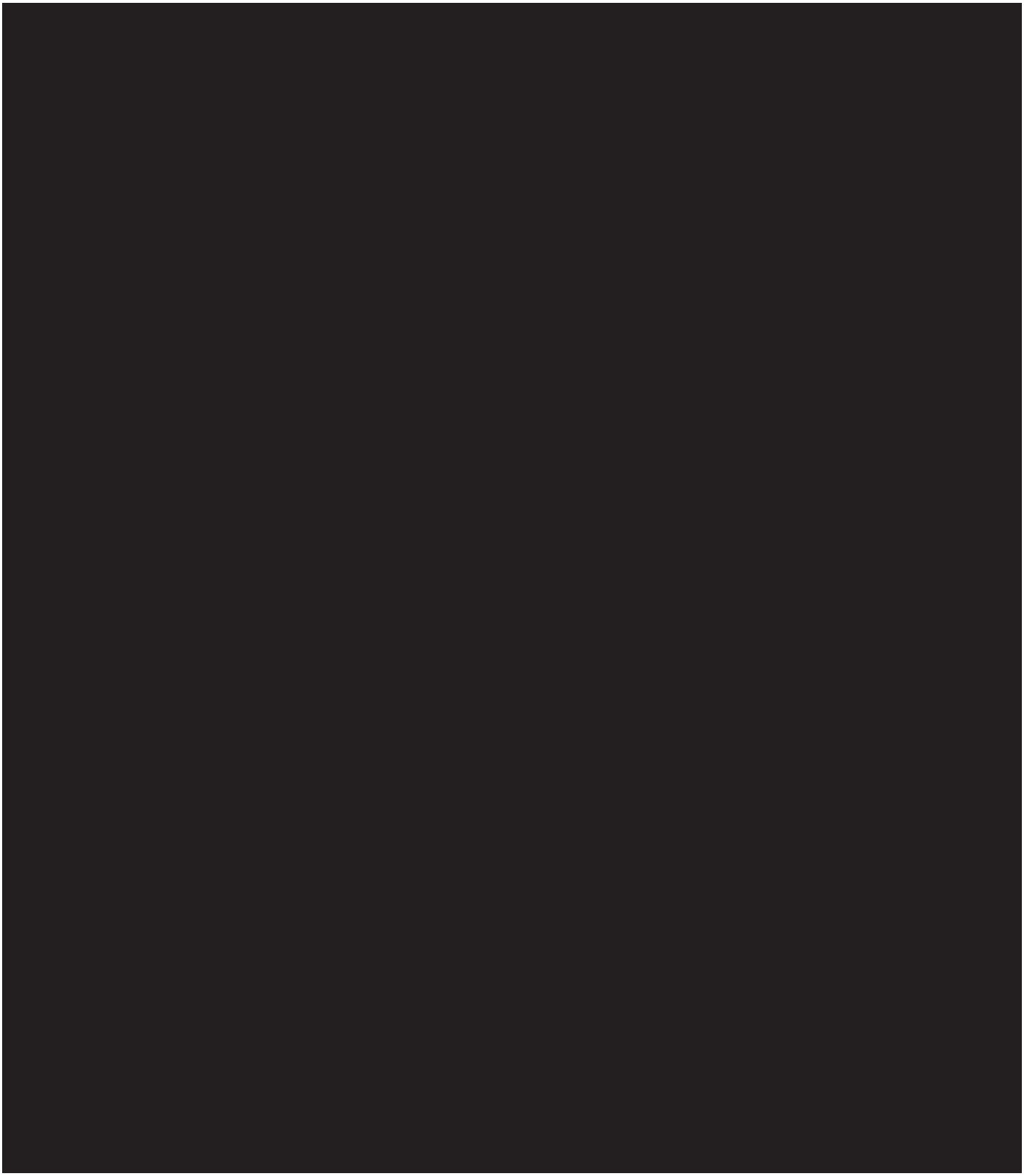
#### *2.4.1.2 System Security Documentation*

[redacted]

### 2.4.2 Threat and Vulnerability Management

[redacted]

### 2.4.3 Information System Risk Assessment



[redacted]

### 2.4.4 Additional Information

[redacted]

[redacted]

## 2.5 Risk Management Strategy

This section provides policy to ensure that the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

### 2.5.1 Risk Management

[redacted]

[redacted]

## 2.6 Cybersecurity Supply Chain Risk Management

[redacted]

# 3 Section III: Protect

This section provides the policy for developing and implementing safeguards to ensure delivery of SSA services. It includes the following categories:

- Access Control; (PR.AC)
- Awareness and Training Data (PR.AT) ;
- Data Security (PR.DS);
- Information Protection Processes and Procedures (PR.IP);
- Maintenance (PR.MA); and
- Protective Technology (PR.PT)

## 3.1 Access Control

### 3.1.1 Identity and Credential Management

[redacted]

#### *3.1.1.1 Identity Management*

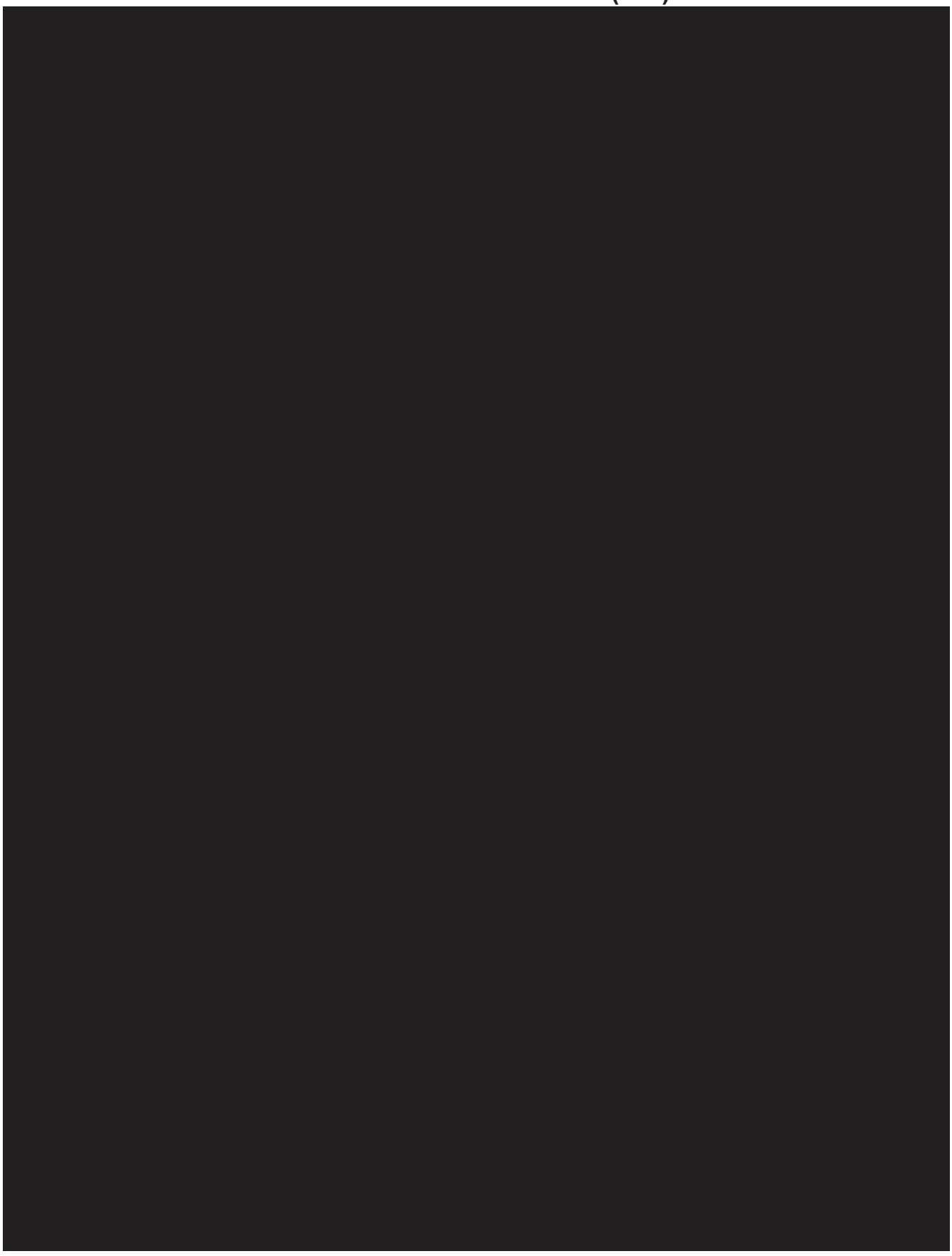
[redacted]

#### *3.1.1.2 Credential Management*

[redacted]

**Section 3 Access Control Administration**
**Section 3.6 - Application For Access To SSA Systems.**

# INFORMATION SECURITY POLICY (ISP)



[redacted]

#### *3.1.1.3 Password Policy*

[redacted]

[redacted]

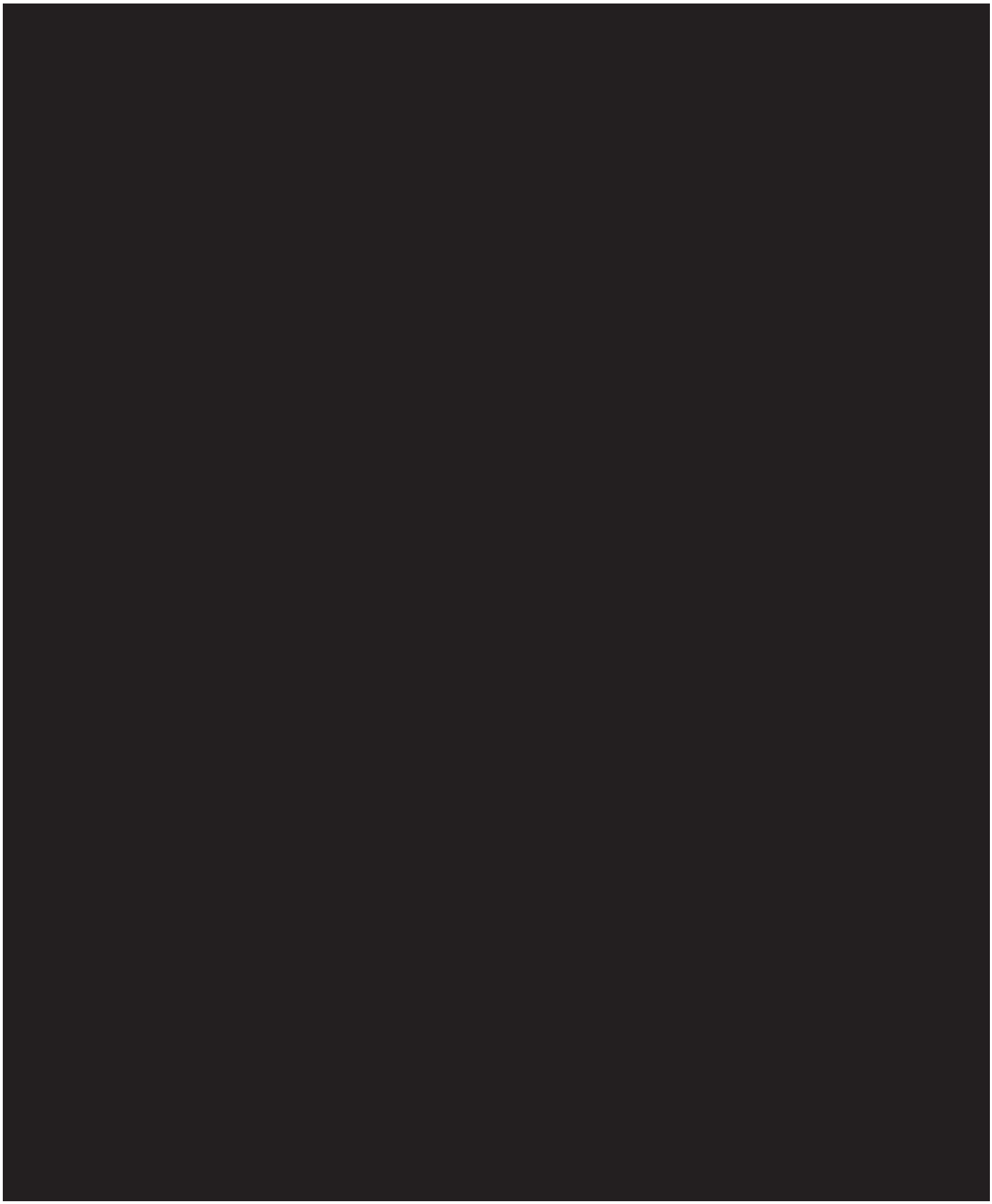
### 3.1.2 Remote Access

[redacted]

### 3.1.3 Account Policy

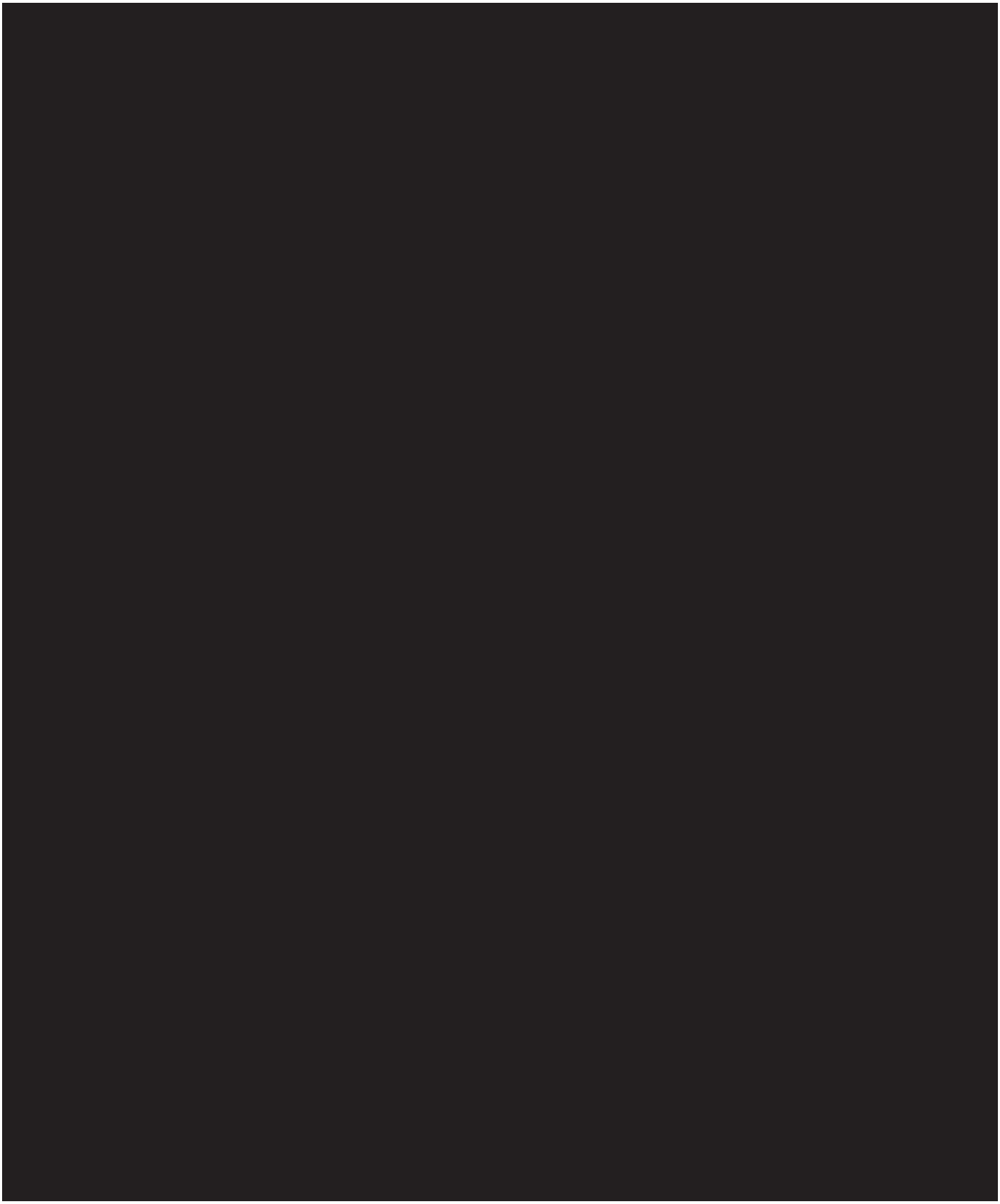
[redacted]

# INFORMATION SECURITY POLICY (ISP)



#### *3.1.3.1 Access Management*

# INFORMATION SECURITY POLICY (ISP)



[redacted]

#### *3.1.3.2 Systems Access Security Administration*

[redacted]

[redacted]

#### *3.1.3.3 Sanctions for Unauthorized Systems Access*

[redacted]

### 3.1.4 Network Integrity and Protection

#### *3.1.4.1 Network Segmentation*

[redacted]

#### *3.1.4.2 Split Tunneling*

[redacted]

#### *3.1.4.3 Multi-Homing*

[redacted]

#### *3.1.4.4 Modems in SSA Facilities*

[redacted]

#### *3.1.4.5 Broadband Internet Connections*

[redacted]

#### *3.1.4.6 Restricted Hardware and Software*

[redacted]

#### *3.1.4.7 Prohibited Security Practices / Activities*

[redacted]

### 3.1.5 Limited Personal Use of Government Office Equipment, Including IT

[redacted]

### 3.1.6 Wireless Technology

[redacted]

#### *3.1.6.1 Mobile Computing Devices*

[redacted]

#### *3.1.6.2 Personally Owned Mobile Computing Devices*

[redacted]

#### *3.1.6.3 Bluetooth Devices*

[redacted]

#### *3.1.6.4 Prohibited Wireless Technology*

[redacted]

[redacted]

#### *3.1.6.5 Wireless Exception*

[redacted]

### 3.1.7 Web Services Security

#### *3.1.7.1 Background*

[redacted]

#### *3.1.7.2 External Clients (Accessing SSA Web Services from outside of SSANet)*

[redacted]

### 3.1.8 Cloud Security

[redacted]

#### *3.1.8.1 Policy*

[redacted]

#### *3.1.8.2 Agency Security Requirements*

[redacted]

#### *3.1.8.3 Chief Information Officer Approval*

[redacted]

### 3.1.9 Mobile Device Security

#### *3.1.9.1 Background*

[redacted]

[redacted]

#### *3.1.9.2 International Travel*

[redacted]

## 3.2 Awareness and Training

The following subsections provide policy and guidance related to the agency's annual information security training requirements

### 3.2.1 Information Security Training and Awareness Policy

[redacted]

### 3.2.2 Role-Based Training for Personnel with Significant Cybersecurity Responsibilities

[redacted]

### 3.2.3 Training Records Retention

[redacted]

### 3.2.4 Agency Reporting of Information Security Training

[redacted]

## 3.3 Data Security

[redacted]

### 3.3.1 Protection of Information in Transit and at Rest

[redacted]

[redacted]

#### *3.3.1.1 Laptop Encryption*

[redacted]

#### *3.3.1.2 Removable Media Encryption*

[redacted]

#### *3.3.1.3 Key Management*

[redacted]

### 3.3.2 Data Protection throughout the Lifecycle

#### *3.3.2.1 Data Custodianship*

[redacted]

[redacted]

#### *3.3.2.2 Information Sharing*

[redacted]

#### *3.3.2.3 External Information Systems*

[redacted]

[redacted]

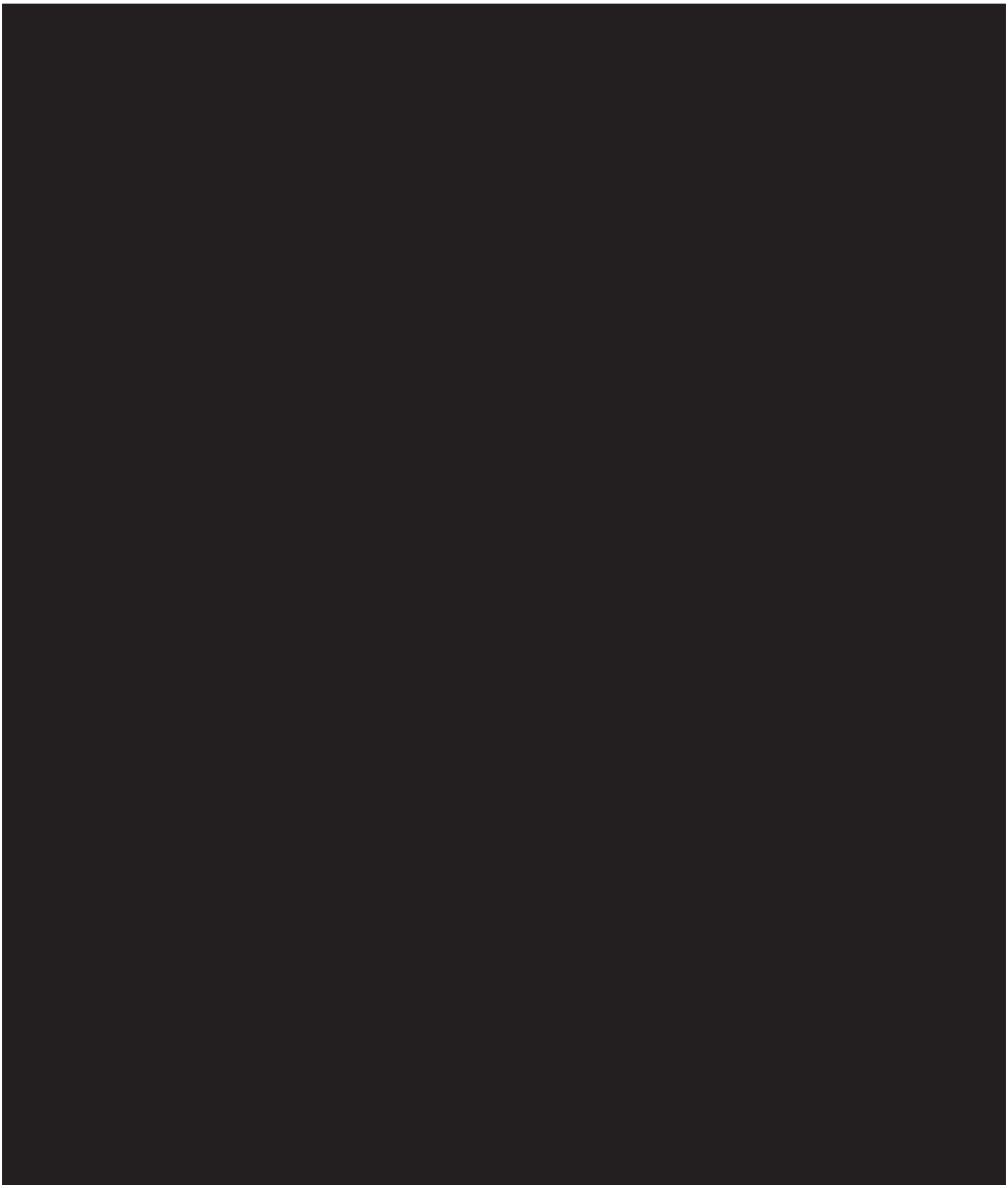
#### 3.3.2.4 Handling and Exchange

[redacted]

#### 3.3.2.5 Data Definitions

[redacted]

# INFORMATION SECURITY POLICY (ISP)



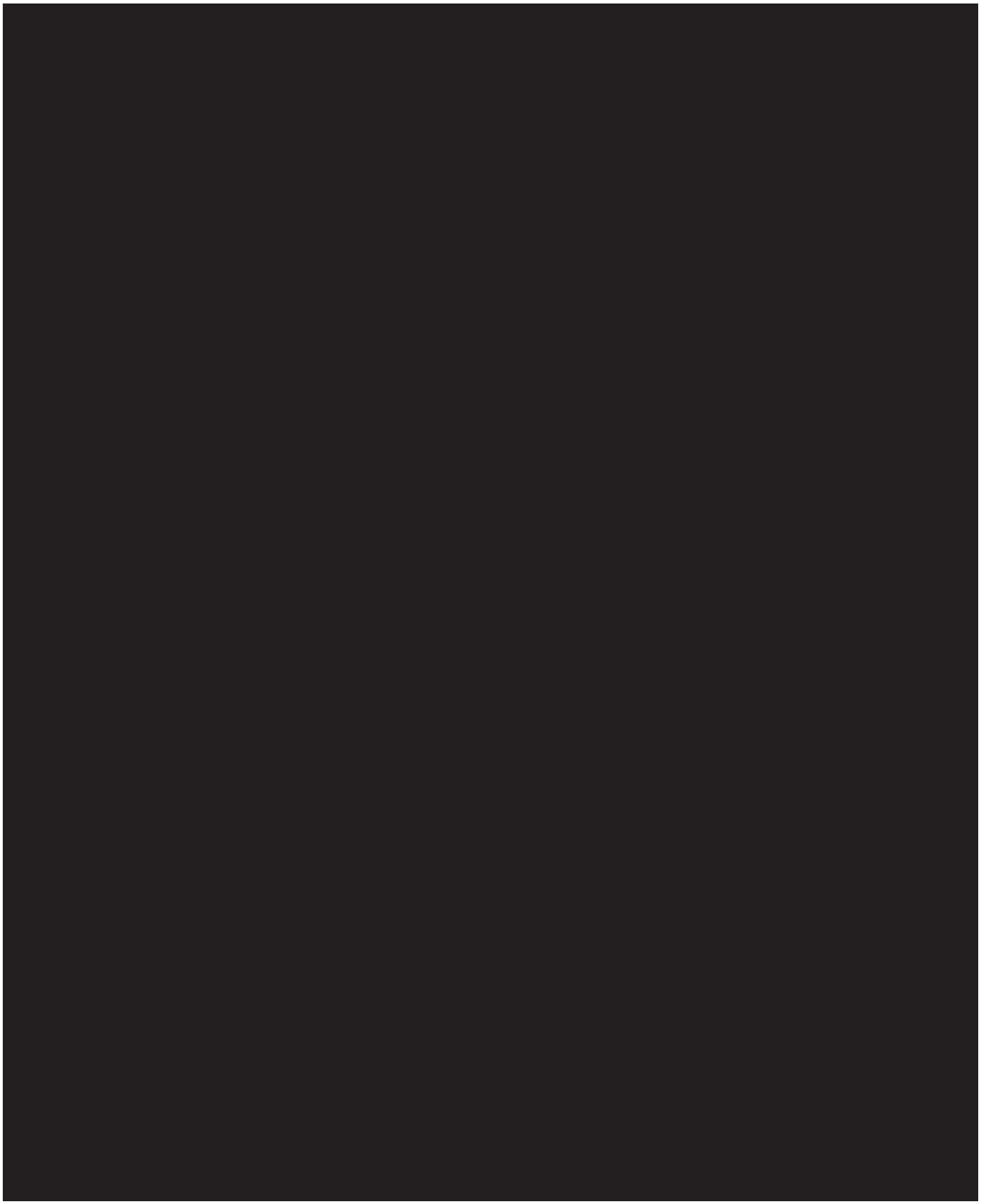
### 3.3.3 Data Integrity

#### *3.3.3.1 Automated Integrity Reviews*

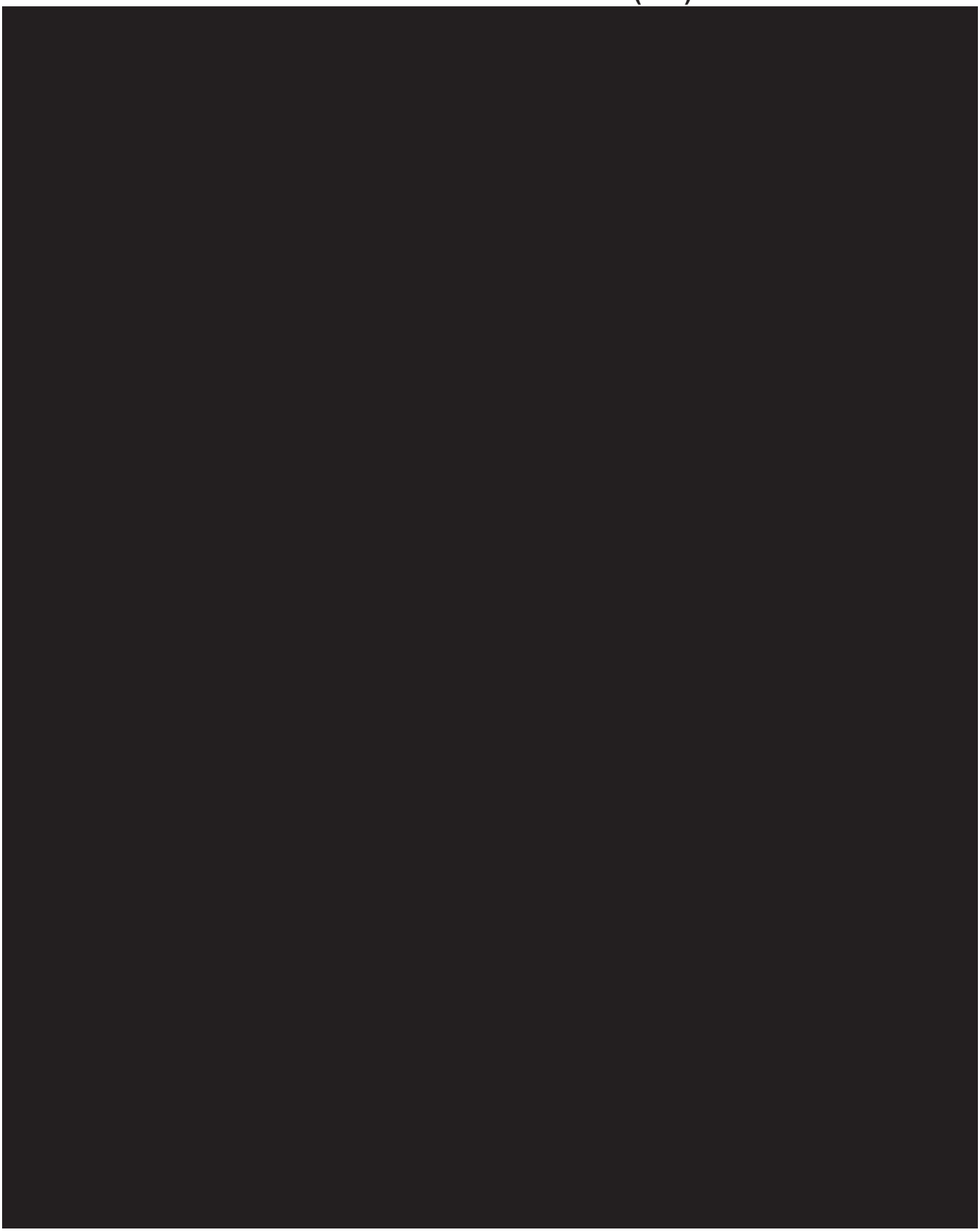
### 3.3.4 IT Equipment Safeguards

### 3.3.5 Secure Email Use Policy

# INFORMATION SECURITY POLICY (ISP)



# INFORMATION SECURITY POLICY (ISP)



[redacted]

### 3.3.6 Secure Fax Use Policy

[redacted]

[redacted]

### 3.3.7 Prohibited Security Practices / Activities

[redacted]

### 3.3.8 IRS Federal Tax Information (FTI)

[redacted]

#### *3.3.8.1 Directive*

[redacted]

#### *3.3.8.2 What is FTI?*

[redacted]

[redacted]

#### *3.3.8.3 Taxpayer First Act (TFA)*

[redacted]

#### *3.3.8.4 Sanctions and Unauthorized Inspection — Important Reminders to All Employees and Contractors to SSA*

[redacted]

### 3.3.10 Records Retention Policy

### 3.3.11 Mandatory Encryption of Electronic Data on Mobile Computers and Devices

### 3.3.12 Other Agency Guidance on Email/Fax Not Listed Above

[redacted]

### 3.3.13 Paper Records Disposal

[redacted]

## 3.4 Information Protection Process Policy

[redacted]

### 3.4.1 Configuration Management

[redacted]

[redacted]

#### *3.4.1.1 Security Configuration Standards*

[redacted]

#### *3.4.1.2 Configuration Management Plan*

#### *3.4.1.3 Exceptions*

### 3.4.2 System Development Lifecycle Security

[redacted]

#### *3.4.2.1 Information Technology (IT) Security Requirements for Agency Acquisitions*

[redacted]

[redacted]

#### 3.4.2.1.1 Contracts Involving IT Systems

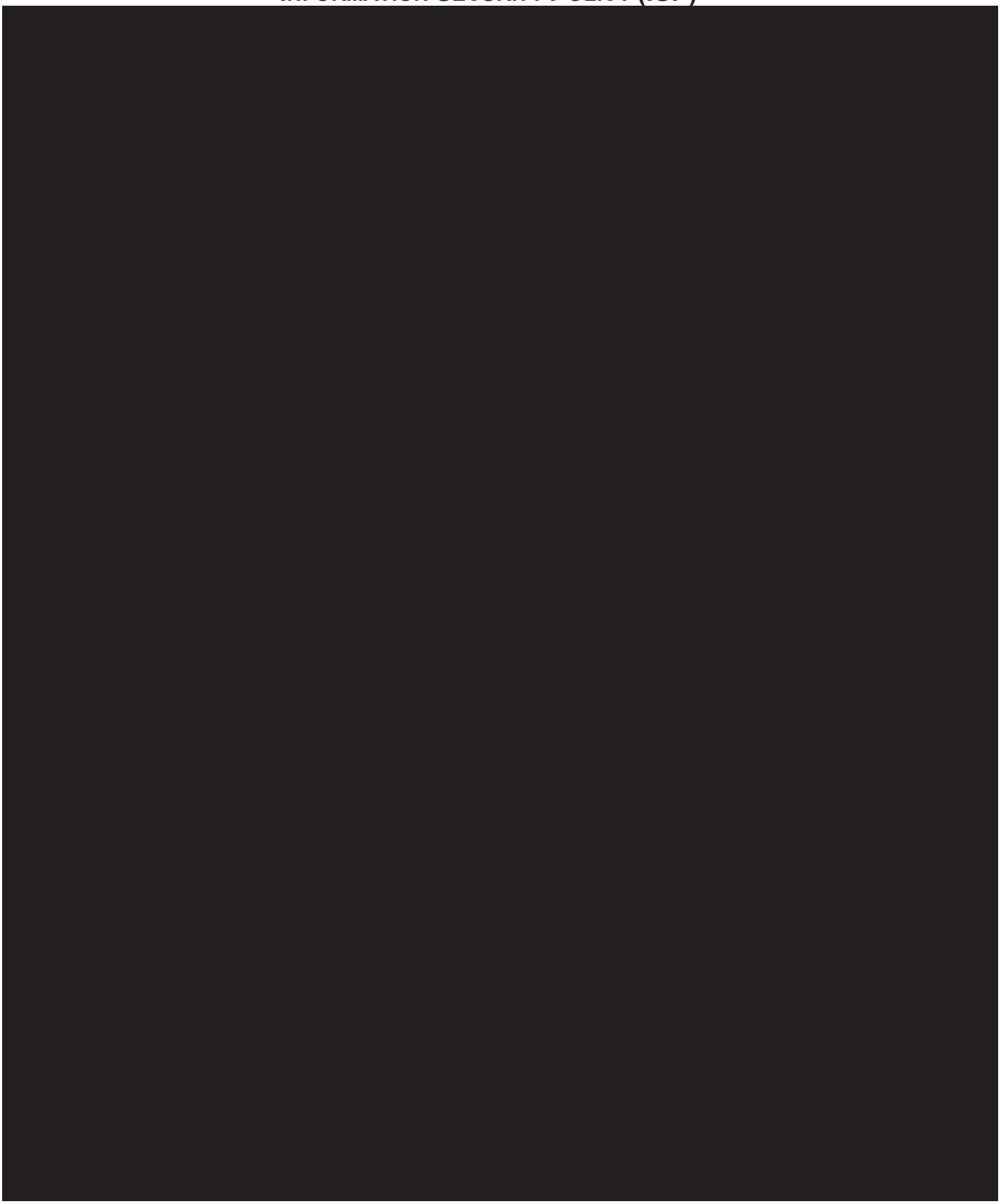
[redacted]

### 3.4.3 Web Application Development Policy

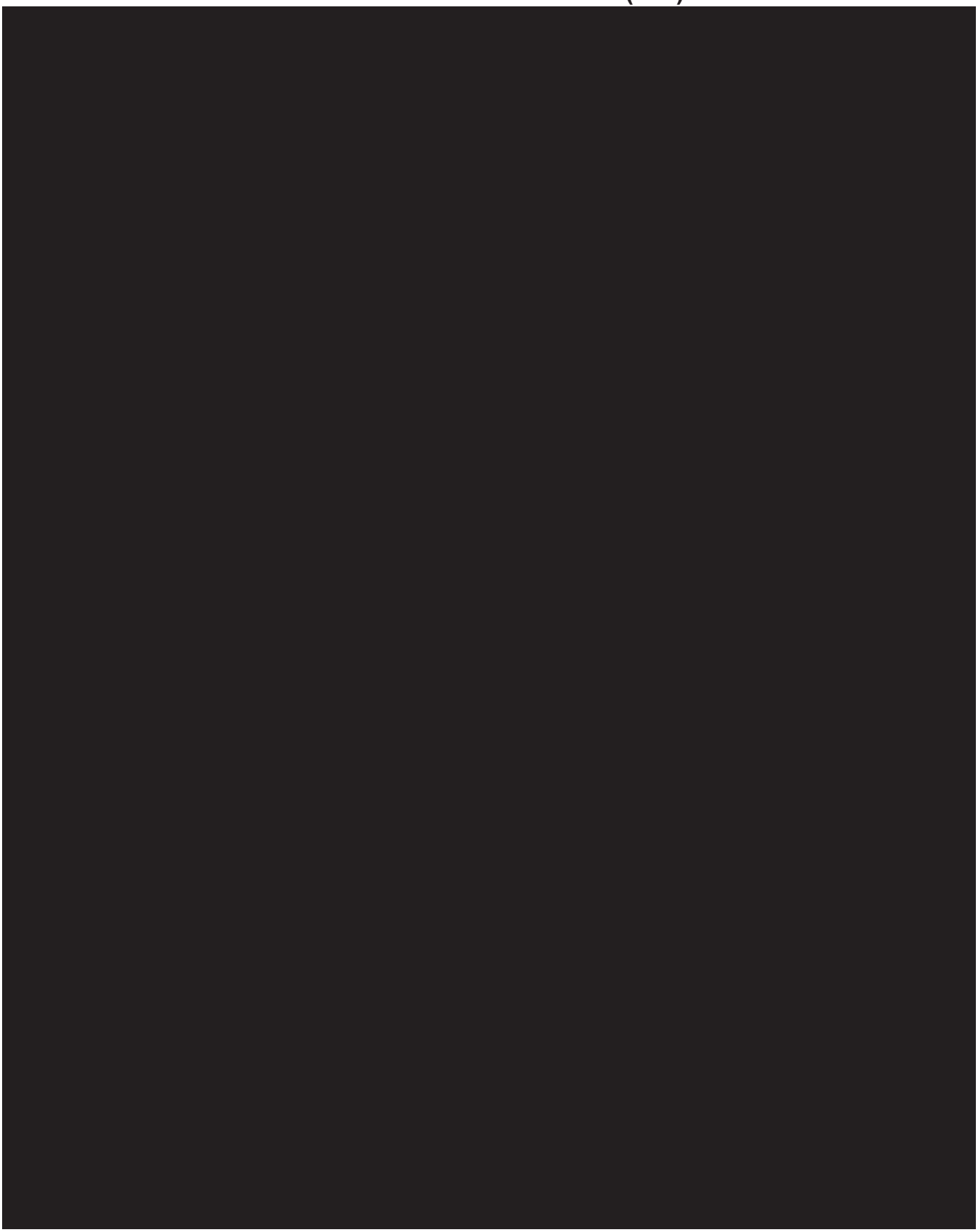
#### *3.4.3.1 Web Application Development Rules*

[redacted]

# INFORMATION SECURITY POLICY (ISP)



# INFORMATION SECURITY POLICY (ISP)



[redacted]

### 3.4.4 Configuration Change Control

[redacted]

### 3.4.5 System Backup

[redacted]

### 3.4.6 Media Sanitization

[redacted]

### 3.4.7 Continuous Monitoring

[redacted]

### 3.4.8 Incident Response

[redacted]

### 3.4.9 Personnel Security

#### *3.4.9.1 Determining Proper Risk Levels*

#### *3.4.9.2 Background Investigations*

#### *3.4.9.3 Personnel Transfer*

#### *3.4.9.4 Sensitive Position Changes*

## 3.5 Maintenance

### 3.5.1 Maintenance Policy

[redacted]

### 3.5.2 Controlled Maintenance

[redacted]

### 3.5.3 Remote Maintenance

[redacted]

[redacted]

### 3.5.4 Maintenance Personnel

[redacted]

## 3.6 Protective Technology

### 3.6.1 System Logging Requirements

[redacted]

[redacted]

#### *3.6.1.1 Logged Events*

[redacted]

#### *3.6.1.2 Log Review*

[redacted]

#### *3.6.1.3 Event Log Access*

[redacted]

#### *3.6.1.4 Log Format and Storage*

[redacted]

[redacted]

### 3.6.2 Individuals of Extraordinary National Prominence (IENP) and Own SSN Requirements

[redacted]

### 3.6.3 Removable Media and Protection from Data Loss Policy

#### *3.6.3.1 Media Protection*

#### *3.6.3.2 Removable Media Devices*

[redacted]

#### *3.6.3.3 Data Loss Protection*

[redacted]

[redacted]

#### *3.6.3.4 Local Manager Responsibilities*

[redacted]

### 3.6.4 Access Enforcement

[redacted]

### 3.6.5 Communication and Control Network Protection

#### *3.6.5.1 Network Boundary Protection*

[redacted]

#### *3.6.5.2 Network Control Devices*

[redacted]

[redacted]

### *3.6.5.3 Peer-to-Peer (P2P) and Web Conferencing / Collaboration Technologies*

[redacted]

[redacted]

#### *3.6.5.4 Instant Messaging*

[redacted]

# 4 Section IV: Detect

This section provides the Information Security policy for developing the organizational understanding to identify the occurrence of a cybersecurity event. It includes the following categories.

- Anomalies and Events (DE.AE);
- Security Continuous Monitoring (DE.CM); and
- Detection Processes (DE.DP)

## 4.1 Anomalies and Events

[redacted]

### 4.1.1 Network and Security Operations

[redacted]

### 4.1.2 Security Event Analysis and Response

[redacted]

### 4.1.3 Reporting

[redacted]

#### 4.1.3.1 Incidents Relating to Program and Employee Fraud

[redacted]

#### 4.1.3.2 Reporting Loss of Personally Identifiable Information (PII)

[redacted]

#### 4.1.3.3 Reporting Unauthorized Federal Tax Information (FTI) Access or Improper FTI Disclosure

[redacted]

#### 4.1.3.4 Criminal Violations and Fraud Policy

[redacted]

[redacted]

#### 4.1.3.4.1 Violations Reporting Process

[redacted]

#### 4.1.3.4.2 Programmatic Violations

[redacted]

#### 4.1.3.4.3 Employee Fraud

[redacted]

#### 4.1.3.4.4 Request for Assistance by SSA OIG

#### 4.1.3.4.5 Request for Information by Other Law Enforcement Agencies and Investigators

## 4.2 Security Continuous Monitoring

### 4.2.1 Personnel Activity Monitoring

### 4.2.2 Malicious Code Detection

### 4.2.3 Service Provider Monitoring

### 4.2.4 Monitoring for Unauthorized Connections, Devices, and Software

[redacted]

### 4.2.5 Monitoring for Software, Firmware and Information Integrity

[redacted]

### 4.2.6 Vulnerability Scanning

[redacted]

# 5 Section V: Respond

This section oulines the agency's policy for responding to a detected cybersecurity event. It includes the following categories.

- Response Planning (RS.RP);
- Communications (RS.CO);
- Analysis (RS.AN); and
- Mitigation (RS.MI)

## 5.1 Response Planning

## 5.2 Communications

### 5.2.1 Security Event Notification

## 5.3 Analysis

### 5.3.1 Impact Analysis

## 5.4 Mitigation

### 5.4.1 Incident Handling

[redacted]

### 5.4.2 Information Sharing and Reporting

[redacted]

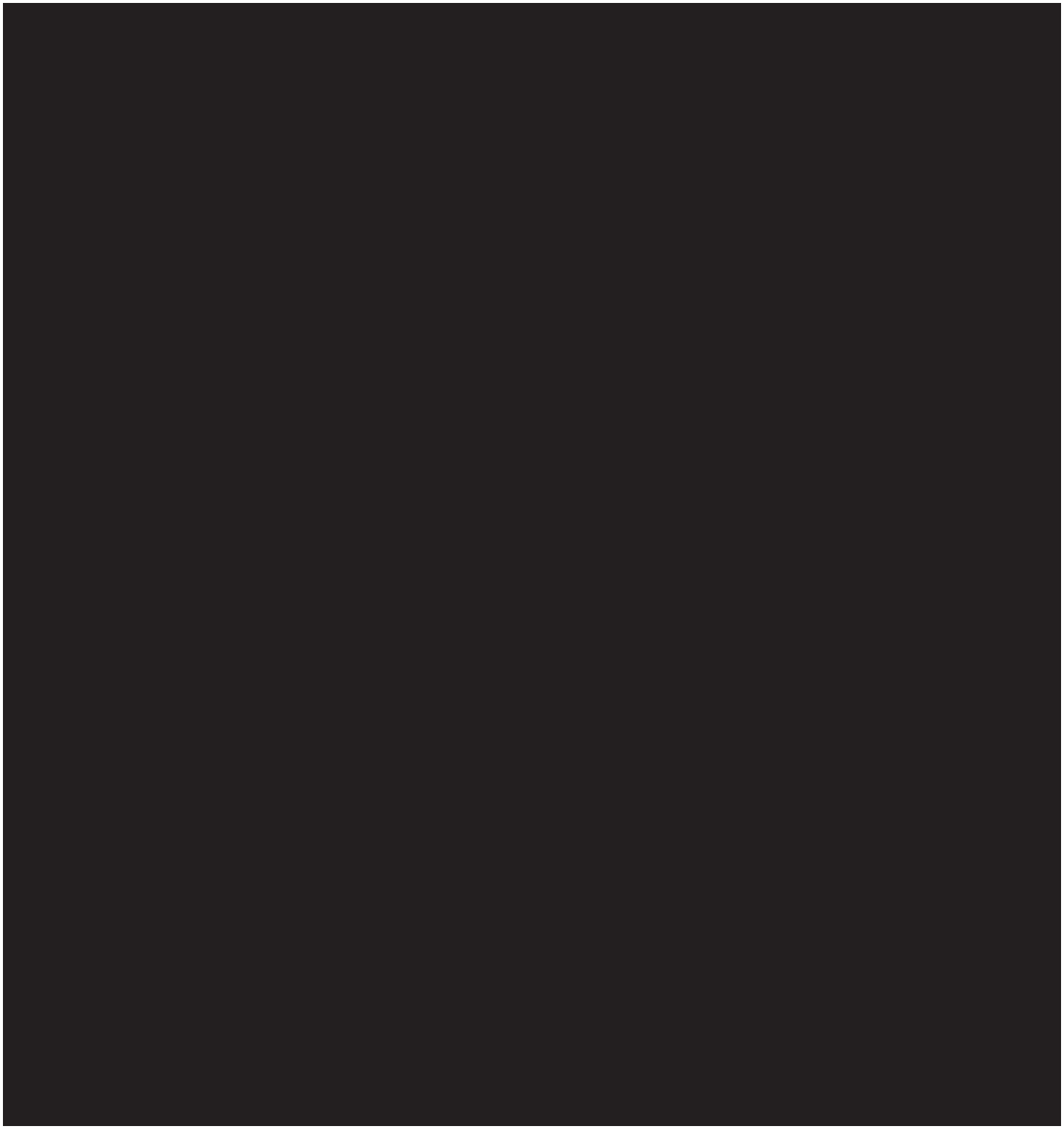
# 6 Section VI: Recover

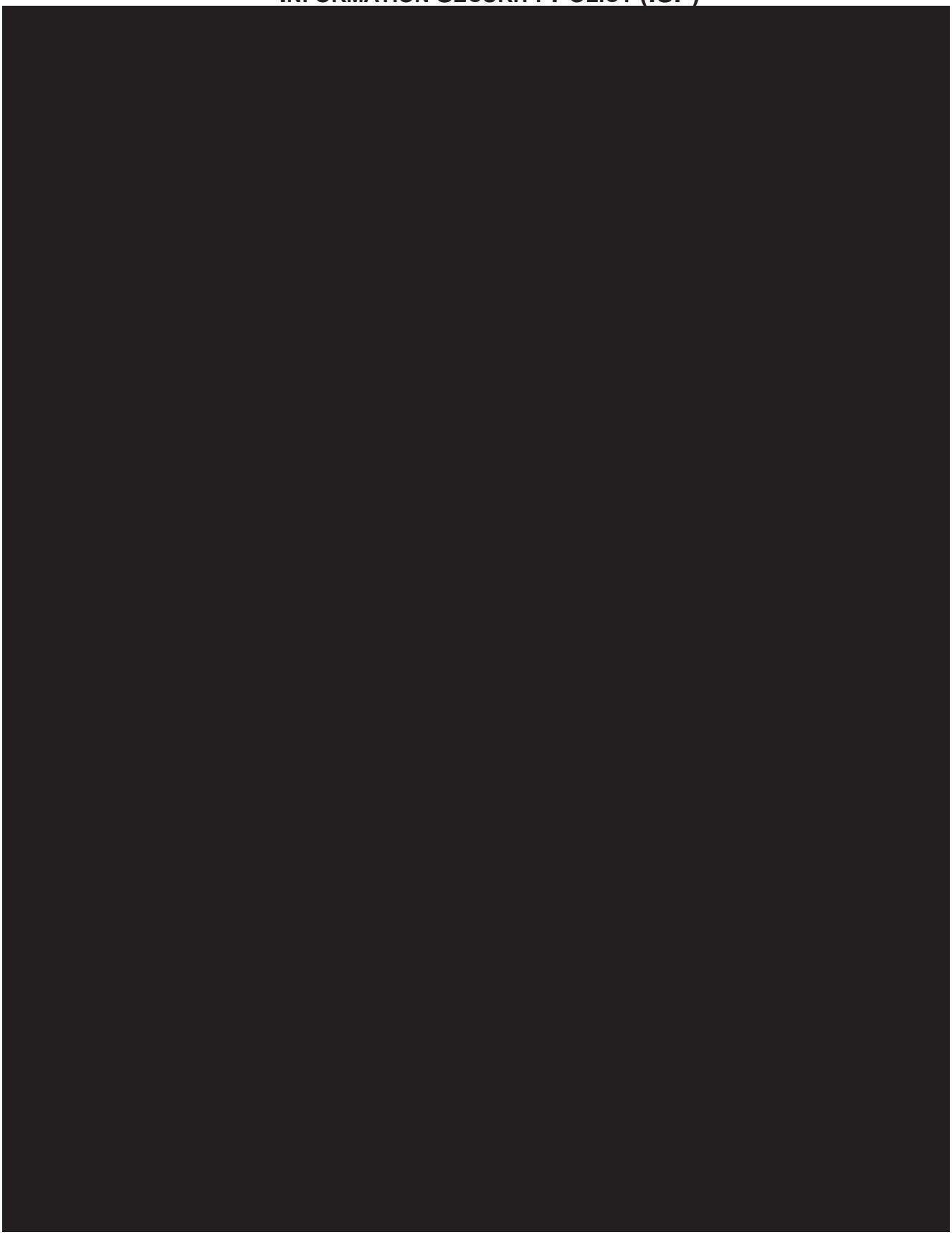
## 6.1 Recovery Planning

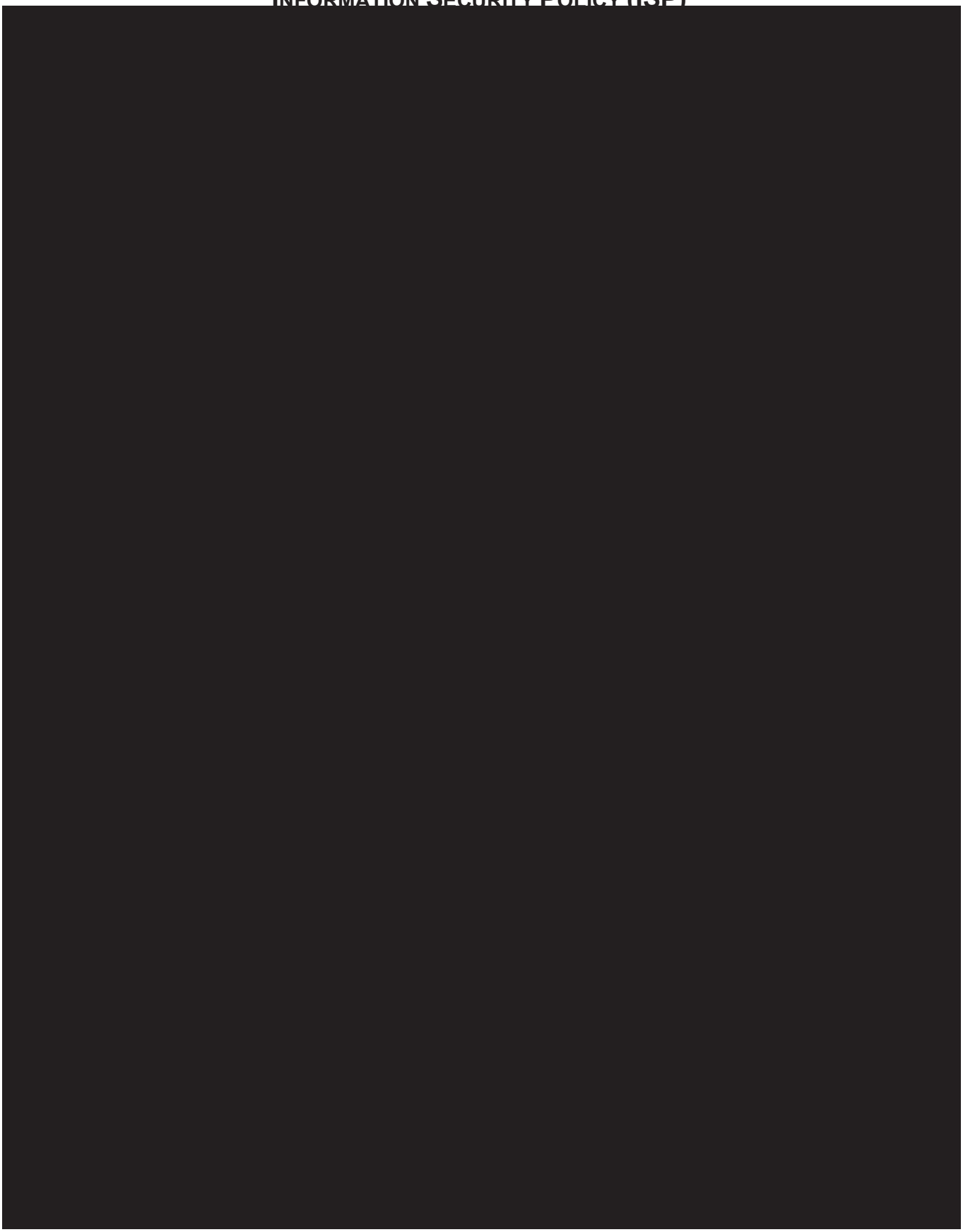
## 6.2 Improvements

# 7 Section VII: Appendices

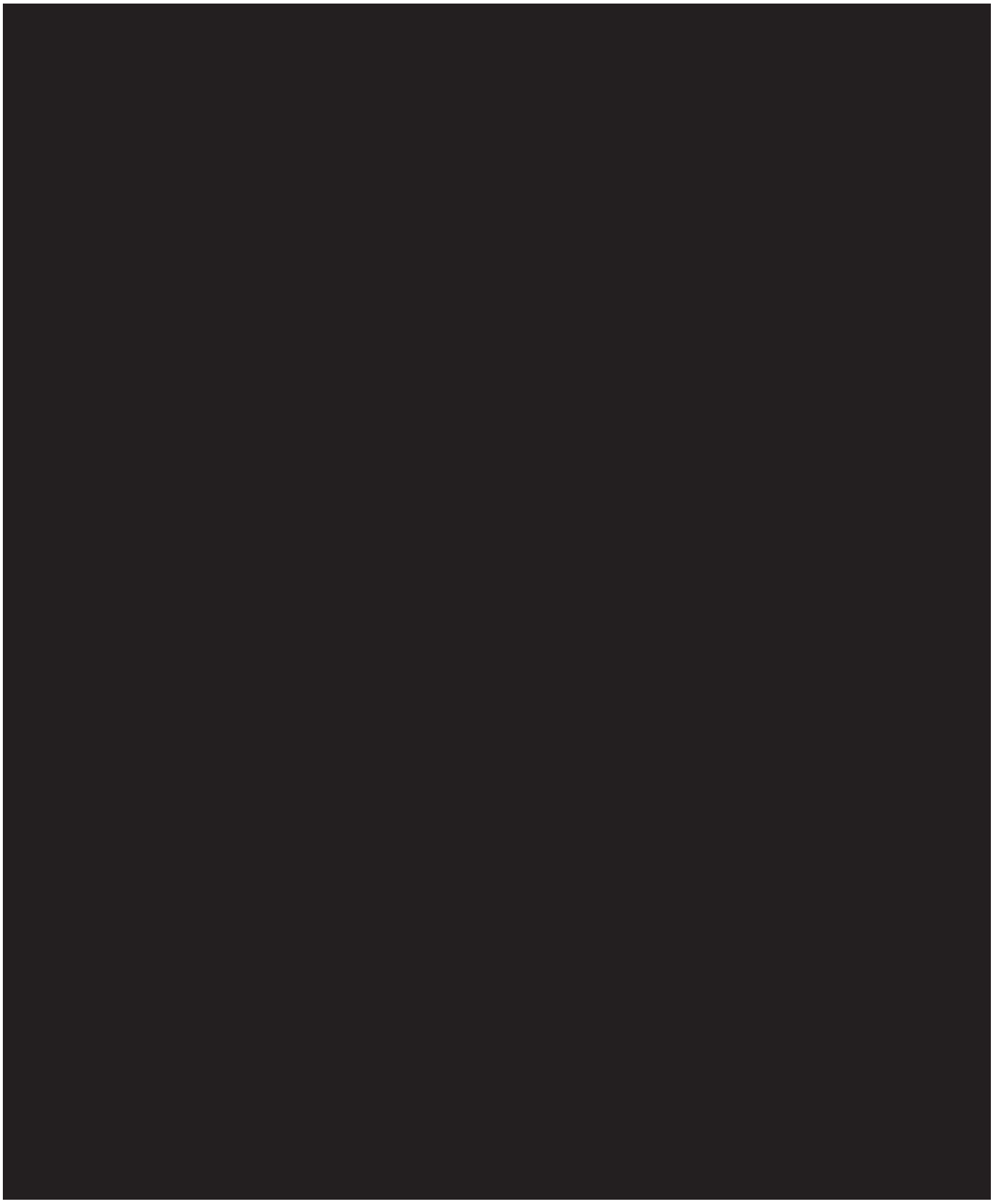
## Appendix B: Roles and Responsibilities



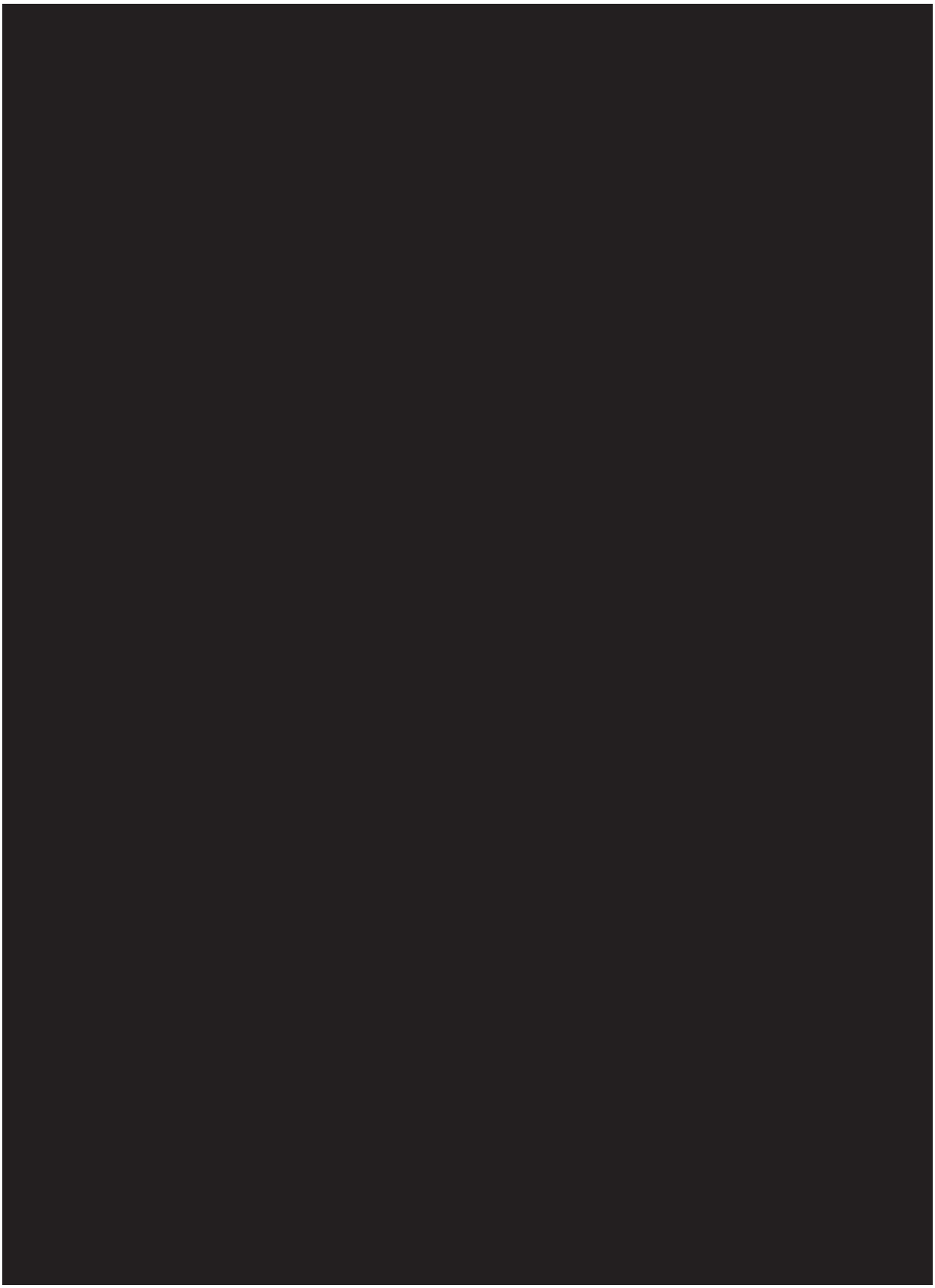




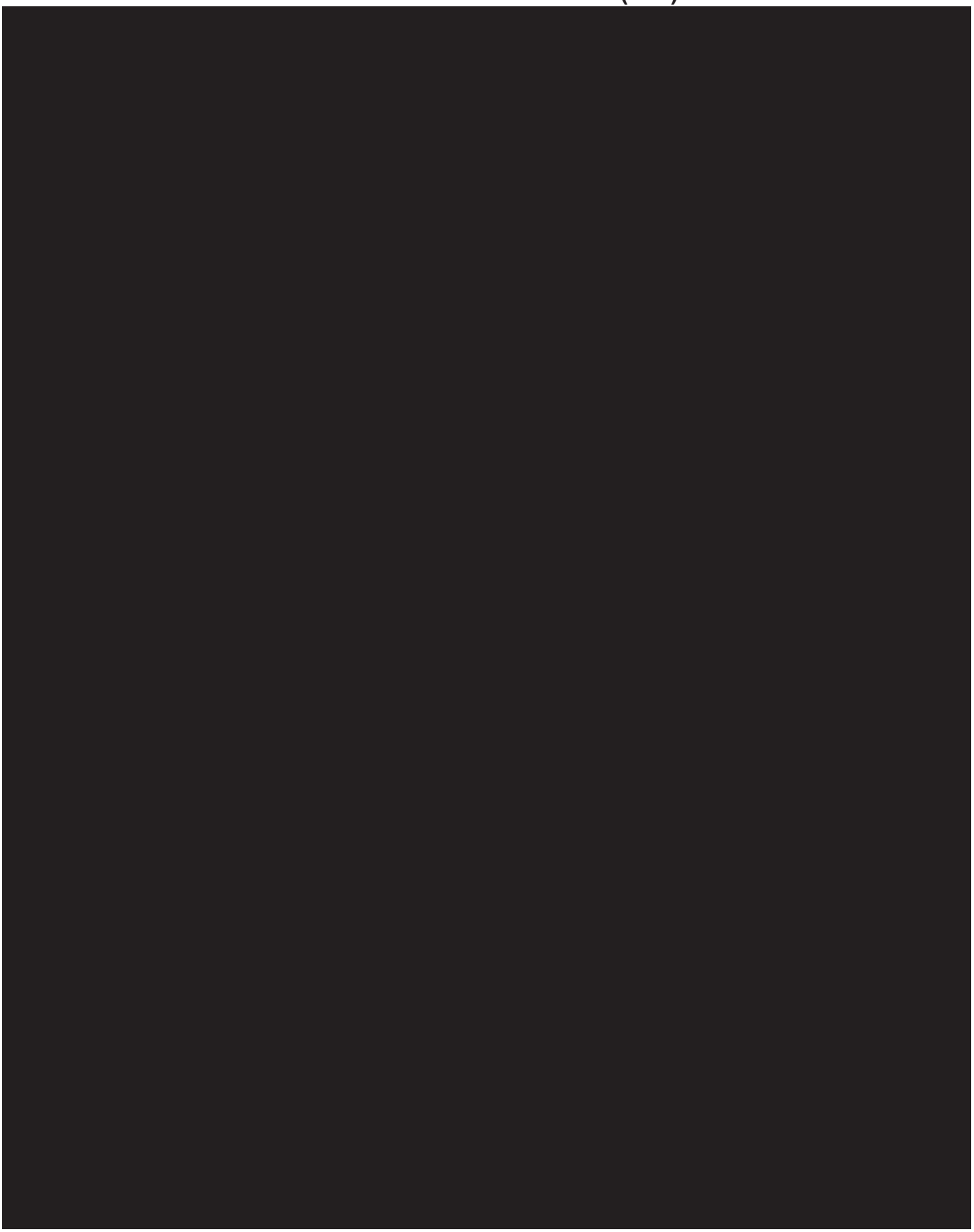
# INFORMATION SECURITY POLICY (ISP)



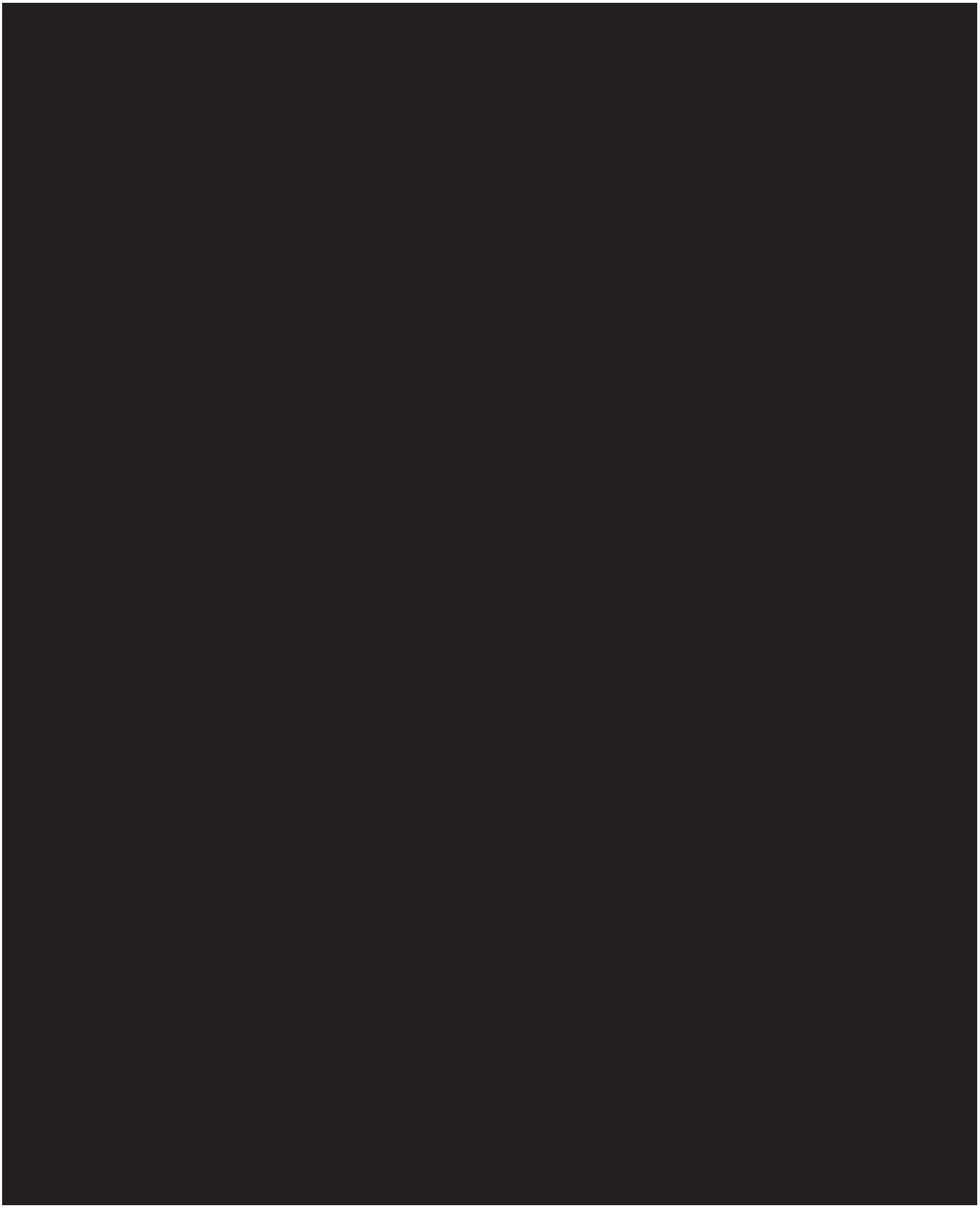
# INFORMATION SECURITY POLICY (ISP)



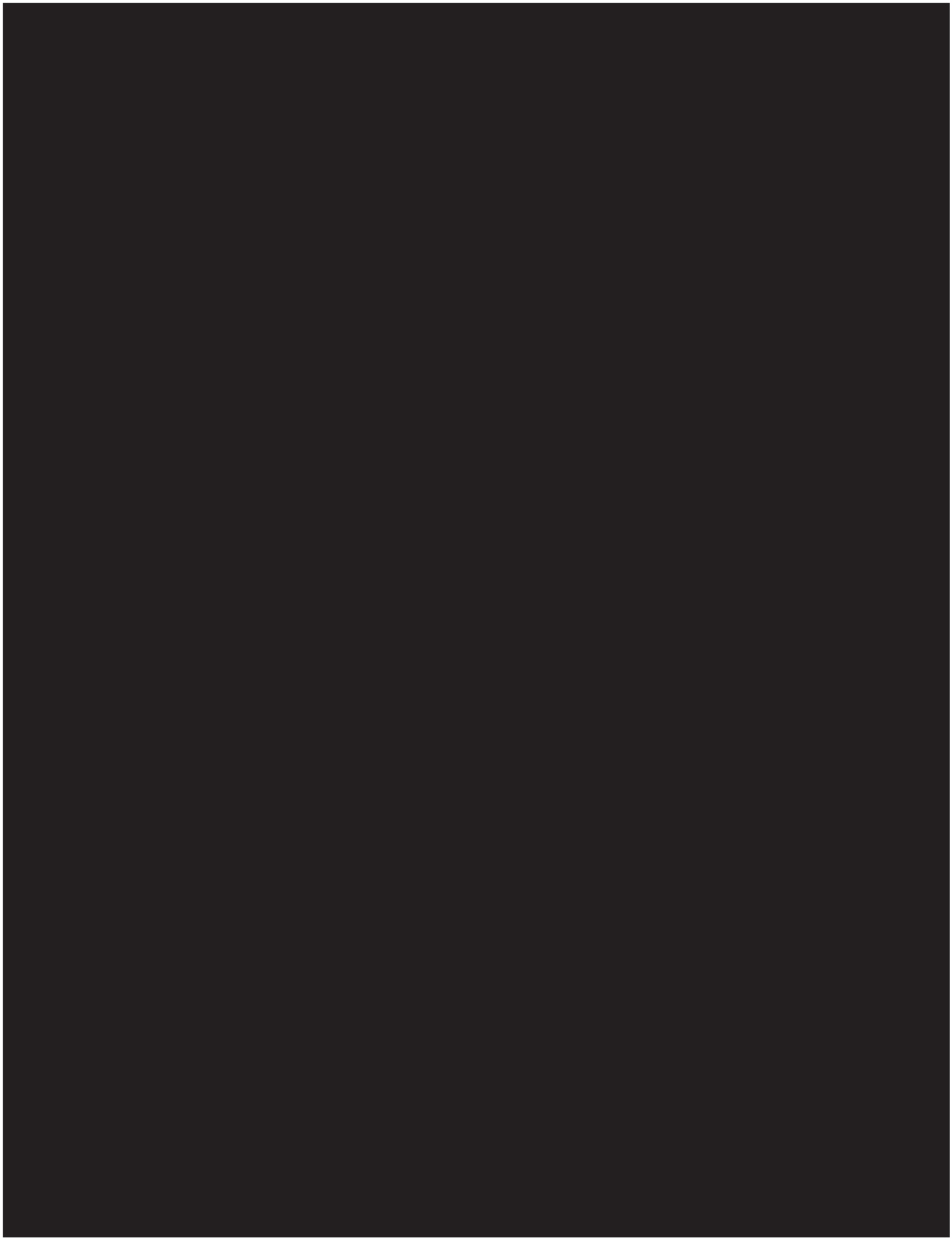
# INFORMATION SECURITY POLICY (ISP)



# INFORMATION SECURITY POLICY (ISP)

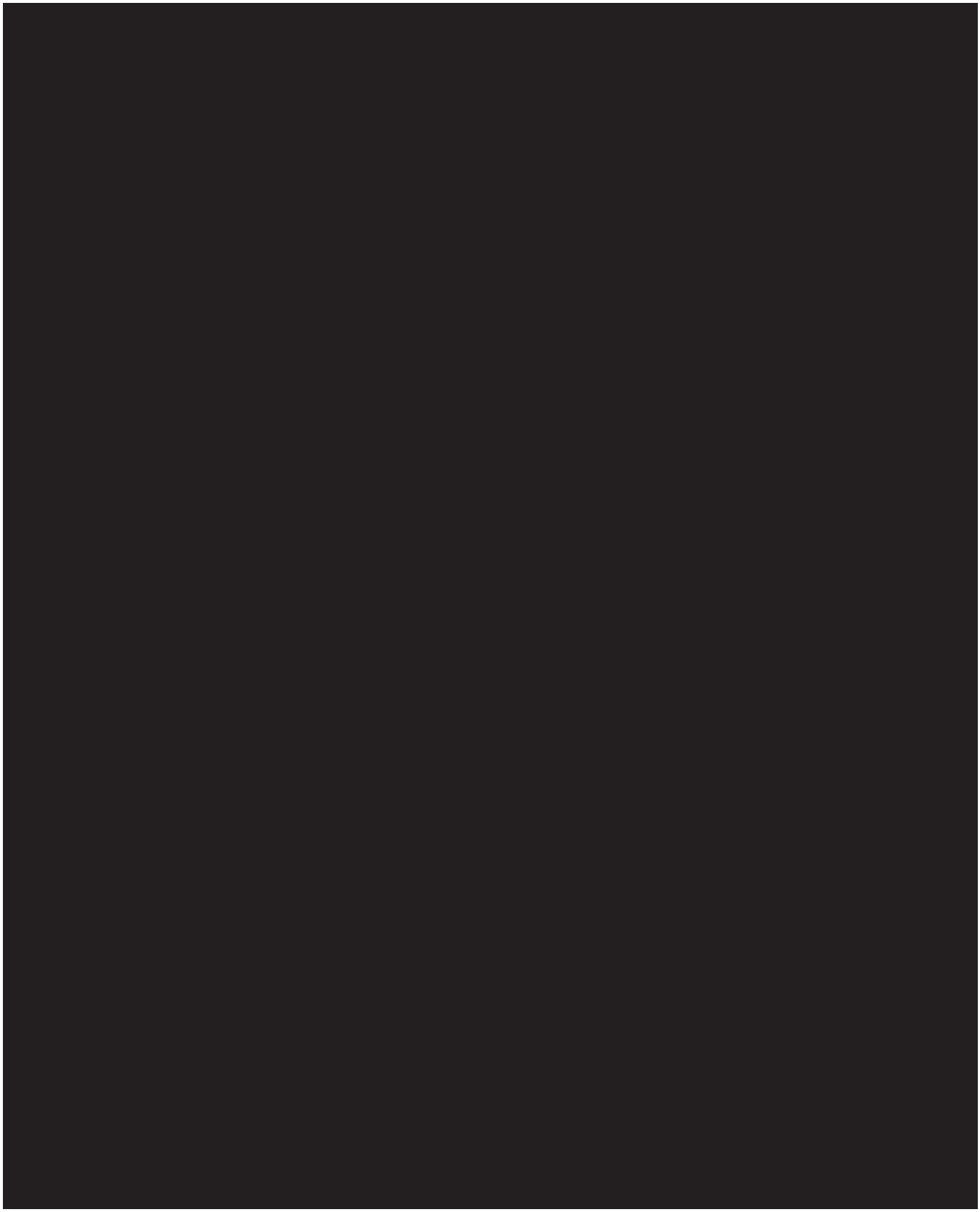


# INFORMATION SECURITY POLICY (ISP)

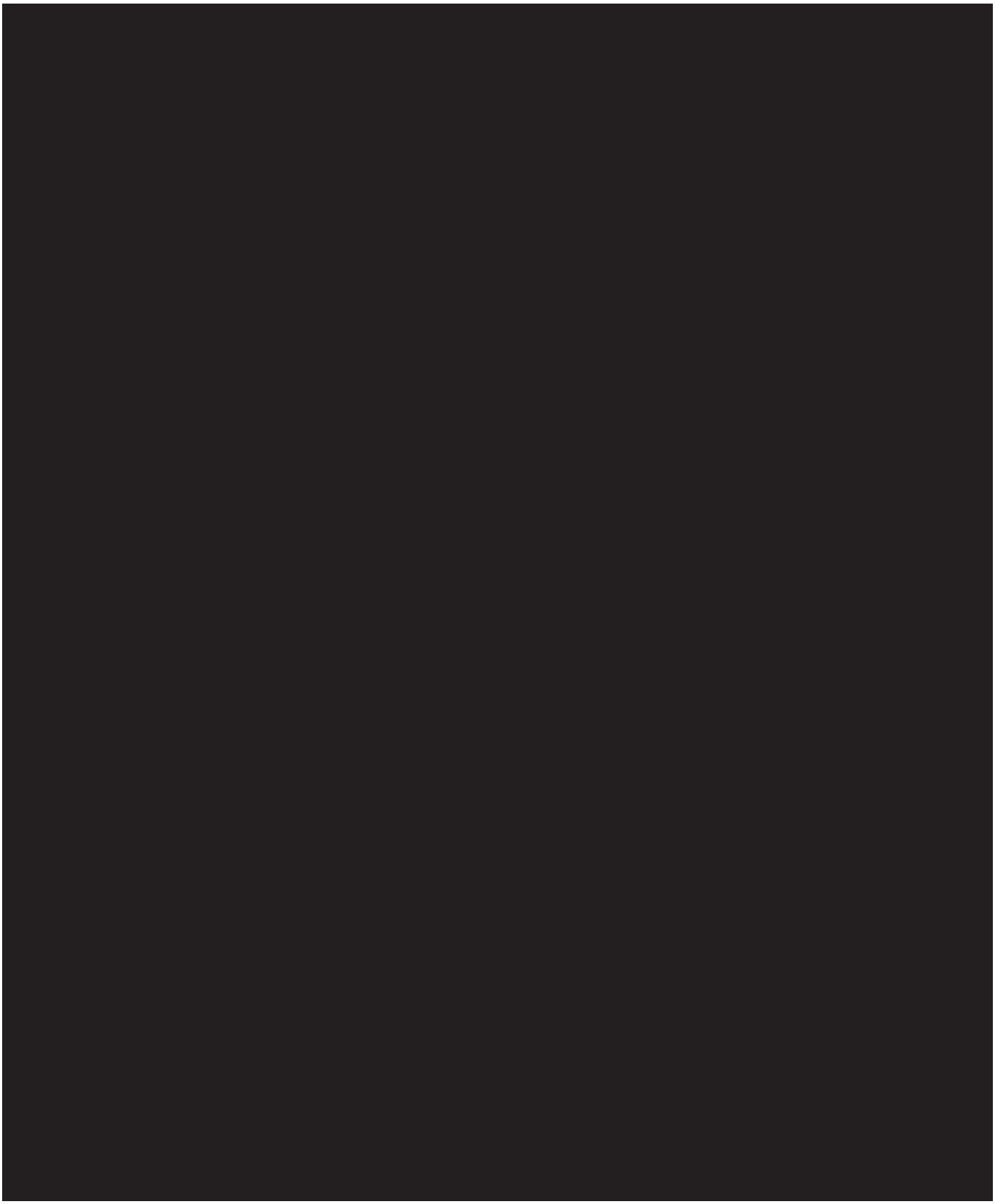


# INFORMATION SECURITY POLICY (ISP)

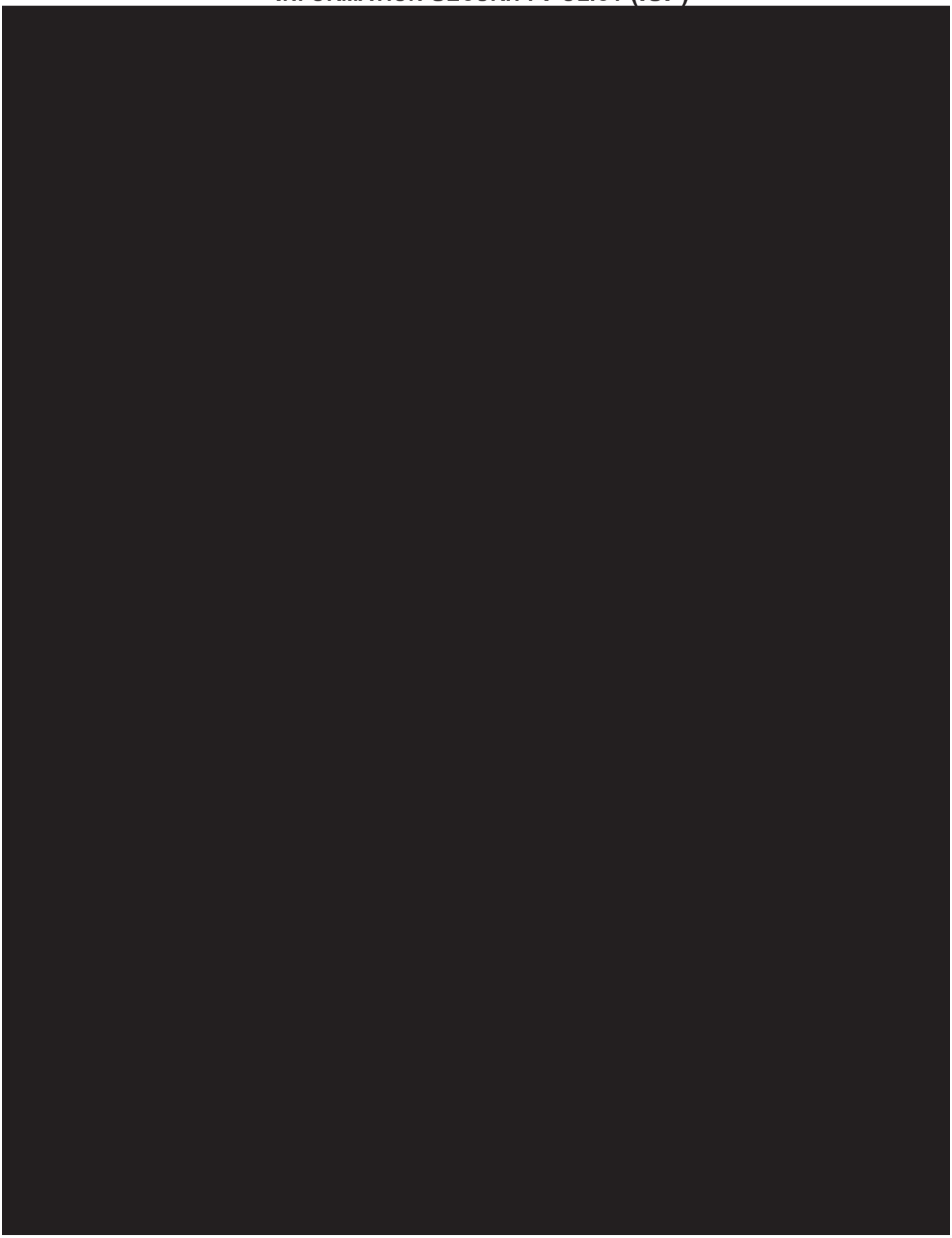
# INFORMATION SECURITY POLICY (ISP)



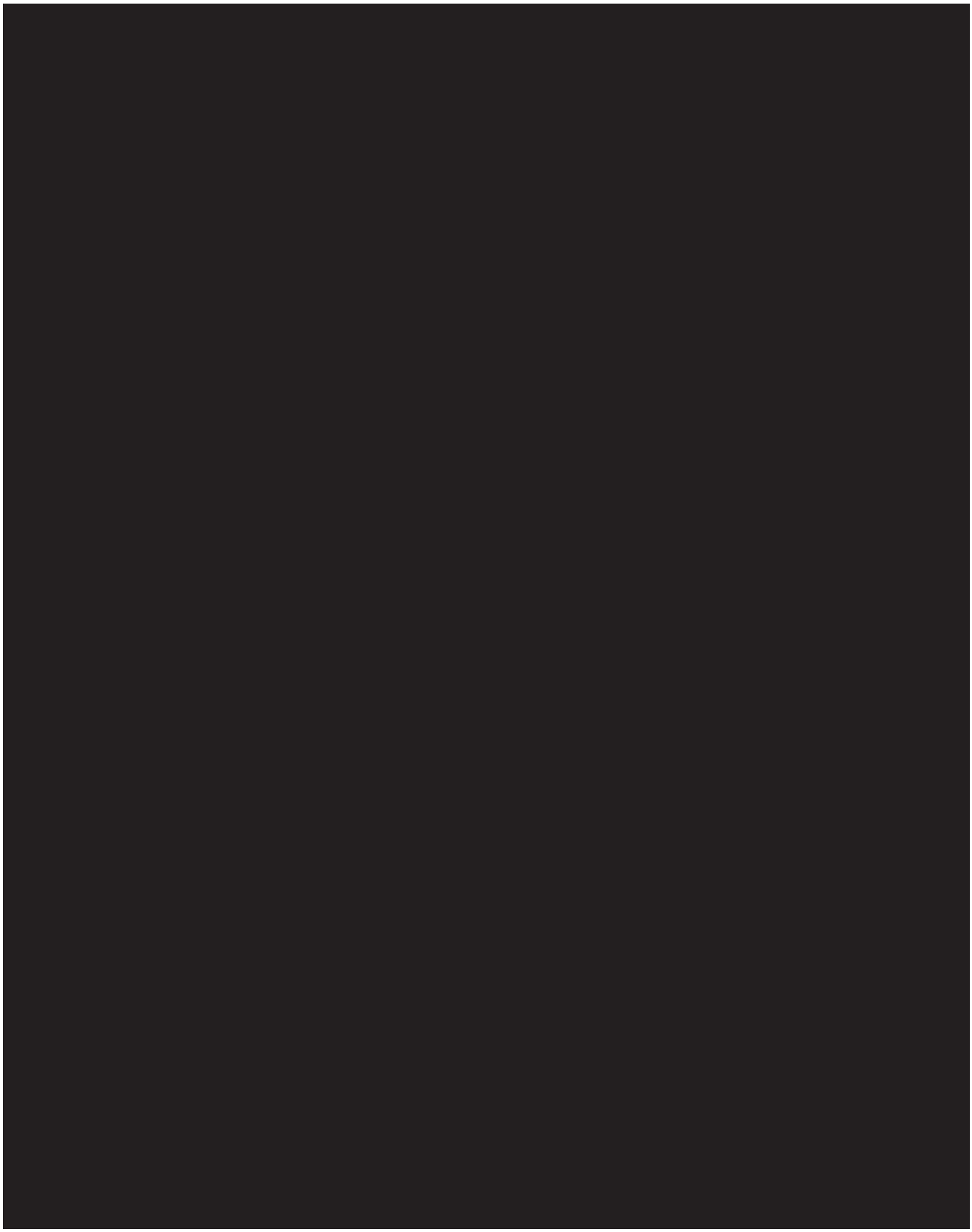
# INFORMATION SECURITY POLICY (ISP)



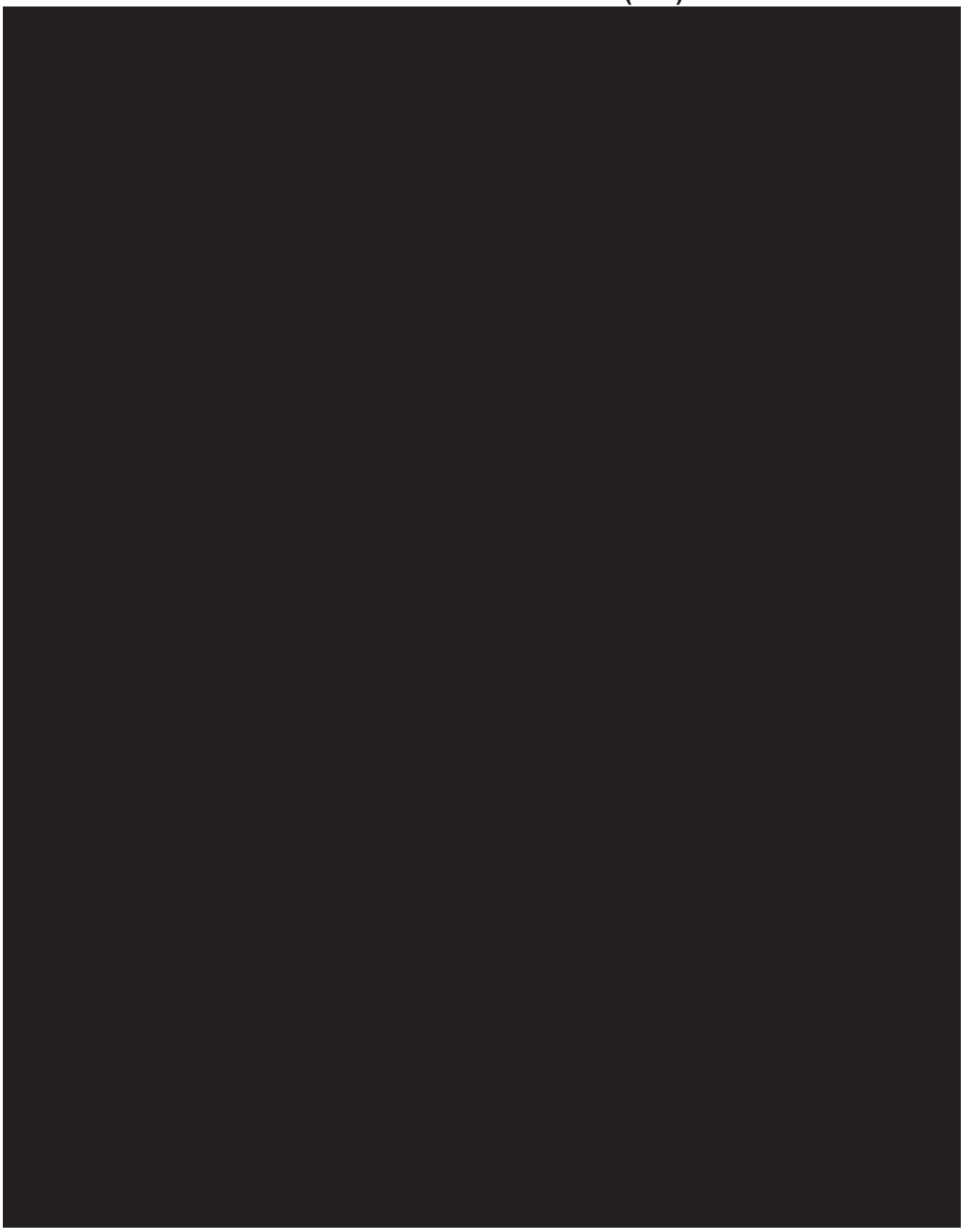
# INFORMATION SECURITY POLICY (ISP)



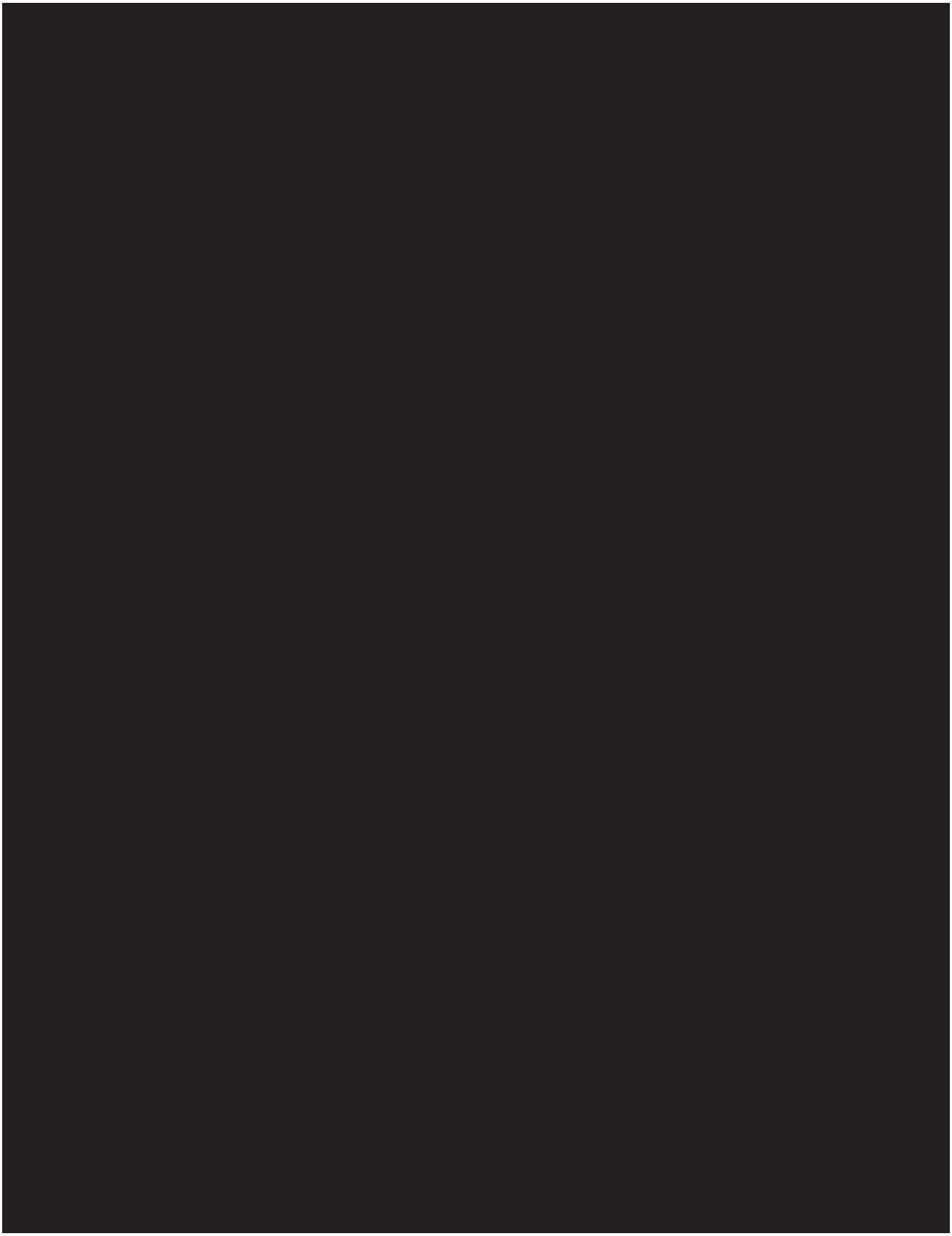
# INFORMATION SECURITY POLICY (ISP)



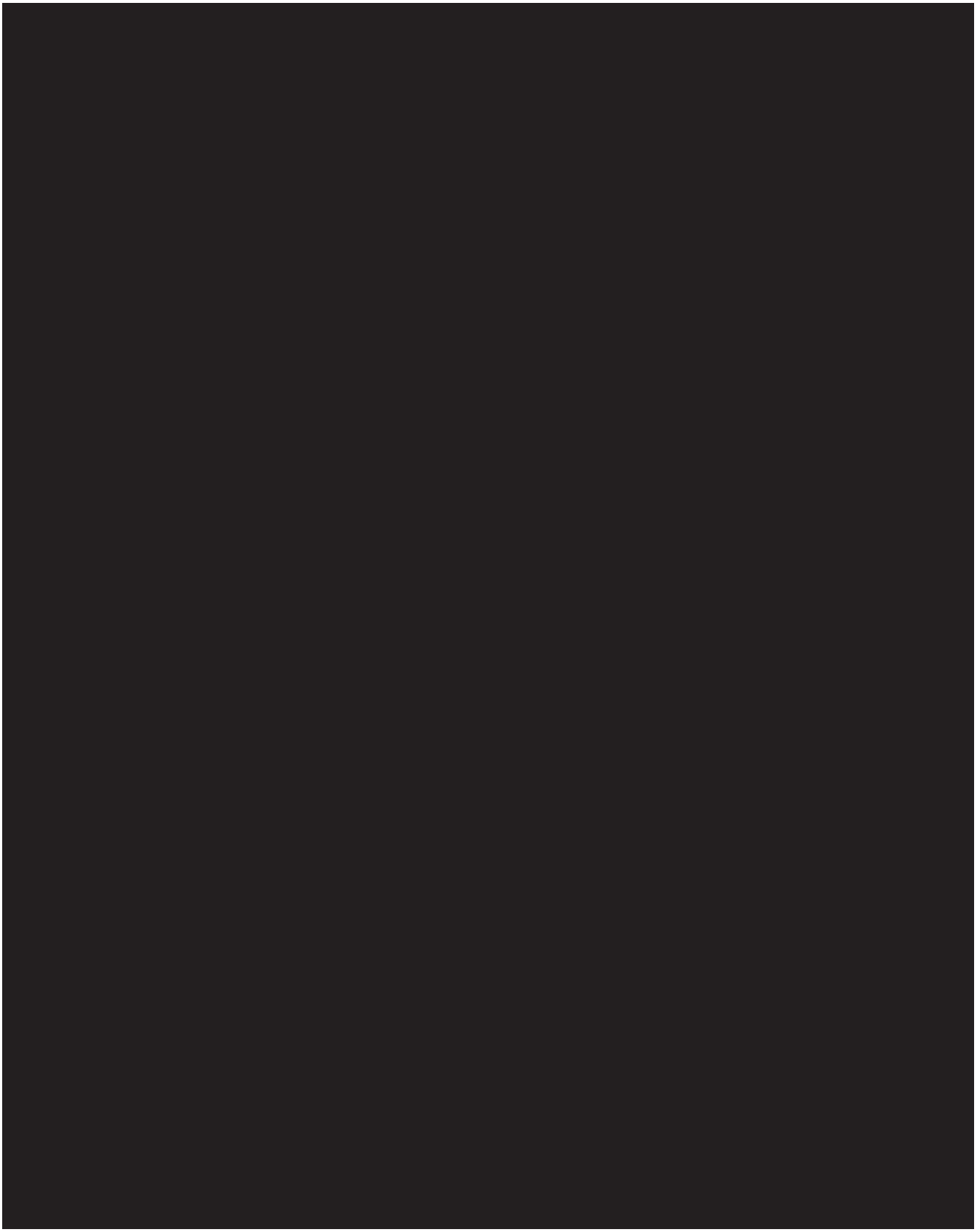
# INFORMATION SECURITY POLICY (ISP)



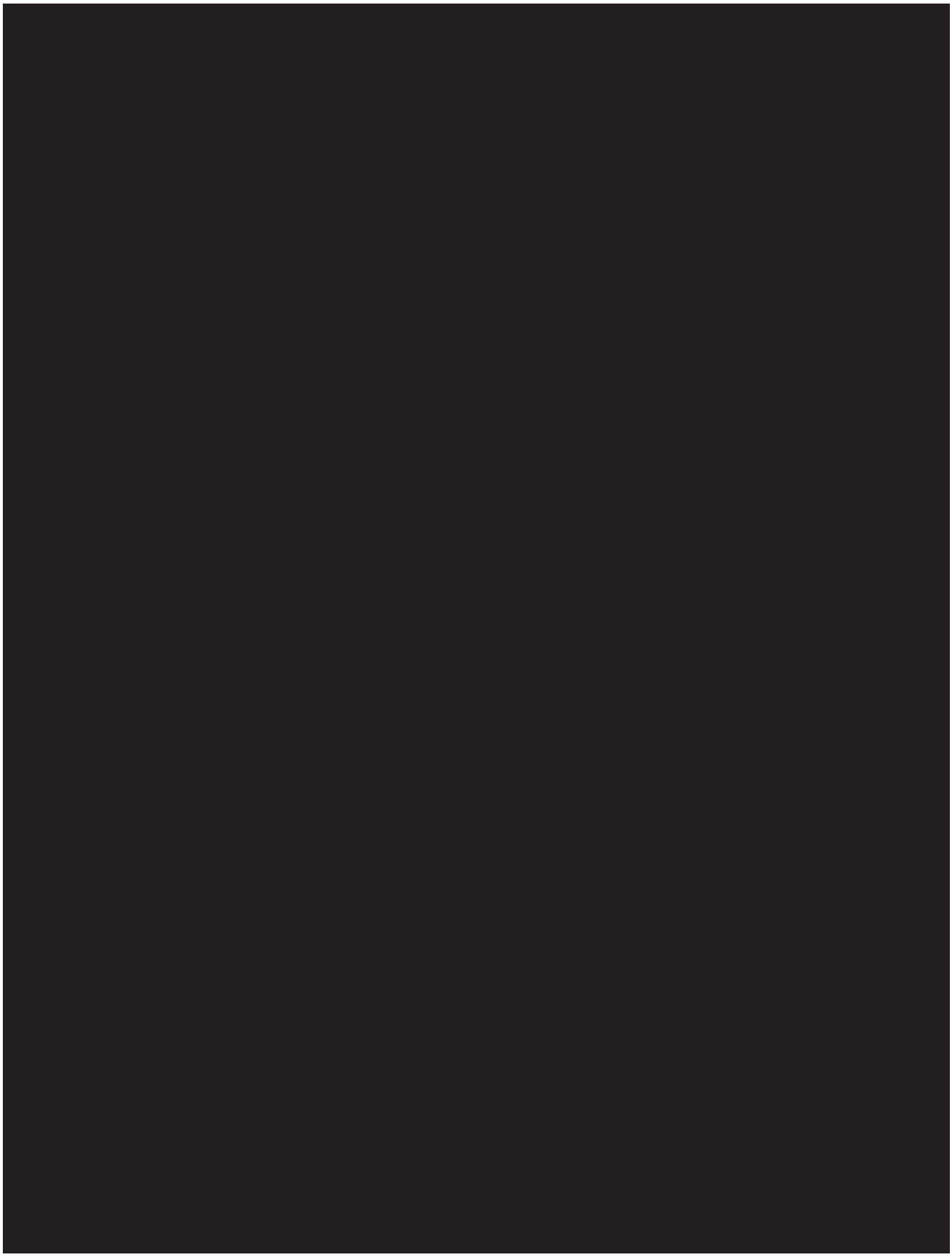
# INFORMATION SECURITY POLICY (ISP)



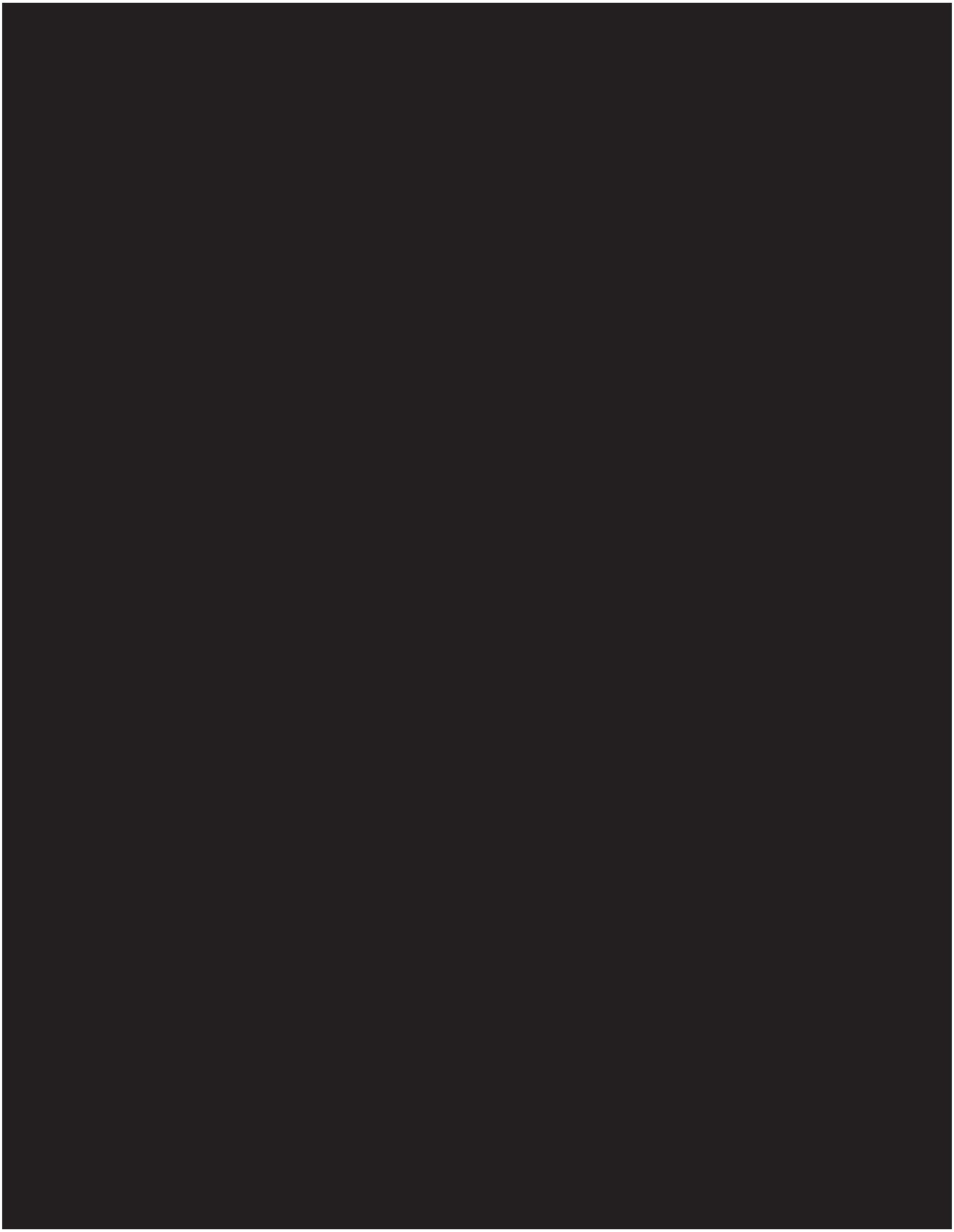
# INFORMATION SECURITY POLICY (ISP)



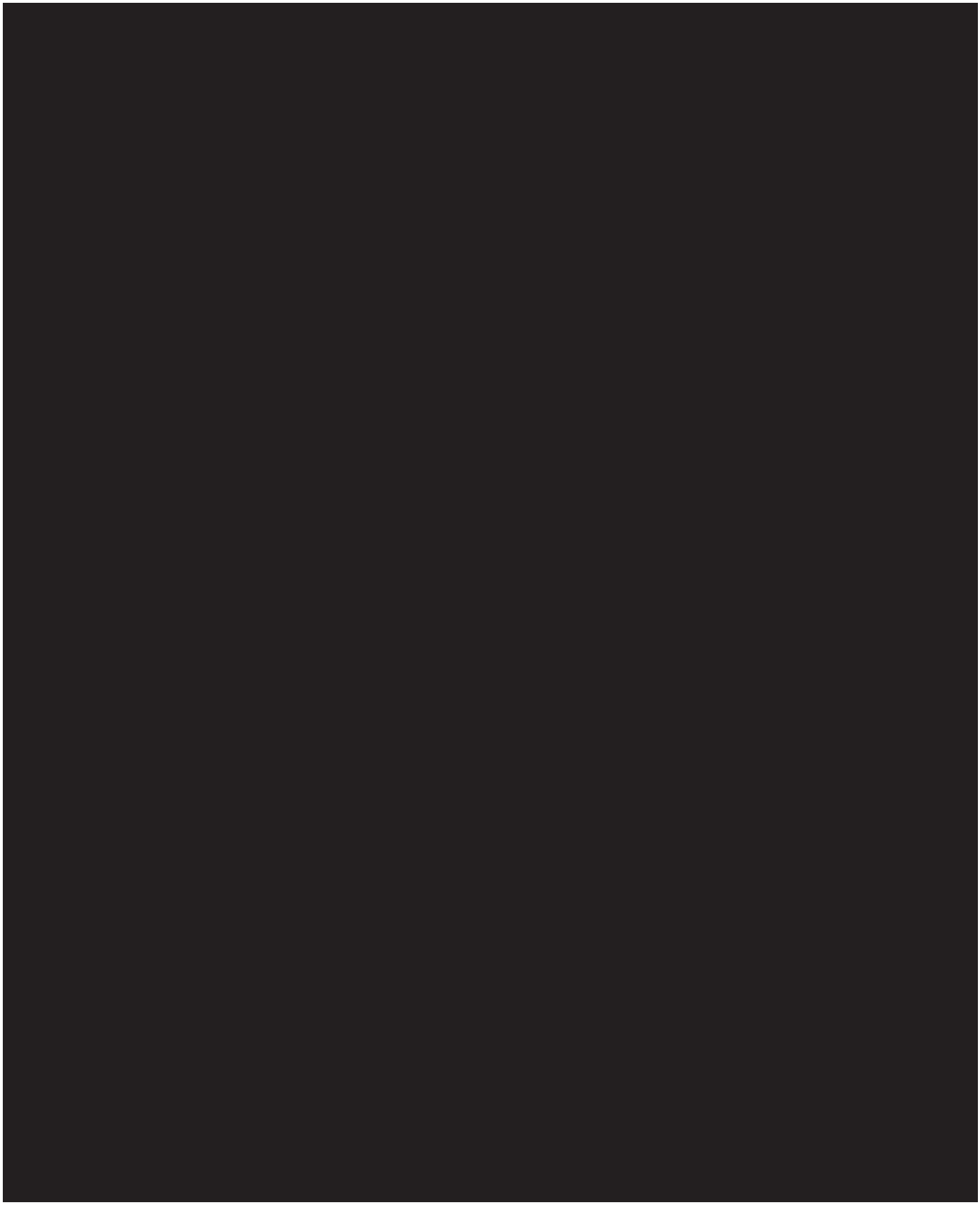
# INFORMATION SECURITY POLICY (ISP)



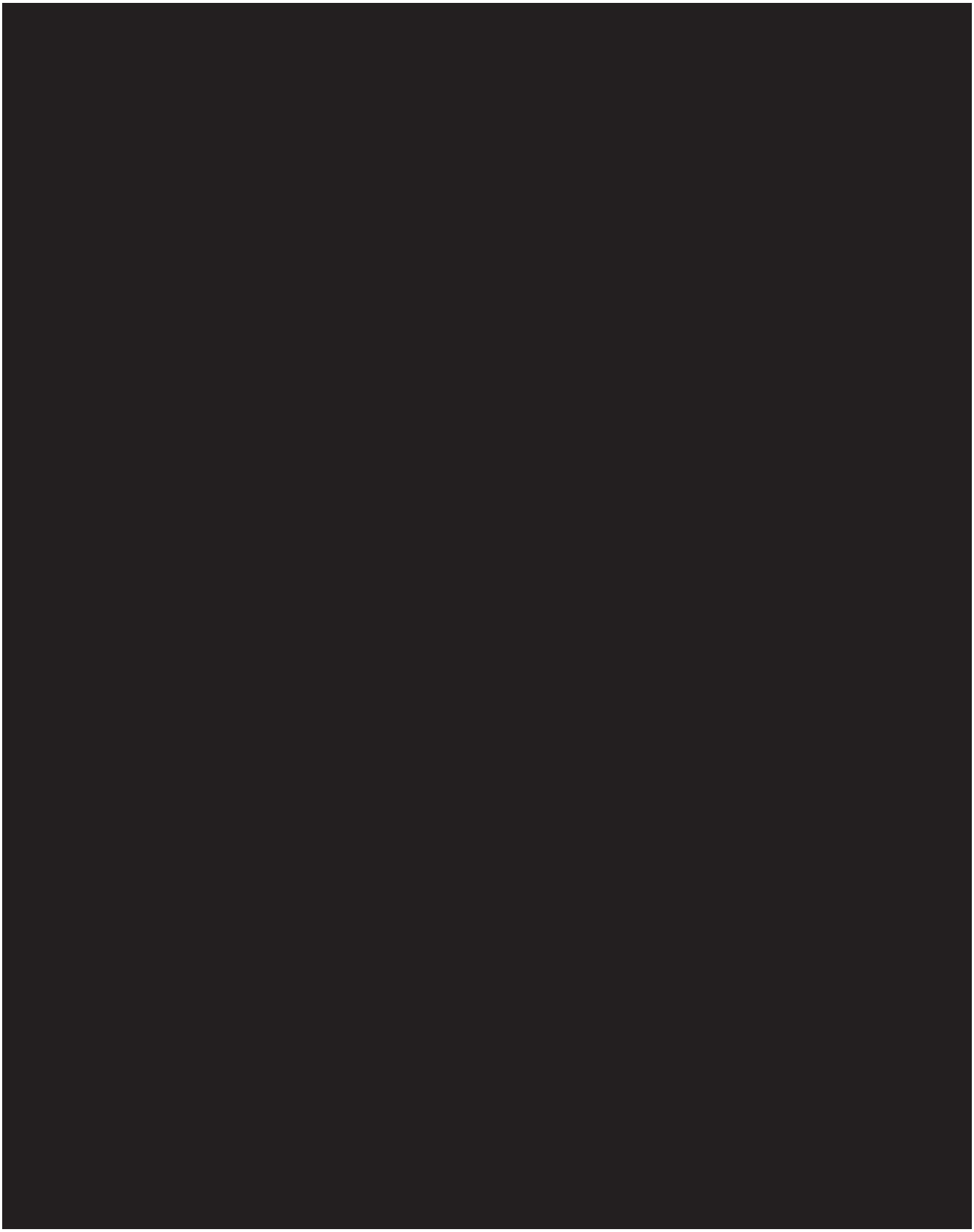
# INFORMATION SECURITY POLICY (ISP)



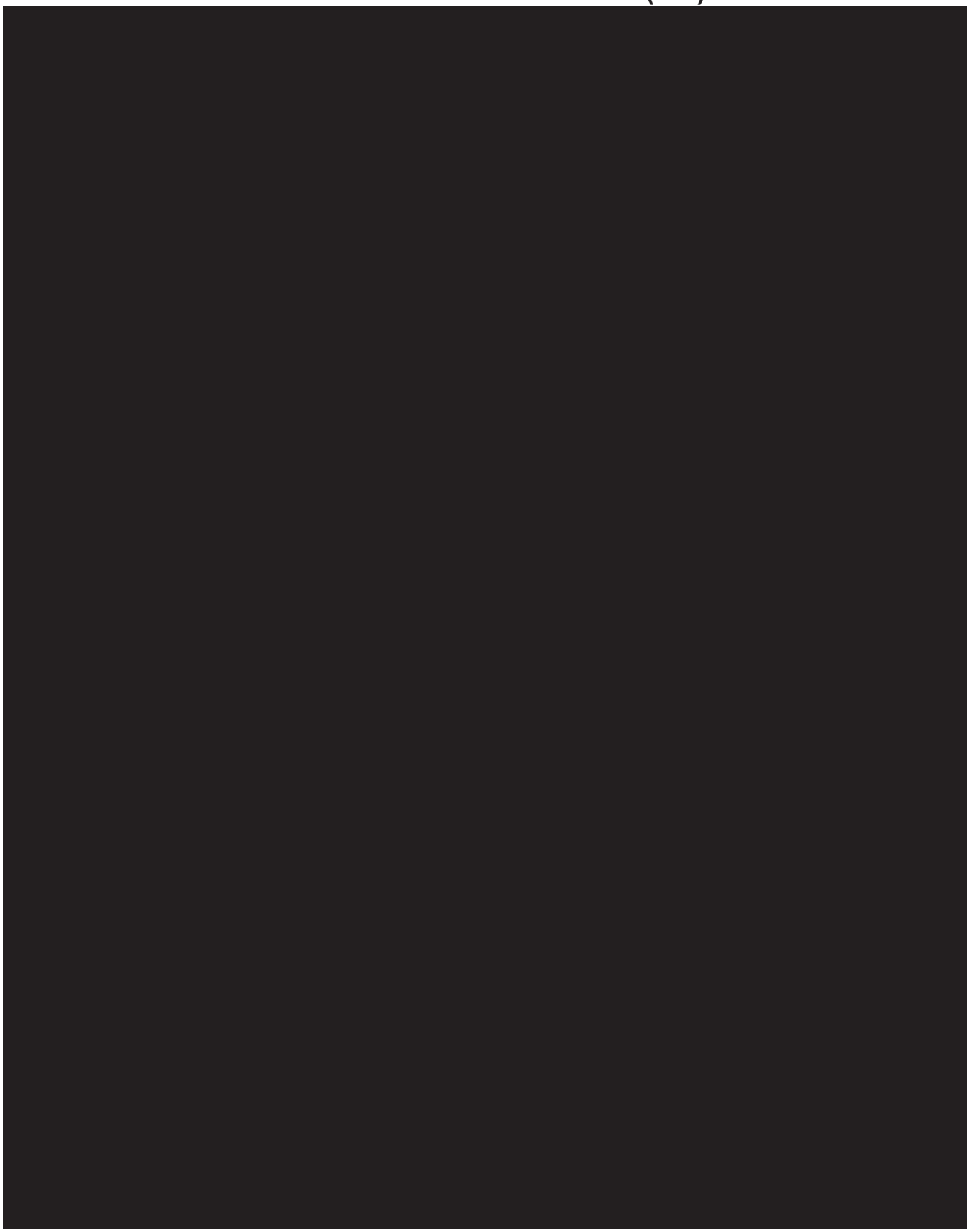
# INFORMATION SECURITY POLICY (ISP)



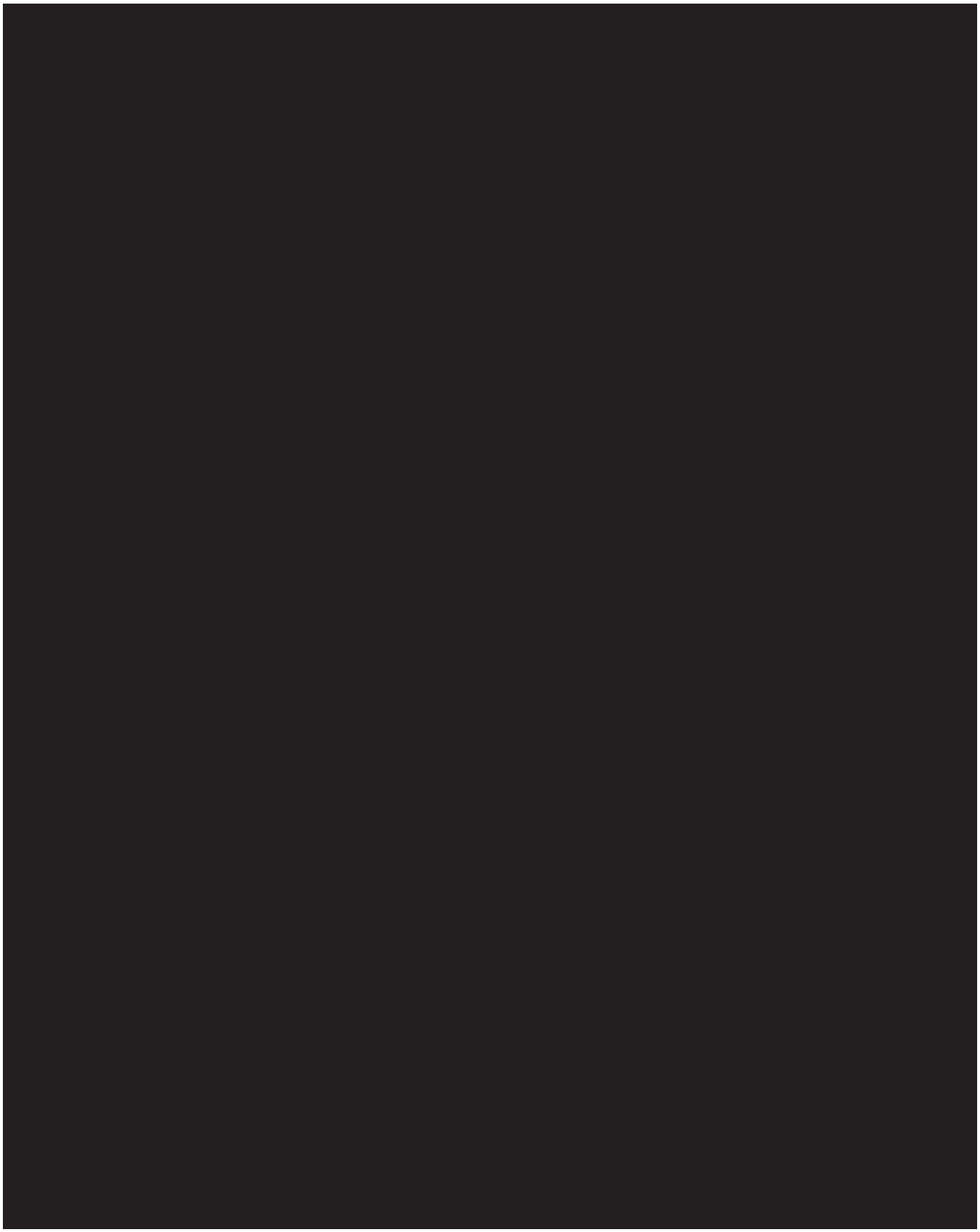
# INFORMATION SECURITY POLICY (ISP)



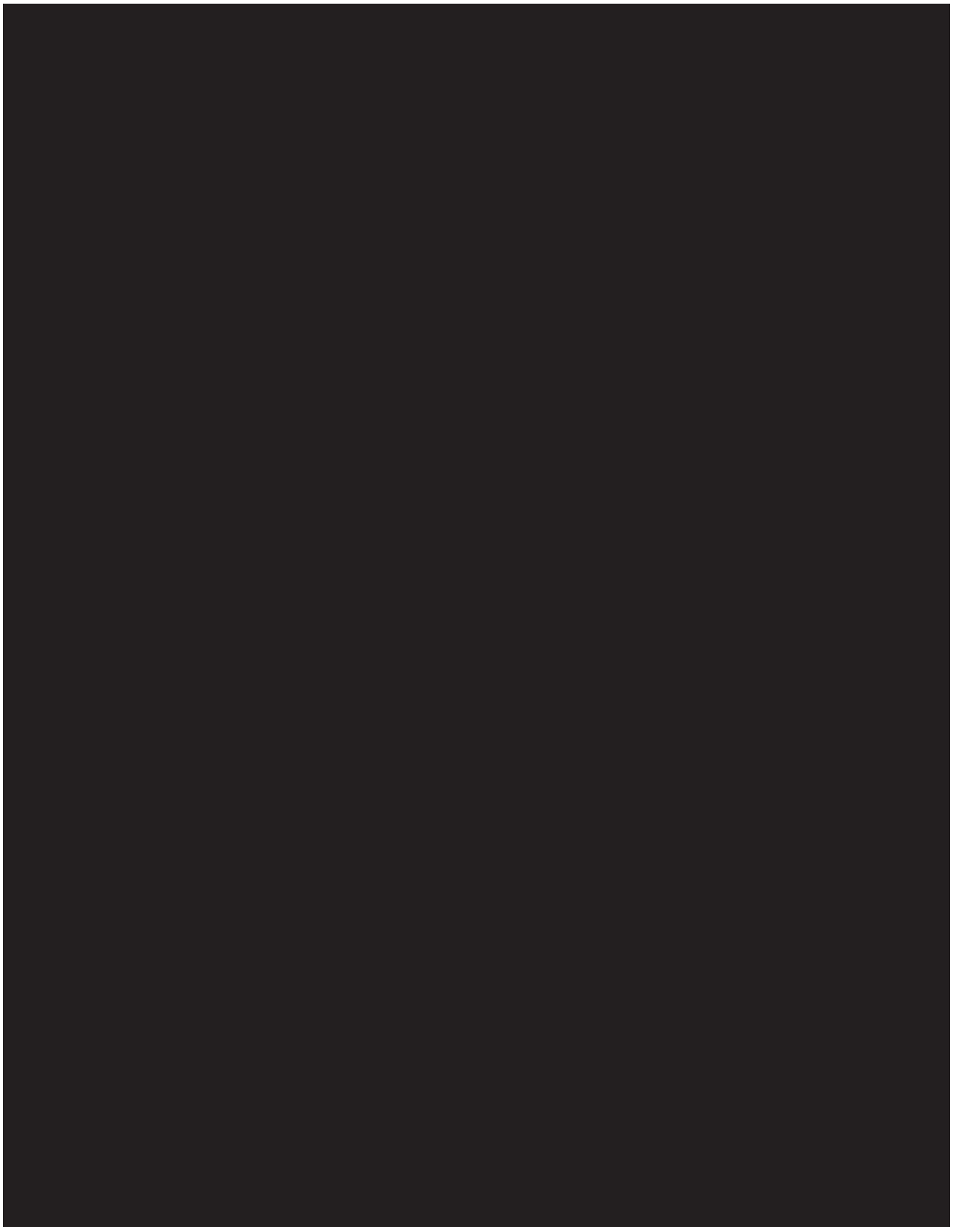
# INFORMATION SECURITY POLICY (ISP)



# INFORMATION SECURITY POLICY (ISP)

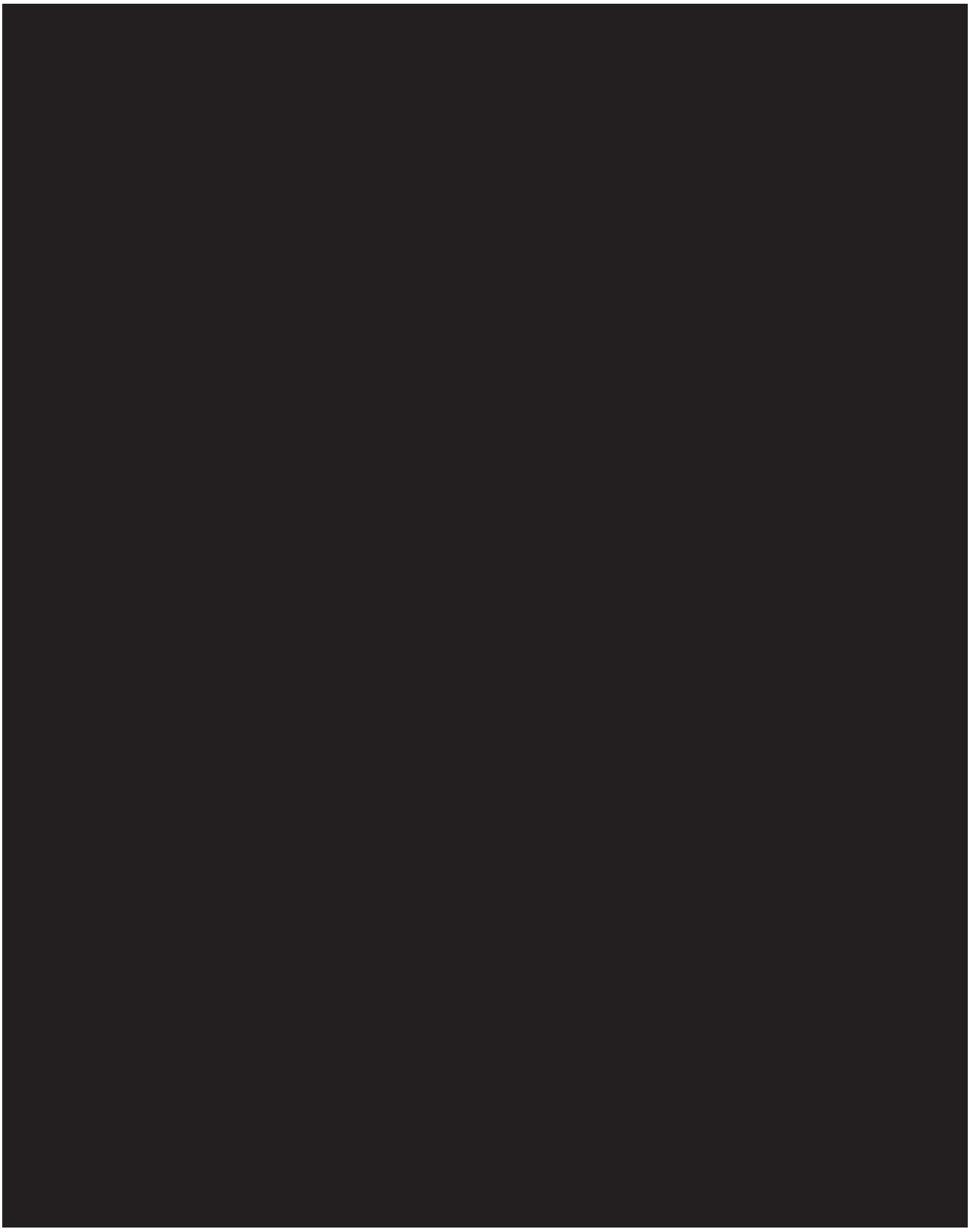


# INFORMATION SECURITY POLICY (ISP)

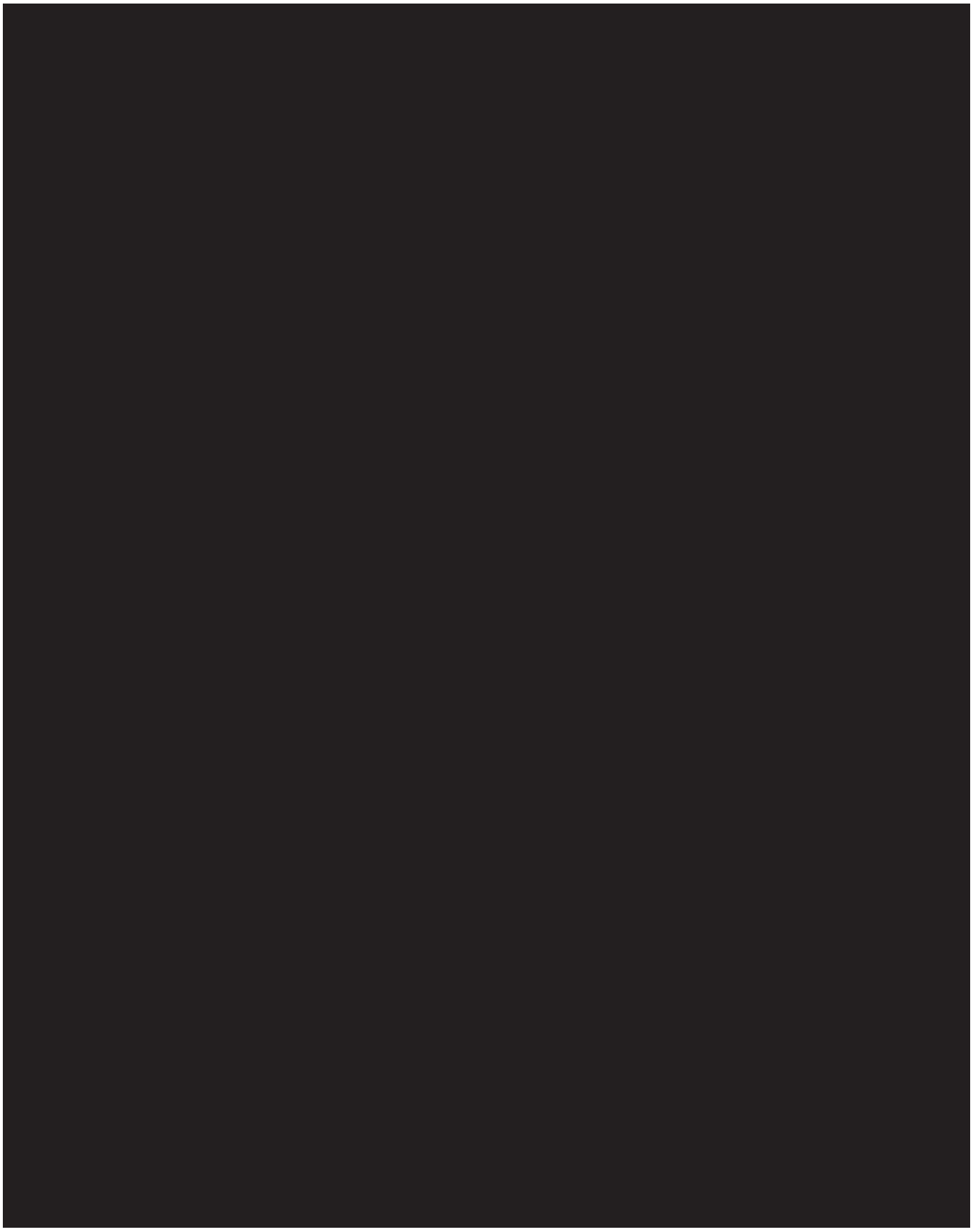


# INFORMATION SECURITY POLICY (ISP)

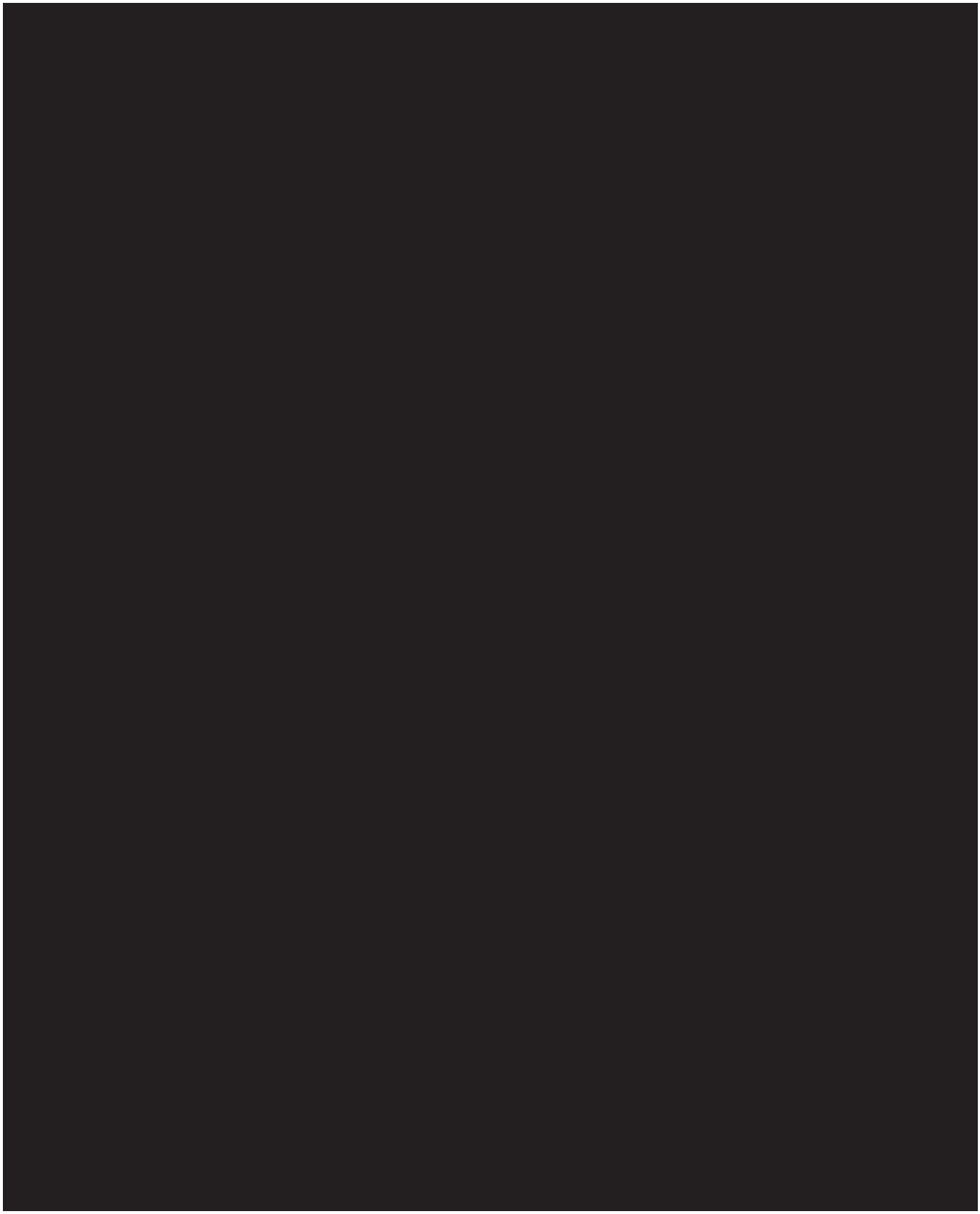
# INFORMATION SECURITY POLICY (ISP)



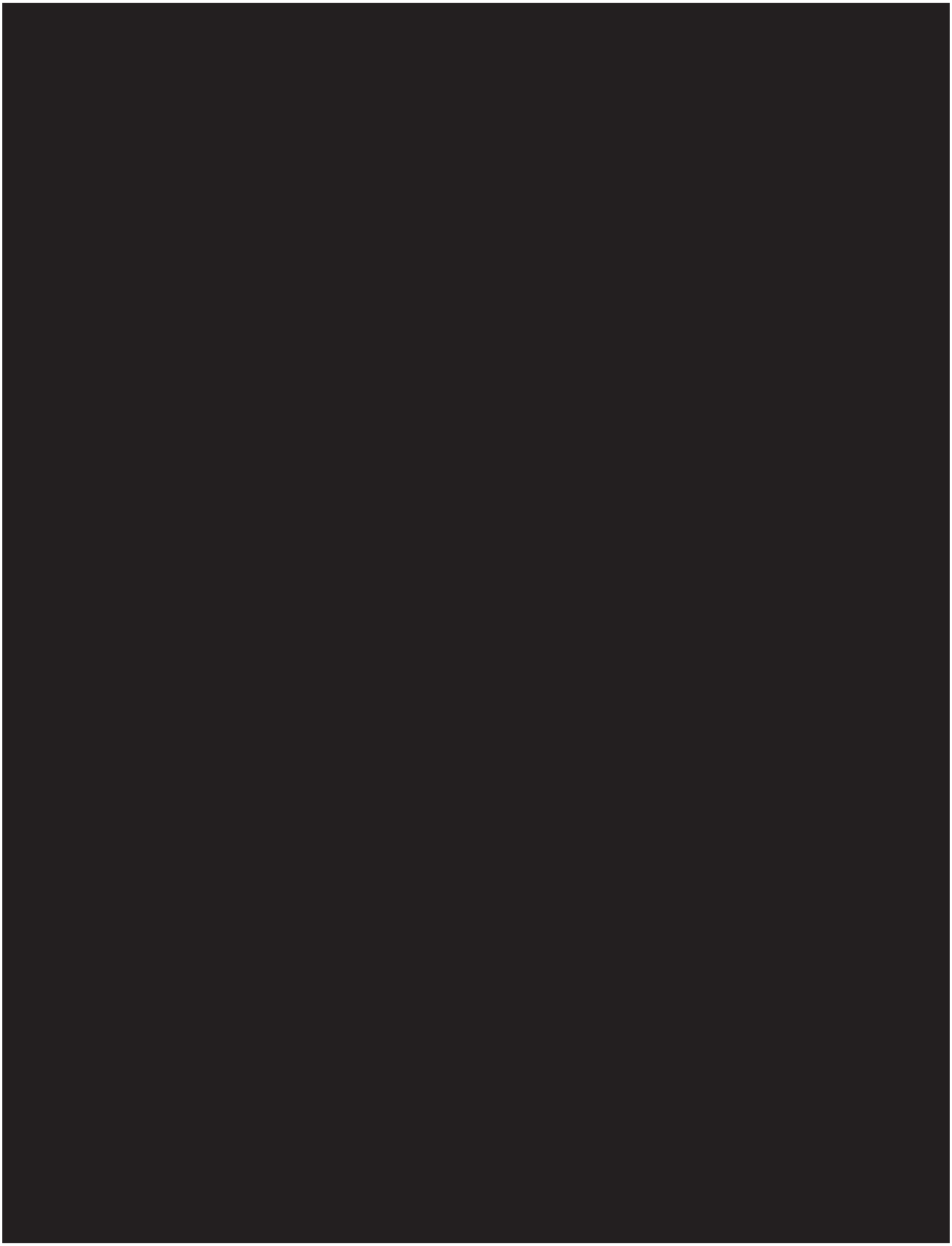
# INFORMATION SECURITY POLICY (ISP)



# INFORMATION SECURITY POLICY (ISP)



# INFORMATION SECURITY POLICY (ISP)



# INFORMATION SECURITY POLICY (ISP)

# Personnel Security and Suitability

**For bargaining unit employees, see applicable Union/Management Contracts in addition to the Personnel Policy Manual (PPM). Contract provisions take precedence over the PPM.**


1. ISSUE DATE
2. EMPLOYEES COVERED
3. LAW AND REGULATION
   3.1. Establishing a Security and Suitability Program
   3.2. Inquiring About Applicant's Criminal or Financial Information
   3.3. Inquiring About Other Applicant Factors
   3.4. Suitability and Security Adverse Actions
4. SSA DELEGATIONS OF AUTHORITY
5. SSA POLICY
   5.1. Establishing a Security and Suitability Program
   5.2. Inquiring About Applicants Criminal or Financial Information
   5.3. Making Security and Suitability Determinations and Taking Suitability Actions
   5.4. Complying with the Security and Suitability Program
   5.5. Taking Security and Suitability Adverse Actions
6. RECORDS RETENTION


## 1. ISSUE DATE – March 20, 2017 (Revised May 2017)

## 2. EMPLOYEES COVERED – All SSA employees.

## 3. LAW AND REGULATION

### 3.1. Establishing a Security and Suitability Program (See Section 5.1.)

All Federal agencies are responsible for ensuring that their employees are suitable for Federal employment. SSA makes personnel security and suitability determinations for its employees and takes suitability actions. Security and suitability is a condition of employment, and SSA employees must fully comply with the security and suitability process.

### 3.2. Inquiring About Applicant's Criminal or Financial Background (See Section 5.2.)

SSA may not make specific inquiries concerning an applicant's criminal or financial background of the sort asked on the Optional Form-306 or other forms used to conduct suitability investigations for Federal employment (i.e., inquiries into an applicant's criminal or adverse credit history) unless SSA has made a conditional offer of employment to the applicant.

In certain situations, agencies may have a business need to obtain information about the criminal or credit background of applicants earlier in the process. If so, agencies must request an exception from the Office of Personnel Management (OPM), in accordance with the provisions of 5 CFR part 330 subpart M. (See Section 5.2.)

### 3.3. Inquiring About other Applicant Factors

Agencies may make inquiries into, but not limited to, an applicant's Selective Service registration, military service, citizenship status, or previous work history, prior to a conditional offer of employment to an applicant.

### 3.4 Suitability and Security Adverse Actions (See section 5.5.)

Agencies may, upon a suitability finding, non-select a candidate after a conditional offer of employment is accepted, or take a suitability action. Agencies may take a suitability action before or after entrance on duty.

## 4. SSA DELEGATIONS OF AUTHORITY

## 5. SSA POLICY

### 5.1. Establishing a Security and Suitability Program (See Section 3.1.)

SSA provides a comprehensive security and suitability program. For persons who have access to SSA systems, records, data, and/or facilities, the agency is required to make suitability determinations based on a person's character or conduct that may have an impact on the integrity or efficiency of the service they provide for the agency. SSA accomplishes this through conscientious, fair, and thoughtful application of federal statutes and rules pertaining to suitability and security.

**5.2. Inquiring About Applicant's Criminal or Financial Information (See Section 3.2.)**

Servicing personnel offices may request information regarding an applicant's criminal or adverse financial history after a conditional job offer, and the selecting official may rescind the job offer if SSA discovers unfavorable information.

In addition, if components believe there is a business need to obtain information about the suitability or background of certain applicants earlier in the hiring process, they should send their request for an e [redacted]. The request should include the position title, series, grade and a detailed explanation of the business need warranting the exception.

**5.3. Making Security and Suitability Determinations and Taking Suitability Actions**

Delegated officials (See Section 4.) are responsible for making security and suitability determinations and taking suitability actions for SSA employees.

**5.4. Complying with the Security and Suitability Program**

All employees are subject to personnel security and suitability investigations and must:

- Comply with the SSA Security and Suitability Program, which requires completion of documents, fingerprinting, possible recompletion of forms, and requests for supplemental information and documentation as deemed necessary by the agency; and
- Timely submit all required documentation and provide all supplemental information as requested by the agency.

SSA will determine if prior background investigations performed by other Federal agencies are acceptable under OPM's rules of reciprocity.

To the extent possible, supervisors must ensure that their employees comply with SSA's Security and Suitability Program.

Supervisors must inform the Center for Suitability and Personnel Security promptly of employee behavior that could affect the efficiency or integrity of service or that indicates possible variances with the SSA Security and Suitability Program standards and criteria to the delegated official (See Section 4).

Supervisors must complete the Position Risk Designation Management Survey and provide all information required to determine a position's appropriate risk designation level and investigative requirements to the delegated official (See Section 4) when:

- A new Position Description is created; or
- An existing Position Description is modified.

**5.5. Taking Security and Suitability Adverse Actions**

The security and suitability process may include subject interviews, subject submission of documents to SSA's security and suitability program, and SSA collection of documents, or other requests. Employees must fully comply with the suitability process.

Dependent upon the findings of the security and suitability process, SSA may rescind conditional offers of employment or take suitability actions prior to entrance on duty. SSA may take suitability actions after entrance on duty.

## 6. RECORDS RETENTION

Records must be kept according to the National Archives and Records Administration (NARA) General Records Schedule 2.1., Employee Acquisition Records. This schedule can be accessed through the NARA web site.

Office of Information Security



## Principle of *Least Privilege*

This guidance is to provide further details on the definition of the principle of *Least Privilege*.

- What is *Least Privilege?*
  - The principle of Least Privilege requires that a user be given no more privileges than those necessary to perform their job.
  - *Least Privilege* restricts user access to the minimum amount of systems resources needed to perform assigned job duties or responsibilities. Whenever access is granted, it is always limited to those who have a legitimate need for these resources to perform their assigned position responsibilities.
- Why *Least Privilege?*
  - Unlimited rights and access can equate to unlimited potential for damage. The more privileges an account or user has, the greater potential for abuse or errors.
- Guidance for applying *Least Privilege*:
  - Identify the user's current job
  - Determine the minimum privileges required
  - Restrict the user to those privileges
  - Consider the resource you are trying to protect. What is the *Least Privilege* amount of access you should grant in order to protect the resource and still allow those employees who need access to do their job?
- What can you do to ensure you are in compliance with SSA's *Least Privilege* policy?

  Managers/Component Security Officers must:
  - Review who has access to resources
  - Know the content of your resources
  - Know the sensitivity of your resources
  - Review permissions and remove any inappropriate access

Emergency Numbers Emergency Preparedness Medical Emergency Numbers

Maintained by OIS Web Team

Last reviewed or modified: 06/17/2024

# EXPERT OR CONSULTANT
# APPOINTMENT REQUEST & CERTIFICATION

| | |
|---|---|
| 1. NAME OF PERSON *(Last, first, middle initial)*<br>2. Employee 1 | 2. TOTAL PERIOD FOR WHICH APPOINTMENT IS REQUESTED *365* |
| 3. MAILING ADDRESS | 4. APPROXIMATE NUMBER OF DAYS PERSON IS EXPECTED TO PERFORM SERVICES DURING THIS PERIOD.365 |

5. SERVICES TO BE PERFORMED

A. EXPLAIN IN FULL THE SERVICES TO BE PERFORMED.

Access to all SSA systems and the associated source code to assist with modernization efforts agreed to by the CIO

The duties relate to improper payments and the Death Master File. Below is a beginning description, but this is a work in progress:

1. Evaluate the existence of matches between the agency's pay list and the Death Master File and analyze the causes. If matches are found offer recommendations for improvements.
2. Evaluate the existence of matches between the agency's pay list and the "Do Not Pay" file and analyze causes. If matches are found offer recommendations for improvements.
3. Assess the current process used by SSA to obtain information for the Death Master File and offer recommendations for improvement of the process by which information is obtained.
4. Prepare recommendations related to the duties above and without using the active production system, provide examples of code improvements.

Employee 1 will be performing analysis of SSA payment data to reduce concerns raised by the administration. This will include analyzing our current payments to beneficiaries against other SSA records to identify potential improper payments. Data needed to perform the analysis will be SSA payment files sent to Treasury and potentially the Numident, Master Beneficiary Record (MBR), and Supplemental Security Record (SSR). Security controls will be implemented to prevent Employee 1 from accessing or viewing sensitive data within any of these records.

B. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE TRANSACTION OF BUSINESS ON BEHALF OF THE GOVERNMENT WITH ANY PROFIT OR NON-PROFIT ORGANIZATION.

None

C. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE RENDERING OF ADVICE TO THE GOVERNMENT WHICH WILL HAVE DIRECT AND PREDICTABLE EFFECT ON THE INTERESTS OF ANY PROFIT OR NON-PROFIT ORGANIZATION.

None

6. SPECIAL QUALIFICATIONS OF THE PERSON RECOMMENDED FOR APPOINTMENT *(List those which relate specifically to the services to be performed.*

Hands-on software engineer that is an expert in modern computer programming languages, cloud and other infrastucture, AI, etc.

5 years of experience using numerous computer code languages, leadership of teams in technical, software design, and infrastructure areas.

CERTIFICATION

In approving the appointment of this consultant/expert, I have considered the requirements of law, relevant decisions of the Comptroller General, and Office of Personnel Management Department policies and instructions. More specifically, I have satisfied myself that:

1. The services of the individual are essential for effective program management

2. The duties to be performed are those of (check one)

   ___a consultant (that is, they are purely advisory in nature and will not include the performance or supervision of operating functions)

   X__an expert (that is, they require a high level of expertise not available in the regular work force)

3. The proposed appointee is qualified to (check one)

   ___provide advisory services as a consultant under 5 CFR 304

   X__serve as an expert under 5 CFR 304

4. The appointment is appropriately designated as (check one)

   ___Intermittent not to exceed 1 year (the individual will work occasionally and irregularly) not to exceed the equivalent of 6 months.

   ___Part-time not to exceed 1 year.

   Provide tour: _____

   X___Full-time not to exceed 1 year

5. The appropriate appointment authority is being used

6. The pay level is GS grade/step _13/1_____ equivalent. This is appropriate for the duties to be performed and the qualifications of the appointee (Minimum GS 13/1 base salary. Maximum GS-15/10 base salary.)

   ___Appointee will waive compensation (attach written agreement)

7. The record of appointment has been clearly documented to show the services to be performed and the special qualifications of the appointee which relate specifically to those services.

8. A statement of employment and financial interests has been obtained and it has been determined that no conflict of interest exists (OGE Form 450 was reviewed. Components retain this form).

2/13/25
Date

[redacted]
Signature of Component Program Manager Authorized to Obtain the Consultant's/Expert's Services (This certification relates particularly to items 1, 2, 3, 6, 7 and 8)

2/13/25
Date

[redacted]
Signature of DCHR/CPPS Appointing Official (This certification relates particularly to items 2 through 8)

EXPERT OR CONSULTANT
APPOINTMENT REQUEST & CERTIFICATION
**(Submit with Resume)**

| | |
|---|---|
| 1. NAME OF PERSON *(Last, first, middle initial)* Employee 4 | 2. TOTAL PERIOD FOR WHICH APPOINTMENT IS REQUESTED *(entire year (365) days or a shorter period). List dates from beginning to end month/day/year.* 365 days |
| 3. MAILING ADDRESS [redacted] | 4. APPROXIMATE NUMBER OF DAYS PERSON IS EXPECTED TO PERFORM SERVICES DURING THIS PERIOD. 365 days |

5. SERVICES TO BE PERFORMED

A. EXPLAIN IN FULL DETAIL THE NON-CONTINUOUS/TEMPORARY NATURE OF THE WORK TO BE PERFORMED AND THE NECESSITY FOR THE POSITION TO ACTUALLY REQUIRE AN EXPERT'S OR CONSULTANT'S SERVICES AS OPPOSED TO A REGULAR GOVERNMENT EMPLOYEE, OR IN THE CASE OF A REAPPOINTMENT (WITH SAME DUTIES), THE CONTINUING NEED FOR THE SERVICES OF AN EXPERT OR CONSULTANT (AND HOURS/DAYS WORKED IN PRECEDING YEAR).

SSA is facing significant issues that require immediate attention. Two of the most substantial areas in need of timely attention include: (1) Numident records with death data and (2) Payment data, focused on reducing improper payments.

B. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE TRANSACTION OF BUSINESS ON BEHALF OF THE GOVERNMENT WITH ANY PROFIT OR NON-PROFIT ORGANIZATION.

1. Examine the recent Ernst & Young audit of SSA.

2. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

3. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

4. Review prior audits and studies concerning improvements to SSA's Numident death records and assess the current process used by SSA to obtain death information for SSA's programs and offer recommendations for improvement of the process by which information is obtained;

5. Prepare recommendations related to the duties above and, without using the active production system, provide examples of code improvements;

6. Conduct analysis of SSA payment data to reduce concerns improper payments. This will include analyzing data of SSA current payments to beneficiaries against other SSA records to identify potential improper payments; and

7. Data needed to perform the analysis will be SSA payment files sent to Treasury and potentially the Numident, Master Beneficiary Record (MBR), and Supplemental Security Record (SSR). Security controls will be implemented to prevent detailee from accessing or viewing sensitive data within any of these records.

C. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE RENDERING OF ADVICE TO THE GOVERNMENT WHICH WILL HAVE DIRECT AND PREDICTABLE EFFECT ON THE INTERESTS OF ANY PROFIT OR NON-PROFIT ORGANIZATION.

None

6. SPECIAL QUALIFICATIONS OF THE PERSON RECOMMENDED FOR APPOINTMENT *(List those which relate specifically to the services to be performed.*

Employee 4 is the Founder, Chief Executive Officer, and Chief Investment Officer of [redacted] founded [redacted] in [redacted] He has over 25 years of experience in private equity investing. Employee 4 was a Director of [redacted] During his tenure, he served as [redacted] He is a Director of [redacted]. He is a member of [redacted].

CERTIFICATION

In approving the appointment of this consultant/expert, I have considered the requirements of law, relevant decisions of the Comptroller General, and Office of Personnel Management Department policies and instructions. More specifically, I have satisfied myself that:

1. The services of the individual are essential for effective program management

2. The service of the expert or consultant does not duplicate any previously performed work or service, and that the service is not currently available within SSA

3. The duties to be performed are those of (check one)

   ___a consultant (that is, they are purely advisory in nature and will not include the performance or supervision of operating functions)

   X__an expert (that is, they require a high level of expertise not available in the regular work force)

4. The proposed appointee has a high degree of attainment in the field and is qualified to (check one):

   ___provide advisory services as a consultant under 5 CFR 304

   X__Intermittent not to exceed 1 year (the individual will work occasionally and irregularly) not to exceed the equivalent of 6 months.

   ___Part-time not to exceed 1 year.

   Provide tour: _____

   ___Full-time not to exceed 1 year

5. The expert and consultant appointing authority is the most appropriate authority to use

6. The pay level is GS grade/step _15/10_____ equivalent. This is appropriate for the duties to be performed and the qualifications of the appointee (Minimum GS 13/1 base salary. Maximum GS-15/10 base salary.)

   _X__Appointee will waive compensation (attach written agreement)

7. The record of appointment has been clearly documented to show the services to be performed and the special qualifications of the appointee, which relate specifically to those services.

8. A statement of employment and financial interests will be obtained to determine if any conflict of interest exists (OGE Form 450 will be obtained after onboarding. Components retain OGC comments).

Michael Russo Digitally signed by Michael Russo Date: 2025.02.24 17:44:54 -05'00'

Date — Signature of Component Program Manager Authorized to Obtain the Consultant's/Expert's Services (This certification relates particularly to items 1, 2, 3, 6, 7 and 8)

2/27/25 [redacted]

Date — Signature of DCHR Appointing Official (This certification relates particularly to items 2 through 8)

**ADDENDUM TO THE EXPERT/CONSULTANT APPOINTMENT REQUEST AND CERTIFICATION**

1. During Appointee's term of service to SSA, Appointee voluntarily waives compensation, as described in the Appointment Request and Certification, from SSA.

2. While on duty time at SSA, Appointee shall only perform duties for SSA.

3. While on duty time for SSA or at SSA Headquarters (HQ) Woodlawn, Maryland, Appointee shall not perform any work for or on behalf of any other entity, government or private.

4. Appointee shall perform SSA work only at SSA Headquarters (HQ) in Woodlawn, Maryland.

5. SSA shall provide any necessary equipment or systems access to ensure access to SSA systems consistent with the Appointee's specific duties as described in the Appointment Request and Certification.

6. Appointee shall not perform any non-SSA work using SSA equipment or resources.

7. Appointee shall not perform SSA work non-SSA equipment or resources.

8. Appointee shall not share any Personally Identifiable Information accessed or obtained through the use of SSA systems or work performed for SSA, with any external entity, organization, or agency federal or state.

9. Appointee shall not share or disclose SSA information that is non- PII, non-public information with any non-federal entity. Any disclosure of non- PII, non-public information to another federal entity, organization, or agency shall be made only with expressed permission of the Office of the Commissioner.

10. Appointee shall abide by all SSA regulations and policies regarding access to and protection of any agency records, information, and work products.

11. Appointee shall abide all SSA regulations and policies regarding ethics and employee conduct.

12. In the event of any lapse in appropriations, the Appointee will follow the instructions issued by SSA related to his SSA service.

EXPERT OR CONSULTANT
APPOINTMENT REQUEST & CERTIFICATION
**(Submit with Resume)**

| 1. NAME OF PERSON *(Last, first, middle initial)* | 2. TOTAL PERIOD FOR WHICH APPOINTMENT IS REQUESTED *(entire year (365) days or a shorter period). List dates from beginning to end month/day/year.* 365 days |
|---|---|
| Employee 6 | |
| 3. MAILING ADDRESS [redacted] | 4. APPROXIMATE NUMBER OF DAYS PERSON IS EXPECTED TO PERFORM SERVICES DURING THIS PERIOD. 365 days |

5. SERVICES TO BE PERFORMED

A. EXPLAIN IN FULL DETAIL THE NON-CONTINUOUS/TEMPORARY NATURE OF THE WORK TO BE PERFORMED AND THE NECESSITY FOR THE POSITION TO ACTUALLY REQUIRE AN EXPERT'S OR CONSULTANT'S SERVICES AS OPPOSED TO A REGULAR GOVERNMENT EMPLOYEE, OR IN THE CASE OF A REAPPOINTMENT (WITH SAME DUTIES), THE CONTINUING NEED FOR THE SERVICES OF AN EXPERT OR CONSULTANT (AND HOURS/DAYS WORKED IN PRECEDING YEAR).

SSA is facing significant issues that require immediate attention. Two of the most substantial areas in need of timely attention include: (1) Numident records with death data and (2) Payment data, focused on reducing improper payments.

B. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE TRANSACTION OF BUSINESS ON BEHALF OF THE GOVERNMENT WITH ANY PROFIT OR NON-PROFIT ORGANIZATION.

1. Examine the Ernst & Young recent SSA audit report.

2. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

3. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

4. Review prior audits and studies concerning improvements to SSA's Numident death records and assess the current process used by SSA to obtain death information for SSA's programs and offer recommendations for improvement of the process by which information is obtained;

5. Prepare recommendations related to the duties above and, without using the active production system, provide examples of code improvements;

6. Conduct analysis of SSA payment data to reduce concerns improper payments. This will include analyzing data of SSA current payments to beneficiaries against other SSA records to identify potential improper payments; and

7. Data needed to perform the analysis will be SSA payment files sent to Treasury and potentially the Numident, Master Beneficiary Record (MBR), and Supplemental Security Record (SSR). Security controls will be implemented to prevent detailee from accessing or viewing sensitive data within any of these records.

C. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE RENDERING OF ADVICE TO THE GOVERNMENT WHICH WILL HAVE DIRECT AND PREDICTABLE EFFECT ON THE INTERESTS OF ANY PROFIT OR NON-PROFIT ORGANIZATION.

None

6. SPECIAL QUALIFICATIONS OF THE PERSON RECOMMENDED FOR APPOINTMENT *(List those which relate specifically to the services to be performed.*

*Growth Equity Vice President (Accelerated Promotion from Senior Associate) March 2022 – Present*

- ~$19B AUM investing out of flagship growth Fund VI (~$2.4B), late-stage Opportunity Fund I (~$550M), venture fund VSV II (~$595M), and multiple directly managed co-invest vehicles
- Executed investment thesis creation and underwriting for 11 core growth investments representing $1.1B+ in [redacted] invested capital in industries including artificial intelligence, compute infrastructure, drone systems, and more
- Assisted in onsite operational support projects for multiple portfolio companies at request of senior leadership

CERTIFICATION

In approving the appointment of this consultant/expert, I have considered the requirements of law, relevant decisions of the Comptroller General, and Office of Personnel Management Department policies and instructions. More specifically, I have satisfied myself that:

1. The services of the individual are essential for effective program management

2. The service of the expert or consultant does not duplicate any previously performed work or service, and that the service is not currently available within SSA

3. The duties to be performed are those of (check one)

   ___a consultant (that is, they are purely advisory in nature and will not include the performance or supervision of operating functions)

   X__an expert (that is, they require a high level of expertise not available in the regular work force)

4. The proposed appointee has a high degree of attainment in the field and is qualified to (check one):

   ___provide advisory services as a consultant under 5 CFR 304

   X__serve as an expert under 5 CFR 304

5. The appointment is non-continuous/temporary and necessary, and as such, is designated as (check one):

   X__Intermittent not to exceed 1 year (the individual will work occasionally and irregularly) not to exceed the equivalent of 6 months.

   ___Part-time not to exceed 1 year.

   Provide tour: _____

   ___Full-time not to exceed 1 year

6. The expert and consultant appointing authority is the most appropriate authority to use

7. The pay level is GS grade/step _15/10__ equivalent. This is appropriate for the duties to be performed and the qualifications of the appointee (Minimum GS 13/1 base salary. Maximum GS-15/10 base salary.)

   _X__Appointee will waive compensation (attach written agreement)

8. The record of appointment has been clearly documented to show the services to be performed and the special qualifications of the appointee, which relate specifically to those services.

9. A statement of employment and financial interests will be obtained to determine if any conflict of interest exists (OGE Form 278 will be obtained after onboarding. Components retain OGC comments).

Michael Russo Digitally signed by Michael Russo Date: 2025.02.24 17:43:27 -05'00'

Date

Signature of Component Program Manager Authorized to Obtain the Consultant's/Expert's Services (This certification relates particularly to items 1, 2, 3, 6, 7 and 8)

2/27/25

Date

[redacted]

Signature of DCHR Appointing Official (This certification relates particularly to items 2 through 8)

**ADDENDUM TO THE EXPERT/CONSULTANT APPOINTMENT REQUEST AND CERTIFICATION**

1. During Appointee's term of service to SSA, Appointee voluntarily waives compensation, as described in the Appointment Request and Certification, from SSA.

2. While on duty time at SSA, Appointee shall only perform duties for SSA.

3. While on duty time for SSA or at SSA Headquarters (HQ) Woodlawn, Maryland, Appointee shall not perform any work for or on behalf of any other entity, government or private.

4. Appointee shall perform SSA work only at SSA Headquarters (HQ) in Woodlawn, Maryland.

5. SSA shall provide any necessary equipment or systems access to ensure access to SSA systems consistent with the Appointee's specific duties as described in the Appointment Request and Certification.

6. Appointee shall not perform any non-SSA work using SSA equipment or resources.

7. Appointee shall not perform SSA work non-SSA equipment or resources.

8. Appointee shall not share any Personally Identifiable Information accessed or obtained through the use of SSA systems or work performed for SSA, with any external entity, organization, or agency federal or state.

9. Appointee shall not share or disclose SSA information that is non- PII, non-public information with any non-federal entity. Any disclosure of non- PII, non-public information to another federal entity, organization, or agency shall be made only with expressed permission of the Office of the Commissioner.

10. Appointee shall abide by all SSA regulations and policies regarding access to and protection of any agency records, information, and work products.

11. Appointee shall abide all SSA regulations and policies regarding ethics and employee conduct.

12. In the event of any lapse in appropriations, the Appointee will follow the instructions issued by SSA related to his SSA service.

EXPERT OR CONSULTANT
APPOINTMENT REQUEST & CERTIFICATION
**(Submit with Resume)**

| | |
|---|---|
| 1. NAME OF PERSON *(Last, first, middle initial)* Employee 11 | 2. TOTAL PERIOD FOR WHICH APPOINTMENT IS REQUESTED *(entire year (365) days or a shorter period). List dates from beginning to end month/day/year.* 365 days |
| 3. MAILING ADDRESS | 4. APPROXIMATE NUMBER OF DAYS PERSON IS EXPECTED TO PERFORM SERVICES DURING THIS PERIOD. 365 days |

5. SERVICES TO BE PERFORMED

A. EXPLAIN IN FULL DETAIL THE NON-CONTINUOUS/TEMPORARY NATURE OF THE WORK TO BE PERFORMED AND THE NECESSITY FOR THE POSITION TO ACTUALLY REQUIRE AN EXPERT'S OR CONSULTANT'S SERVICES AS OPPOSED TO A REGULAR GOVERNMENT EMPLOYEE, OR IN THE CASE OF A REAPPOINTMENT (WITH SAME DUTIES), THE CONTINUING NEED FOR THE SERVICES OF AN EXPERT OR CONSULTANT (AND HOURS/DAYS WORKED IN PRECEDING YEAR).

SSA is facing significant issues that require immediate attention. Two of the most substantial areas in need of timely attention include: (1) Numident records with death data and (2) Payment data, focused on reducing improper payments.

B. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE TRANSACTION OF BUSINESS ON BEHALF OF THE GOVERNMENT WITH ANY PROFIT OR NON-PROFIT ORGANIZATION.

1. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

2. Review prior audits and studies concerning improvements to SSA's Numident death records and assess the current process used by SSA to obtain death information for SSA's programs and offer recommendations for improvement of the process by which information is obtained;

3. Prepare recommendations related to the duties above and, without using the active production system, provide examples of code improvements;

4. Conduct analysis of SSA payment data to reduce concerns with improper payments. This will include analyzing data of SSA current payments to beneficiaries against other SSA records to identify potential improper payments; and

5. Data needed to perform the analysis will be SSA payment files sent to Treasury and potentially the Numident, Master Beneficiary Record (MBR), and Supplemental Security Record (SSR). Security controls will be implemented to prevent detailee from accessing or viewing sensitive data within any of these records.

In Performance of His Work, Expert Shall:

1. Report to and be supervised by the Commissioner of the Social Security Administration or his or her designee when performing SSA work. In all circumstances, Expert will comply with all instructions, rules, regulations, and restrictions of the supervising agency.

2. Not knowingly take any actions that undermine SSA's responsibilities under governing statutes, regulations, or directives, including but not limited to FISMA, FITARA, the Privacy Act, the Federal Acquisition Regulation, and the Trade Secrets Act.
3. Not knowingly take any measures that create cybersecurity risks to SSA systems.
4. Not knowingly access SSA systems in a manner that fails to comply with all relevant federal, security, ethics, and confidentiality laws, regulations, and policies, including SSA records management and information security requirements.
5. Not access, or attempt to access, classified information without proper security clearance.
6. Access SSA data, information, and systems for only legitimate purposes, including but not limited to IT modernization, the facilitation of SSA operations, and the improvement of Government efficiency.
7. Comply with the requirements of the Privacy Act for information that SSA collects on individuals, including, if necessary, publishing or amending Systems of Records Notices to adequately account for the information it collects.
8. With permission of the assigned SSA supervisor, securely destroy or erase copied SSA data or information when no longer needed for official SSA purposes. Prior to access, disclosure, and other handling of any personally identifiable information in SSA records, ensure permission from the assigned SSA supervisor for such action, to ensure authority exists for access, disclosure, or handling.
9. To the greatest extent possible, use the program agency system documentation to understand how to use the data and information which is being accessed.
10. Remains subject to the Standards for Ethical Conduct for Employees of the Executive Branch as noted by 5 C.F.R. Part 2635.
11. Is bound by any other laws and regulations applicable to Federal employees including, but not limited to, representations as attorney or agent for any person (18 U.S.C. Sections 203 and 205); political activity (Hatch Act, 5 U.S.C. Sections 7321-7326); financial conflicts of interest (18 U.S.C. Section 208); post- employment restrictions (18 U.S.C. Section 207); and salary supplementation prohibitions (18 U.S.C. Section 209);

C. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE RENDERING OF ADVICE TO THE GOVERNMENT WHICH WILL HAVE DIRECT AND PREDICTABLE EFFECT ON THE INTERESTS OF ANY PROFIT OR NON-PROFIT ORGANIZATION.

None

6. SPECIAL QUALIFICATIONS OF THE PERSON RECOMMENDED FOR APPOINTMENT *(List those which relate specifically to the services to be performed.*

Employee 11 is a Senior Software Engineer with over ten years of experience building cloud-native geospatial solutions. Adept at architecting geospatial infrastructures, implementing geospatial algorithms, and leading full-stack development. Experienced in collaborating with cross-functional teams to deliver mission-critical capabilities and driving technical decisions and best practices.

CERTIFICATION

In approving the appointment of this consultant/expert, I have considered the requirements of law, relevant decisions of the Comptroller General, and Office of Personnel Management Department policies and instructions. More specifically, I have satisfied myself that:

1. The services of the individual are essential for effective program management

2. The service of the expert or consultant does not duplicate any previously performed work or service, and that the service is not currently available within SSA

3. The duties to be performed are those of (check one)

   ___a consultant (that is, they are purely advisory in nature and will not include the performance or supervision of operating functions)

   X expert (that is, they require a high level of expertise not available in the regular work force)

4. The proposed appointee has a high degree of attainment in the field and is qualified to (check one):

   ___provide advisory services as a consultant under 5 CFR 304

   X___serve as an expert under 5 CFR 304

5. The appointment is non-continuous/temporary and necessary, and as such, is designated as (check one):

   ___Intermittent not to exceed 1 year (the individual will work occasionally and irregularly) not to exceed the equivalent of 6 months.

   ___Part-time not to exceed 1 year.

   Provide tour: _____

   _X__Full-time not to exceed 1 year

6. The expert and consultant appointing authority is the most appropriate authority to use

7. The pay level is GS grade/step _15/10_____ equivalent. This is appropriate for the duties to be performed and the qualifications of the appointee (Minimum GS 13/1 base salary. Maximum GS-15/10 base salary.)

   ___Appointee will waive compensation (attach written agreement)

8. The record of appointment has been clearly documented to show the services to be performed and the special qualifications of the appointee, which relate specifically to those services.

9. A statement of employment and financial interests will be obtained to determine if any conflict of interest exists (OGE Form 450 will be obtained after onboarding. Components retain OGC comments).

3/14/25 — Date

Michael L. Russo — Signature of Co ponent Program Manager Authorized to Obtain the Consultant's/Ex ert's Services This certification relates particularly to items 1, 2, 3, 6, 7 and 8)

3/17/25 — Date

Florence Felix-Lawson — Signature f DCHR Appointing Official (This certification relates particularly to items 2 through 8)

EXPERT OR CONSULTANT
APPOINTMENT REQUEST & CERTIFICATION
**(Submit with Resume)**

| 1. NAME OF PERSON *(Last, first, middle initial)* | 2. TOTAL PERIOD FOR WHICH APPOINTMENT IS REQUESTED *(entire year (365) days or a shorter period). List dates from beginning to end month/day/year.* 365 days |
|---|---|
| Employee 9 | |
| 3. MAILING ADDRESS [redacted] | 4. APPROXIMATE NUMBER OF DAYS PERSON IS EXPECTED TO PERFORM SERVICES DURING THIS PERIOD. 365 days |

5. SERVICES TO BE PERFORMED

A. EXPLAIN IN FULL DETAIL THE NON-CONTINUOUS/TEMPORARY NATURE OF THE WORK TO BE PERFORMED AND THE NECESSITY FOR THE POSITION TO ACTUALLY REQUIRE AN EXPERT'S OR CONSULTANT'S SERVICES AS OPPOSED TO A REGULAR GOVERNMENT EMPLOYEE, OR IN THE CASE OF A REAPPOINTMENT (WITH SAME DUTIES), THE CONTINUING NEED FOR THE SERVICES OF AN EXPERT OR CONSULTANT (AND HOURS/DAYS WORKED IN PRECEDING YEAR).

SSA is facing significant issues that require immediate attention. Two of the most substantial areas in need of timely attention include: (1) Numident records with death data and (2) Payment data, focused on reducing improper payments.

B. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE TRANSACTION OF BUSINESS ON BEHALF OF THE GOVERNMENT WITH ANY PROFIT OR NON-PROFIT ORGANIZATION.

1. Examine the recent Ernst & Young audit of SSA.

2. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

3. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

4. Review prior audits and studies concerning improvements to SSA's Numident death records and assess the current process used by SSA to obtain death information for SSA's programs and offer recommendations for improvement of the process by which information is obtained;

5. Prepare recommendations related to the duties above and, without using the active production system, provide examples of code improvements;

6. Conduct analysis of SSA payment data to reduce concerns improper payments. This will include analyzing data of SSA current payments to beneficiaries against other SSA records to identify potential improper payments; and

7. Data needed to perform the analysis will be SSA payment files sent to Treasury and potentially the Numident, Master Beneficiary Record (MBR), and Supplemental Security Record (SSR). Security controls will be implemented to prevent detailee from accessing or viewing sensitive data within any of these records.

C. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE RENDERING OF ADVICE TO THE GOVERNMENT WHICH WILL HAVE DIRECT AND PREDICTABLE EFFECT ON THE INTERESTS OF ANY PROFIT OR NON-PROFIT ORGANIZATION.

None

6. SPECIAL QUALIFICATIONS OF THE PERSON RECOMMENDED FOR APPOINTMENT *(List those which relate specifically to the services to be performed.*

*Senior Associate, Data Engineer*
Developed a Call Center Scheduling Tool for a [redacted] company using a Genetic Algorithm, reducing [redacted] wait times by over 95%.
Built a lightweight Manufacturing Execution System (MES) to track inventory and manage home battery deployments for [redacted].
Designed and implemented a data pipeline, analytics database, and Looker dashboard for a [redacted] production facility using Airflow, DBT, and LookML.
Developed a time series forecasting model using Meta Prophet to predict bookings for a [redacted] company.
Created an Accounts Payable automation tool in Google Cloud Run for an AI company, streamlining invoice processing

CERTIFICATION

In approving the appointment of this consultant/expert, I have considered the requirements of law, relevant decisions of the Comptroller General, and Office of Personnel Management Department policies and instructions. More specifically, I have satisfied myself that:

1. The services of the individual are essential for effective program management

2. The service of the expert or consultant does not duplicate any previously performed work or service, and that the service is not currently available within SSA

3. The duties to be performed are those of (check one)

   ___a consultant (that is, they are purely advisory in nature and will not include the performance or supervision of operating functions)

   X__an expert (that is, they require a high level of expertise not available in the regular work force)

4. The proposed appointee has a high degree of attainment in the field and is qualified to (check one):

   ___provide advisory services as a consultant under 5 CFR 304

   X__serve as an expert under 5 CFR 304

5. The appointment is non-continuous/temporary and necessary, and as such, is designated as (check one):

   X__Intermittent not to exceed 1 year (the individual will work occasionally and irregularly) not to exceed the equivalent of 6 months.

   ___Part-time not to exceed 1 year.

   Provide tour: _____

   ___Full-time not to exceed 1 year

6. The expert and consultant appointing authority is the most appropriate authority to use

7. The pay level is GS grade/step __15/10_____ equivalent. This is appropriate for the duties to be performed and the qualifications of the appointee (Minimum GS 13/1 base salary. Maximum GS-15/10 base salary.)

   _X__Appointee will waive compensation (attach written agreement)

8. The record of appointment has been clearly documented to show the services to be performed and the special qualifications of the appointee, which relate specifically to those services.

9. A statement of employment and financial interests will be obtained to determine if any conflict of interest exists (OGE Form 278 will be obtained after onboarding. Components retain OGC comments).

Michael Russo Digitally signed by Michael Russo Date: 2025.02.24 17:45:40 -05'00'

Date

Signature of Component Program Manager Authorized to Obtain the Consultant's/Expert's Services (This certification relates particularly to items 1, 2, 3, 6, 7 and 8)

2/27/25

Date

[redacted]

Signature of DCHR Appointing Official (This certification relates particularly to items 2 through 8)

# ADDENDUM TO THE EXPERT/CONSULTANT APPOINTMENT REQUEST AND CERTIFICATION

1. During Appointee's term of service to SSA, Appointee voluntarily waives compensation, as described in the Appointment Request and Certification, from SSA.

2. While on duty time at SSA, Appointee shall only perform duties for SSA.

3. While on duty time for SSA or at SSA Headquarters (HQ) Woodlawn, Maryland, Appointee shall not perform any work for or on behalf of any other entity, government or private.

4. Appointee shall perform SSA work only at SSA Headquarters (HQ) in Woodlawn, Maryland.

5. SSA shall provide any necessary equipment or systems access to ensure access to SSA systems consistent with the Appointee's specific duties as described in the Appointment Request and Certification.

6. Appointee shall not perform any non-SSA work using SSA equipment or resources.

7. Appointee shall not perform SSA work non-SSA equipment or resources.

8. Appointee shall not share any Personally Identifiable Information accessed or obtained through the use of SSA systems or work performed for SSA, with any external entity, organization, or agency federal or state.

9. Appointee shall not share or disclose SSA information that is non- PII, non-public information with any non-federal entity. Any disclosure of non- PII, non-public information to another federal entity, organization, or agency shall be made only with expressed permission of the Office of the Commissioner.

10. Appointee shall abide by all SSA regulations and policies regarding access to and protection of any agency records, information, and work products.

11. Appointee shall abide all SSA regulations and policies regarding ethics and employee conduct.

12. In the event of any lapse in appropriations, the Appointee will follow the instructions issued by SSA related to his SSA service.

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296–33, Subch. 4

# NOTIFICATION OF PERSONNEL ACTION

| 1. Name (Last, First, Middle) | 2. Social Security Number | 3. Date of Birth | 4. Effective Date |
|---|---|---|---|
| Employee 11 | [redacted] | [redacted] | 03/16/2025 |

## FIRST ACTION

| 5–A. Code | 5–B. Nature of Action |
|---|---|
| 171 | EXC APPT NTE 03-15-26 |
| **5–C. Code** | **5–D. Legal Authority** |
| H2L | REG 304.103 |
| **5–E. Code** | **5–F. Legal Authority** |
| | |

## SECOND ACTION

| 6–A. Code | 6–B. Nature of Action |
|---|---|
| | |
| **6–C. Code** | **6–D. Legal Authority** |
| | |
| **6–E. Code** | **6–F. Legal Authority** |
| | |

**7. FROM: Position Title and Number**

**15. TO: Position Title and Number**
EXPERT
EXPERT
S4C KNX0390

| 8. Pay Plan | 9. Occ. Code | 10. Grade or Level | 11. Step or Rate | 12. Total Salary | 13. Pay Basis |
|---|---|---|---|---|---|
| | | | | | |

| 16. Pay Plan | 17. Occ. Code | 18. Grade or Level | 19. Step or Rate | 20. Total Salary/Award | 21. Pay Basis |
|---|---|---|---|---|---|
| ED | 0301 | 00 | 00 | $162672.00 | PA |

| 12A. Basic Pay | 12B. Locality Adj. | 12C. Adj. Basic Pay | 12D. Other Pay |
|---|---|---|---|
| | | | |

| 20A. Basic Pay | 20B. Locality Adj. | 20C. Adj. Basic Pay | 20D. Other Pay |
|---|---|---|---|
| $162672.00 | $0.00 | $162672.00 | $0.00 |

**14. Name and Location of Position's Organization**

**22. Name and Location of Position's Organization**
SZ00 SOCIAL SECURITY ADMINISTRATION
CHIEF INFORMATION OFFICER
OFFICE OF CHIEF INFORMATION OFFICER

## EMPLOYEE DATA

**23. Veterans Preference**
1 (1 – None; 2 – 5–Point; 3 – 10–Point/Disability; 4 – 10–Point/Compensable; 5 – 10–Point/Other; 6 – 10–Point/Compensable/30%)

**24. Tenure**
0 (0 – None; 1 – Permanent; 2 – Conditional; 3 – Indefinite)

**25. Agency Use**

**26. Veterans Preference for RIF**
[ ] YES [X] NO

**27. FEGLI**
A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERAG

**28. Annuitant Indicator**
9 NOT APPLICABLE

**29. Pay Rate Determinant**
0

**30. Retirement Plan**
2 FICA

**31. Service Comp. Date (Leave)**
03/16/2025

**32. Work Schedule**
F FULL-TIME

**33. Part–Time Hours Per Biweekly Pay Period**

## POSITION DATA

**34. Position Occupied**
2 (1 – Competitive Service; 2 – Excepted Service; 3 – SES General; 4 – SES Career Reserved)

**35. FLSA Category**
E (E – Exempt; N – Nonexempt)

**36. Appropriation Code**
4003431

**37. Bargaining Unit Status**
8888

**38. Duty Station Code**
24-1698-005

**39. Duty Station (City – County – State or Overseas Location)**
WOODLAWN,BALTIMORE,MARYLAND

| 40. Agency Data | 41. | 42. | 43. | 44. |
|---|---|---|---|---|
| FUNC CLS 00 | VET STAT X | EDUC LVL 17 | SUPV STAT 8 | POSITION SENSITIVITY CRITICAL-SENSITIVE |

**45. Remarks**

APPOINTMENT AFFIDAVIT EXECUTED 03-17-25.
PREVIOUS RETIREMENT COVERAGE: NEVER COVERED
REASON FOR TEMPORARY APPOINTMENT EVALUATE THE DEATH INFORMATION AVAILABLE
AND OFFER RECOMMENDATIONS FOR IMPROVEMENTS; REVIEW PRIOR AUDITS AND
STUDIES CONCERNING DEATH RECORDS AND ASSESS THE CURRENT PROCESS
USED TO OBTAIN DEATH INFORMATION AND OFFER RECOMMENDATIONS FOR
IMPROVEMENT WITHOUT USING THE ACTIVE PRODUCTION SYSTEM; CONDUCT
ANALYSIS OF SSA PAYMENT DATA TO REDUCE CONCERNS WITH IMPROPER
PAYMENTS
YOU ARE SUBJECT TO REGULATIONS GOVERNING CONDUCT AND RESPONSIBILITIES OF SPECIAL GOVERNMENT EMPLOYEES.

**46. Employing Department or Agency**
SZ - SOCIAL SECURITY ADMIN

| 47. Agency Code | 48. Personnel Office ID | 49. Approval Date |
|---|---|---|
| SZ00 | 1166 | 03/16/2025 |

**50. Signature/Authentication and Title of Approving Official**
250997871 / ELECTRONICALLY SIGNED BY:
[redacted]
DIRECTOR, OESS

5–Part 50–316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY



Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540–01–333–6238

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296–33, Subch. 4

# NOTIFICATION OF PERSONNEL ACTION

| 1. Name (Last, First, Middle) | 2. Social Security Number | 3. Date of Birth | 4. Effective Date |
|---|---|---|---|
| Employee 4 | [redacted] | [redacted] | 02/23/2025 |

## FIRST ACTION

| 5–A. Code | 5–B. Nature of Action | 6–A. Code | 6–B. Nature of Action |
|---|---|---|---|
| 002 | CORRECTION | 171 | EXC APPT NTE 02-22-26 |
| 5–C. Code | 5–D. Legal Authority | 6–C. Code | 6–D. Legal Authority |
| | | H2L | REG 304.103 |
| 5–E. Code | 5–F. Legal Authority | 6–E. Code | 6–F. Legal Authority |
| | | | |

| 7. FROM: Position Title and Number | 15. TO: Position Title and Number |
|---|---|
| | EXPERT<br>EXPERT<br>S4C KNX0370 |

| 8. Pay Plan | 9. Occ. Code | 10. Grade or Level | 11. Step or Rate | 12. Total Salary | 13. Pay Basis | 16. Pay Plan | 17. Occ. Code | 18. Grade or Level | 19. Step or Rate | 20. Total Salary/Award | 21. Pay Basis |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | ED | 0301 | 00 | 00 | $0.00 | WC |

| 12A. Basic Pay | 12B. Locality Adj. | 12C. Adj. Basic Pay | 12D. Other Pay | 20A. Basic Pay | 20B. Locality Adj. | 20C. Adj. Basic Pay | 20D. Other Pay |
|---|---|---|---|---|---|---|---|
| | | | | $0.00 | $0.00 | $0.00 | $0.00 |

| 14. Name and Location of Position's Organization | 22. Name and Location of Position's Organization |
|---|---|
| | SZ00 SOCIAL SECURITY ADMINISTRATION<br>CHIEF INFORMATION OFFICER<br>OFFICE OF CHIEF INFORMATION OFFICER |

## EMPLOYEE DATA

| 23. Veterans Preference | 24. Tenure | 25. Agency Use | 26. Veterans Preference for RIF |
|---|---|---|---|
| 1 (1 – None, 2 – 5–Point, 3 – 10–Point/Disability, 4 – 10–Point/Compensable, 5 – 10–Point/Other, 6 – 10–Point/Compensable/30%) | 0 (0 – None, 1 – Permanent, 2 – Conditional, 3 – Indefinite) | | YES [ ] X NO |

| 27. FEGLI | 28. Annuitant Indicator | 29. Pay Rate Determinant |
|---|---|---|
| A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERA | 9 NOT APPLICABLE | 0 |

| 30. Retirement Plan | 31. Service Comp. Date (Leave) | 32. Work Schedule | 33. Part–Time Hours Per Biweekly Pay Period |
|---|---|---|---|
| 2 FICA | 02/23/2025 | I INTERMITTENT | |

## POSITION DATA

| 34. Position Occupied | 35. FLSA Category | 36. Appropriation Code | 37. Bargaining Unit Status |
|---|---|---|---|
| 2 (1 – Competitive Service, 2 – Excepted Service, 3 – SES General, 4 – SES Career Reserved) | E (E – Exempt, N – Nonexempt) | 4003431 | 8888 |

| 38. Duty Station Code | 39. Duty Station (City – County – State or Overseas Location) |
|---|---|
| 24-1698-005 | WOODLAWN,BALTIMORE,MARYLAND |

| 40. Agency Data | 41. | 42. | 43. | 44. |
|---|---|---|---|---|
| FUNC CLS 00 | VET STAT X | EDUC LVL | SUPV STAT 8 | POSITION SENSITIVITY CRITICAL-SENSITIVE |

45. Remarks
CORRECTS ITEM 1 TO READ: Employee 4

| 46. Employing Department or Agency | 50. Signature/Authentication and Title of Approving Official |
|---|---|
| SZ - SOCIAL SECURITY ADMIN | 250928535 / ELECTRONICALLY SIGNED BY: [redacted]<br>DIRECTOR, OESS |

| 47. Agency Code | 48. Personnel Office ID | 49. Approval Date |
|---|---|---|
| SZ00 | 1166 | 03/13/2025 |

5–Part 50–316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Previous Edition Not Usable After 6/30/93
NSN 7540–01–333–6238

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296–33, Subch. 4

# NOTIFICATION OF PERSONNEL ACTION

| 1. Name (Last, First, Middle) | 2. Social Security Number | 3. Date of Birth | 4. Effective Date |
|---|---|---|---|
| Employee 1 | [redacted] | [redacted] | 02/09/2025 |

## FIRST ACTION

| 5–A. Code | 5–B. Nature of Action |
|---|---|
| 171 | EXC APPT NTE 02-08-26 |
| **5–C. Code** | **5–D. Legal Authority** |
| ZLM | 5 U.S.C. 3109 |
| **5–E. Code** | **5–F. Legal Authority** |
| | |

## SECOND ACTION

| 6–A. Code | 6–B. Nature of Action |
|---|---|
| | |
| **6–C. Code** | **6–D. Legal Authority** |
| | |
| **6–E. Code** | **6–F. Legal Authority** |
| | |

| 7. FROM: Position Title and Number |
|---|
| |

| 8. Pay Plan | 9. Occ. Code | 10. Grade or Level | 11. Step or Rate | 12. Total Salary | 13. Pay Basis |
|---|---|---|---|---|---|
| | | | | | |

| 12A. Basic Pay | 12B. Locality Adj. | 12C. Adj. Basic Pay | 12D. Other Pay |
|---|---|---|---|
| | | | |

| 14. Name and Location of Position's Organization |
|---|
| |

| 15. TO: Position Title and Number |
|---|
| EXPERT<br>EXPERT<br>S4C KNX0350 |

| 16. Pay Plan | 17. Occ. Code | 18. Grade or Level | 19. Step or Rate | 20. Total Salary/Award | 21. Pay Basis |
|---|---|---|---|---|---|
| ED | 0301 | 00 | 00 | $90025.00 | PA |

| 20A. Basic Pay | 20B. Locality Adj. | 20C. Adj. Basic Pay | 20D. Other Pay |
|---|---|---|---|
| $90025.00 | $0.00 | $90025.00 | $0.00 |

| 22. Name and Location of Position's Organization |
|---|
| SZ00 SOCIAL SECURITY ADMINISTRATION<br>CHIEF INFORMATION OFFICER<br>OFFICE OF CHIEF INFORMATION OFFICER |

## EMPLOYEE DATA

| 23. Veterans Preference | 24. Tenure | 25. Agency Use | 26. Veterans Preference for RIF |
|---|---|---|---|
| 1 (1 – None, 2 – 5–Point, 3 – 10–Point/Disability, 4 – 10–Point/Compensable, 5 – 10–Point/Other, 6 – 10–Point/Compensable/30%) | 0 (0 – None, 1 – Permanent, 2 – Conditional, 3 – Indefinite) | | YES: X NO: |

| 27. FEGLI | 28. Annuitant Indicator | 29. Pay Rate Determinant |
|---|---|---|
| A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERA | 9 NOT APPLICABLE | 0 |

| 30. Retirement Plan | 31. Service Comp. Date (Leave) | 32. Work Schedule | 33. Part–Time Hours Per Biweekly Pay Period |
|---|---|---|---|
| 2 FICA | 02/09/2025 | F FULL-TIME | |

## POSITION DATA

| 34. Position Occupied | 35. FLSA Category | 36. Appropriation Code | 37. Bargaining Unit Status |
|---|---|---|---|
| 2 (1 – Competitive Service, 2 – Excepted Service, 3 – SES General, 4 – SES Career Reserved) | N (E – Exempt, N – Nonexempt) | 4003431 | 8888 |

| 38. Duty Station Code | 39. Duty Station (City – County – State or Overseas Location) |
|---|---|
| 24-1698-005 | WOODLAWN,BALTIMORE,MARYLAND |

| 40. Agency Data | 41. | 42. | 43. | 44. |
|---|---|---|---|---|
| FUNC CLS 00 | VET STAT X | EDUC LVL | SUPV STAT 8 | POSITION SENSITIVITY CRITICAL-SENSITIVE |

**45. Remarks**

APPOINTMENT AFFIDAVIT EXECUTED 02/10/25.
PREVIOUS RETIREMENT COVERAGE: NEVER COVERED
REASON FOR TEMPORARY APPOINTMENT TO PERFORM ANALYSIS OF SSA PAYMENT DATA TO
REDUCE CONCERNS RAISED BY THE ADMINISTRATION.
CREDITABLE MILITARY SERVICE: NONE
YOU ARE SUBJECT TO REGULATIONS GOVERNING CONDUCT AND RESPONSIBILITIES OF SPECIAL GOVERNMENT EMPLOYEES.

| 46. Employing Department or Agency | 50. Signature/Authentication and Title of Approving Official |
|---|---|
| SZ - SOCIAL SECURITY ADMIN | 250644169 / ELECTRONICALLY SIGNED BY: |
| | [redacted] |
| | DIRECTOR, OESS |

| 47. Agency Code | 48. Personnel Office ID | 49. Approval Date |
|---|---|---|
| SZ00 | 1166 | 02/09/2025 |

5–Part 50–316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540–01–333–6238

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296–33, Subch. 4

# NOTIFICATION OF PERSONNEL ACTION

| 1. Name (Last, First, Middle) | 2. Social Security Number | 3. Date of Birth | 4. Effective Date |
|---|---|---|---|
| Employee 4 | [redacted] | [redacted] | 02/23/2025 |

## FIRST ACTION

| 5–A. Code | 5–B. Nature of Action | 6–A. Code | 6–B. Nature of Action |
|---|---|---|---|
| 171 | EXC APPT NTE 02-22-26 | | |
| **5–C. Code** | **5–D. Legal Authority** | **6–C. Code** | **6–D. Legal Authority** |
| H2L | REG 304.103 | | |
| **5–E. Code** | **5–F. Legal Authority** | **6–E. Code** | **6–F. Legal Authority** |
| | | | |

## SECOND ACTION

| 7. FROM: Position Title and Number | 15. TO: Position Title and Number |
|---|---|
| | EXPERT<br>EXPERT<br>S4C KNX0370 |

| 8. Pay Plan | 9. Occ. Code | 10. Grade or Level | 11. Step or Rate | 12. Total Salary | 13. Pay Basis |
|---|---|---|---|---|---|
| | | | | | |

| 16. Pay Plan | 17. Occ. Code | 18. Grade or Level | 19. Step or Rate | 20. Total Salary/Award | 21. Pay Basis |
|---|---|---|---|---|---|
| ED | 0301 | 00 | 00 | $0.00 | WC |

| 12A. Basic Pay | 12B. Locality Adj. | 12C. Adj. Basic Pay | 12D. Other Pay |
|---|---|---|---|
| | | | |

| 20A. Basic Pay | 20B. Locality Adj. | 20C. Adj. Basic Pay | 20D. Other Pay |
|---|---|---|---|
| $0.00 | $0.00 | $0.00 | $0.00 |

| 14. Name and Location of Position's Organization | 22. Name and Location of Position's Organization |
|---|---|
| | SZ00 SOCIAL SECURITY ADMINISTRATION<br>CHIEF INFORMATION OFFICER<br>OFFICE OF CHIEF INFORMATION OFFICER |

## EMPLOYEE DATA

| 23. Veterans Preference | 24. Tenure | 25. Agency Use | 26. Veterans Preference for RIF |
|---|---|---|---|
| 1 (1 – None; 2 – 5–Point; 3 – 10–Point/Disability; 4 – 10–Point/Compensable; 5 – 10–Point/Other; 6 – 10–Point/Compensable/30%) | 0 (0 – None; 1 – Permanent; 2 – Conditional; 3 – Indefinite) | | YES: ; NO: X |

| 27. FEGLI | 28. Annuitant Indicator | 29. Pay Rate Determinant |
|---|---|---|
| A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERAG | 9 NOT APPLICABLE | 0 |

| 30. Retirement Plan | 31. Service Comp. Date (Leave) | 32. Work Schedule | 33. Part–Time Hours Per Biweekly Pay Period |
|---|---|---|---|
| 2 FICA | 02/23/2025 | I INTERMITTENT | |

## POSITION DATA

| 34. Position Occupied | 35. FLSA Category | 36. Appropriation Code | 37. Bargaining Unit Status |
|---|---|---|---|
| 2 (1 – Competitive Service; 2 – Excepted Service; 3 – SES General; 4 – SES Career Reserved) | E (E – Exempt; N – Nonexempt) | 4003431 | 8888 |

| 38. Duty Station Code | 39. Duty Station (City – County – State or Overseas Location) |
|---|---|
| 24-1698-005 | WOODLAWN,BALTIMORE,MARYLAND |

| 40. Agency Data | 41. | 42. | 43. | 44. |
|---|---|---|---|---|
| FUNC CLS 00 | VET STAT X | EDUC LVL | SUPV STAT 8 | POSITION SENSITIVITY CRITICAL-SENSITIVE |

45. Remarks

APPOINTMENT AFFIDAVIT EXECUTED 02-24-25.
PREVIOUS RETIREMENT COVERAGE: NEVER COVERED
REASON FOR TEMPORARY APPOINTMENT REVIEW PRIOR AUDITS AND STUDIES CONCERNING
IMPROVEMENTS TO SSA'S NUMIDENT DEATH RECORDS AND ASSESS THE CURRENT
PROCESS USED BY SSA TO OBTAIN DEATH INFORMATION FOR SSA'S PROGRAMS
AND OFFER RECOMMENDATIONS FOR IMPROVEMENT.
CONDUCT ANALYSIS OF SSA PAYMENT DATA TO REDUCE CONCERNS IMPROPER
PAYMENTS
YOU ARE SUBJECT TO REGULATIONS GOVERNING CONDUCT AND RESPONSIBILITIES OF SPECIAL GOVERNMENT EMPLOYEES.

| 46. Employing Department or Agency | 50. Signature/Authentication and Title of Approving Official |
|---|---|
| SZ - SOCIAL SECURITY ADMIN | 250727437 / ELECTRONICALLY SIGNED BY: |

| 47. Agency Code | 48. Personnel Office ID | 49. Approval Date | |
|---|---|---|---|
| SZ00 | 1166 | 02/23/2025 | [redacted]<br>DIRECTOR, OESS |

5–Part 50–316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540–01–333–6238

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296–33, Subch. 4

# NOTIFICATION OF PERSONNEL ACTION

| 1. Name (Last, First, Middle) | 2. Social Security Number | 3. Date of Birth | 4. Effective Date |
|---|---|---|---|
| Employee 6 | [redacted] | [redacted] | 02/23/2025 |

## FIRST ACTION

| 5–A. Code | 5–B. Nature of Action |
|---|---|
| 171 | EXC APPT NTE 02-22-26 |
| **5–C. Code** | **5–D. Legal Authority** |
| H2L | REG 304.103 |
| **5–E. Code** | **5–F. Legal Authority** |
| | |

## SECOND ACTION

| 6–A. Code | 6–B. Nature of Action |
|---|---|
| | |
| **6–C. Code** | **6–D. Legal Authority** |
| | |
| **6–E. Code** | **6–F. Legal Authority** |
| | |

| 7. FROM: Position Title and Number | 8. Pay Plan | 9. Occ. Code | 10. Grade or Level | 11. Step or Rate | 12. Total Salary | 13. Pay Basis | 12A. Basic Pay | 12B. Locality Adj. | 12C. Adj. Basic Pay | 12D. Other Pay |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

| 15. TO: Position Title and Number | 16. Pay Plan | 17. Occ. Code | 18. Grade or Level | 19. Step or Rate | 20. Total Salary/Award | 21. Pay Basis | 20A. Basic Pay | 20B. Locality Adj. | 20C. Adj. Basic Pay | 20D. Other Pay |
|---|---|---|---|---|---|---|---|---|---|---|
| EXPERT<br>EXPERT<br>S4C KNX0360 | ED | 0301 | 00 | 00 | $0.00 | WC | $0.00 | $0.00 | $0.00 | $0.00 |

| 14. Name and Location of Position's Organization | 22. Name and Location of Position's Organization |
|---|---|
| | SZ00 SOCIAL SECURITY ADMINISTRATION<br>CHIEF INFORMATION OFFICER<br>OFFICE OF CHIEF INFORMATION OFFICER |

## EMPLOYEE DATA

| 23. Veterans Preference | 24. Tenure | 25. Agency Use | 26. Veterans Preference for RIF |
|---|---|---|---|
| 1 (1 – None, 2 – 5–Point, 3 – 10–Point/Disability, 4 – 10–Point/Compensable, 5 – 10–Point/Other, 6 – 10–Point/Compensable/30%) | 0 (0 – None, 1 – Permanent, 2 – Conditional, 3 – Indefinite) | | YES: X NO: |

| 27. FEGLI | 28. Annuitant Indicator | 29. Pay Rate Determinant |
|---|---|---|
| A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERA( | 9 NOT APPLICABLE | 0 |

| 30. Retirement Plan | 31. Service Comp. Date (Leave) | 32. Work Schedule | 33. Part–Time Hours Per Biweekly Pay Period |
|---|---|---|---|
| 2 FICA | 02/23/2025 | I INTERMITTENT | |

## POSITION DATA

| 34. Position Occupied | 35. FLSA Category | 36. Appropriation Code | 37. Bargaining Unit Status |
|---|---|---|---|
| 2 (1 – Competitive Service, 2 – Excepted Service, 3 – SES General, 4 – SES Career Reserved) | E (E – Exempt, N – Nonexempt) | 4003431 | 8888 |

| 38. Duty Station Code | 39. Duty Station (City – County – State or Overseas Location) |
|---|---|
| 24-1698-005 | WOODLAWN,BALTIMORE,MARYLAND |

| 40. Agency Data | 41. | 42. | 43. | 44. |
|---|---|---|---|---|
| FUNC CLS 00 | VET STAT X | EDUC LVL 13 | SUPV STAT 8 | POSITION SENSITIVITY CRITICAL-SENSITIVE |

**45. Remarks**

APPOINTMENT AFFIDAVIT EXECUTED 02-24-25.
PREVIOUS RETIREMENT COVERAGE: NEVER COVERED
REASON FOR TEMPORARY APPOINTMENT REVIEW PRIOR AUDITS AND STUDIES CONCERNING
IMPROVEMENTS TO SSA'S NUMIDENT DEATHRECORDS AND ASSESS THE CURRENT
PROCESS USED BY SSA TO OBTAIN DEATH INFORMATION FOR SSA PROGRAMS AND
OFFER RECOMMENDATIONS FOR IMPROVEMENT OF THE PROCESS;
CONDUCT ANALYSIS OF SSA PAYMENT DATA TO REDUCE CONCERNS IMPROPER
PAYMENTS.
YOU ARE SUBJECT TO REGULATIONS GOVERNING CONDUCT AND RESPONSIBILITIES OF SPECIAL GOVERNMENT EMPLOYEES.

| 46. Employing Department or Agency | 47. Agency Code | 48. Personnel Office ID | 49. Approval Date |
|---|---|---|---|
| SZ - SOCIAL SECURITY ADMIN | SZ00 | 1166 | 02/23/2025 |

**50. Signature/Authentication and Title of Approving Official**
250726329 / ELECTRONICALLY SIGNED BY:
[redacted]
DIRECTOR, OESS

5–Part 50–316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540–01–333–6238

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296–33, Subch. 4

# NOTIFICATION OF PERSONNEL ACTION

| 1. Name (Last, First, Middle) | 2. Social Security Number | 3. Date of Birth | 4. Effective Date |
|---|---|---|---|
| Employee 9 | [redacted] | [redacted] | 02/23/2025 |

## FIRST ACTION

| 5–A. Code | 5–B. Nature of Action |
|---|---|
| 171 | EXC APPT NTE 02-22-26 |
| **5–C. Code** | **5–D. Legal Authority** |
| H2L | REG 304.103 |
| **5–E. Code** | **5–F. Legal Authority** |
| | |

## SECOND ACTION

| 6–A. Code | 6–B. Nature of Action |
|---|---|
| | |
| **6–C. Code** | **6–D. Legal Authority** |
| | |
| **6–E. Code** | **6–F. Legal Authority** |
| | |

| 7. FROM: Position Title and Number | 8. Pay Plan | 9. Occ. Code | 10. Grade or Level | 11. Step or Rate | 12. Total Salary | 13. Pay Basis |
|---|---|---|---|---|---|---|
| | | | | | | |
| **12A. Basic Pay** | **12B. Locality Adj.** | **12C. Adj. Basic Pay** | **12D. Other Pay** | | | |
| | | | | | | |

| 15. TO: Position Title and Number | 16. Pay Plan | 17. Occ. Code | 18. Grade or Level | 19. Step or Rate | 20. Total Salary/Award | 21. Pay Basis |
|---|---|---|---|---|---|---|
| EXPERT<br>EXPERT<br>S4C KNX0380 | ED | 0301 | 00 | 00 | $0.00 | WC |
| **20A. Basic Pay** | **20B. Locality Adj.** | **20C. Adj. Basic Pay** | **20D. Other Pay** | | | |
| $0.00 | $0.00 | $0.00 | $0.00 | | | |

| 14. Name and Location of Position's Organization | 22. Name and Location of Position's Organization |
|---|---|
| | SZ00 SOCIAL SECURITY ADMINISTRATION<br>CHIEF INFORMATION OFFICER<br>OFFICE OF CHIEF INFORMATION OFFICER |

## EMPLOYEE DATA

| 23. Veterans Preference | 24. Tenure | 25. Agency Use | 26. Veterans Preference for RIF |
|---|---|---|---|
| 1 (1 – None, 2 – 5–Point, 3 – 10–Point/Disability, 4 – 10–Point/Compensable, 5 – 10–Point/Other, 6 – 10–Point/Compensable/30%) | 0 (0 – None, 1 – Permanent, 2 – Conditional, 3 – Indefinite) | | YES: X NO: |

| 27. FEGLI | 28. Annuitant Indicator | 29. Pay Rate Determinant |
|---|---|---|
| A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERAG | 9 NOT APPLICABLE | 0 |

| 30. Retirement Plan | 31. Service Comp. Date (Leave) | 32. Work Schedule | 33. Part–Time Hours Per Biweekly Pay Period |
|---|---|---|---|
| 2 FICA | 02/23/2025 | I INTERMITTENT | |

## POSITION DATA

| 34. Position Occupied | 35. FLSA Category | 36. Appropriation Code | 37. Bargaining Unit Status |
|---|---|---|---|
| 2 (1 – Competitive Service, 2 – Excepted Service, 3 – SES General, 4 – SES Career Reserved) | E (E – Exempt, N – Nonexempt) | 4003431 | 8888 |

| 38. Duty Station Code | 39. Duty Station (City – County – State or Overseas Location) |
|---|---|
| 24-1698-005 | WOODLAWN,BALTIMORE,MARYLAND |

| 40. Agency Data | 41. | 42. | 43. | 44. |
|---|---|---|---|---|
| FUNC CLS 00 | VET STAT X | EDUC LVL | SUPV STAT 8 | POSITION SENSITIVITY CRITICAL-SENSITIVE |

**45. Remarks**

APPOINTMENT AFFIDAVIT EXECUTED 02-23-25.
PREVIOUS RETIREMENT COVERAGE: NEVER COVERED
REASON FOR TEMPORARY APPOINTMENT REVIEW PRIOR AUDITS AND STUDIES CONCERNING
IMPROVEMENTS TO SSA'S NUMIDENT DEATH RECORDS AND ASSESS THE CURRENT
PROCESS USED BY SSA TO OBTAIN DEATH INFORMATION FOR SSA'S PROGRAMS
AND OFFER RECOMMENDATIONS FOR IMPROVEMENT OF THE PROCESS;
CONDUCT ANALYSIS OF SSA PAYMENT DATA TO REDUCE CONCERNS IMPROPER
PAYMENTS
YOU ARE SUBJECT TO REGULATIONS GOVERNING CONDUCT AND RESPONSIBILITIES OF SPECIAL GOVERNMENT EMPLOYEES.

| 46. Employing Department or Agency | 47. Agency Code | 48. Personnel Office ID | 49. Approval Date |
|---|---|---|---|
| SZ - SOCIAL SECURITY ADMIN | SZ00 | 1166 | 02/23/2025 |

**50. Signature/Authentication and Title of Approving Official**
250727746 / ELECTRONICALLY SIGNED BY:
[redacted]
DIRECTOR, OESS

5–Part 50–316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540–01–333–6238

# APPOINTMENT AFFIDAVITS

Expert
(Position to which Appointed)

02/10/2025
(Date Appointed)

Social Security Administration
(Department or Agency)

Office of the Chief Informatio
(Bureau or Division)

Woodlawn, Maryland
(Place of Employment)

I, Employee 1, do solemnly swear (or affirm) that--

## A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

## B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

## C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

Employee 1
(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 10th day of February, 2025

at Woodlawn
(City)

Maryland
(State

[redacted]
(Signature of Officer)

(SEAL)

Commission expires
(If by a Notary Public, the date of his/her Commission should be shown)

Deputy Commissioner for Human Resour
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

# APPOINTMENT AFFIDAVITS

Chief Information Officer
(Position to which Appointed)

03/24/2025
(Date Appointed)

Social Security Administration
(Department or Agency)

Office of the Chief Information Officer
(Bureau or Division)

Woodlawn, MD, United States
(Place of Employment)

I, Employee 2, do solemnly swear (or affirm) that--

## A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

## B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

## C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

Employee 2
[redacted]

Subscribed and sworn (or affirmed) before me this 25 day of March, 2025

at Woodlawn (City) MD (State)

[redacted]
(Signature of Officer)

(SEAL)

Commission expires _____
(If by a Notary Public, the date of his/her Commission should be shown)

Director, OESS
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

# APPOINTMENT AFFIDAVITS

Expert
*(Position to which Appointed)*

02/23/2025
*(Date Appointed)*

Social Security Administration | Office of the Chief Informatio | Woodlawn, Maryland
*(Department or Agency)* | *(Bureau or Division)* | *(Place of Employment)*

I, Employee 4, do solemnly swear (or affirm) that--

## A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

## B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

## C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

Employee 4

Subscribed and sworn (or affirmed) before me this 24 day of February, 2025

at Woodlawn (City) Maryland (State)

[redacted]
(Signature of Officer)

(SEAL)

Commission expires_____
(If by a Notary Public, the date of his/her Commission should be shown)

Director, Office of Executive and Special
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

# APPOINTMENT AFFIDAVITS

Expert
*(Position to which Appointed)*

02/23/2025
*(Date Appointed)*

Social Security Administration | Office of the Chief Informatio | Woodlawn, Maryland
*(Department or Agency)* | *(Bureau or Division)* | *(Place of Employment)*

I, Employee 6, do solemnly swear (or affirm) that--

## A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

## B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

## C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

Employee 6
(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 24 day of February, 2025

at Woodlawn (City) Maryland (State)

[redacted]
(Signature of Officer)

(SEAL)

Commission expires
(If by a Notary Public, the date of his/her Commission should be shown)

Director, Office of Executive and Special
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

# APPOINTMENT AFFIDAVITS

Expert
*(Position to which Appointed)*

02/23/2025
*(Date Appointed)*

Social Security Administration | Office of the Chief Informatio | Woodlawn, Maryland
*(Department or Agency)* | *(Bureau or Division)* | *(Place of Employment)*

I, Employee 9, do solemnly swear (or affirm) that--

## A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

## B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

## C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

Employee 9

Subscribed and sworn (or affirmed) before me this 24 day of February, 2025

at Woodlawn (City) Maryland (State)

(Signature of Officer)

(SEAL)

Commission expires
(If by a Notary Public, the date of his/her Commission should be shown)

Director, Office of Executive and Special
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

# APPOINTMENT AFFIDAVITS

Expert
*(Position to which Appointed)*

03/16/2025
*(Date Appointed)*

Social Security Administration
*(Department or Agency)*

Office of the Chief Informatic
*(Bureau or Division)*

Woodlawn, MD
*(Place of Employment)*

I, Employee 11, do solemnly swear (or affirm) that--

## A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

## B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

## C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

Employee 11
(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 17 day of March, 2025

at Woodlawn (City) Maryland (State)

[redacted]
(Signature of Officer)

(SEAL)

Commission expires_____
(If by a Notary Public, the date of his/her Commission should be shown)

Director, OESS
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI) -** Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI) -** Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery t[redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery t[redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

Employee 9

First Name:

Employee 9

Last Name:

[redacted]

Day Phone:

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

Signat Employee 9

Date: 02/24/2025

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI)** - Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI)** - Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

Employee 6

First Name: Employee 6

Last Name: [redacted]

Day Phone:

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

| Signature: Employee 6 | Date: 02/24/2025 |
|---|---|

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI)** - Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI)** - Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees** - Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: [redacted] Employee 3

Last Name: [redacted] Employee 3

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

Signature: [redacted] Employee 3 Date: 2/18/25

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI)** - Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI)** - Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: [redacted]

Last Name: [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

Signature: [redacted] Date: 02/10/2025

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI)** - Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI)** - Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: [redacted]

Last Name: [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Inform[redacted]es of Behavior completed:

Signature: [redacted] Date: 03/05/2025

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI) -** Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI) -** Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: [redacted] Employee 5

Last Name: [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

Signature: [redacted] Employee 5 Date: 07/18/2025

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI) -** Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI) -** Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.

Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.

Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.

For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees** - Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Nam Employee 11 [redacted]

Last Nam [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

| Sig Employee 11 [redacted] | Date: 3/10/25 |
|---|---|

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI) -** Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI) -** Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: Employee 8

Last Name: [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

| Signature: Employee 8 | Date: 02/18/2025 |
|---|---|

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI) -** Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI) -** Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: Employee 4

Last Name: [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

Signatu[redacted] Employee 4 | Date: 2/24/202[illegible]

*If yo[redacted]r illegible, or if your signature is omitted, this form will not be p[redacted]*

Form **SSA-221** (08-2020)
Social Security Administration



# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI) -** Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI) -** Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: Employee 10

Last Name: [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

Signature: Employee 10 [redacted]

Date: 2/18/25

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*

# Why Protect PII?

- Federal laws, regulations, & policies require agencies to appropriately safeguard PII; Examples applying to SSA employees:
  - The Privacy Act of 1974 (5 U.S.C. 552a)
  - The Social Security Act (42 U.S.C. 1306(a))
  - The Internal Revenue Code (26 U.S.C. 6103)
  - SSA Regulations (20 C.F.R. Part 401 & Appendix A, Employee Standards of Conduct)
  - FISMA and related guidance (e.g., 44 U.S.C. 3551 et seq; NIST, BOD)
  - SSA Information Security Policy (ISP)
- These authorities dictate when employees may access and disclose PII, as well as obligations to protect PII.
- Employee Responsibilities:
  - Safeguard and Secure - Know, understand and follow all agency policies and directives on security, privacy and confidentiality practices (including those on PII)
  - Legal Compliance - Access and disclose only as law permits
  - PII Breach - Report the loss or suspected loss of PII immediately to their supervisor, whether suspected or confirmed; share breach information only with agency employees with a need to know or external parties authorized to receive breach information.
- Civil and criminal penalties may also apply for the agency and its employees.
  - Civil lawsuits are frequently brought under 5 U.S.C. 552a(g).
  - Criminal penalties may be brought against specific employees (next slide).

# Need for *Authorized* Access/Disclosure

- What is PII? Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information linked or linkable to a specific individual (OMB A-130; 401 CFR 401.25)
  - Examples: Names, Date of Births, Social Security numbers, Address, Emails, Phone numbers, Earnings Records, Beneficiary or claims information, Personnel Files, Death data
  - Includes aggregates/tabulations that can be traced back to identify people
  - PII still protected when removed from custodial systems
- Before acting, ensure you have authorization to access/disclose
- The Privacy Act (5 USC 552a) and SSA Regulations generally prohibit disclosure of PII from agency records without the consent of the subject of the record, unless certain exceptions apply
  - Agencies may share PII with other SSA employees on a "need to know" basis to perform official job duties
  - Disclosure to contractors, other Federal agencies, or other third parties cannot access based solely on "need to know;" separate legal authority must exist
- Other laws also further restrict SSA usage and disclosure of specific types of data we keep
  - E.g., Tax Return Information, Death Records, Drug and Alcohol Records, Consumer Report Information

# Legal Agreements

**Where disclosure permitted, legal agreements generally required, *e.g.*,:**

- Privacy Act, 5 U.S.C. 552a(e)(10) – requires appropriate safeguards to protect individual records
  - NIST SP 800-47 Rev. 1; OMB Circular A-130 – Further requiring agreements
- Privacy Act, 5 U.S.C. 552a(c) also requires accounting of disclosures, which require documentation to track disclosures made
- Computer Matching and Privacy Protection Act (5 U.S.C. 552a(a)(8), 552a(o))
  - Covers computerized comparisons of 2 or more automated systems of records (SOR) or a SOR with non-Federal records for establishing or verifying eligibility, or compliance with requirements, for payments under Federal benefit programs; recouping payments or debts under Federal benefit programs; or certain personnel or payroll system matching
  - Requires Federal Register publication and other requirements (e.g., submit to OMB/Congress, DIB clearance, CBA)
- Routine Use Conditions – Some agency routine uses (Federal Register published) require agreements (5 U.S.C. 552a(b)(3))
- Privacy regulations – For instance 20 CFR 401.165 requires certain safeguards (including agreement terms) for research agreements

**Common Legal Agreement Types:** Contracts, Grants, Cooperative Awards, Data Exchange/Computer Matching Agreements, Interagency/Reimbursable Agreements

- Interconnection Security Agreements (ISA) are NOT legal agreements but established with a legal agreement (e.g., NIST SP 800-47 Rev. 1); ISAs specify the technical and security requirements for establishing, operating, and maintaining an interconnection between systems

**If no agreement, the information would generally be public.**

# Penalties for Wrongful Use/Access/Disclosure

| Law | Penalty |
|---|---|
| 42 U.S.C. 1306(a)(1) – Governing disclosure of records, reports or information in violation of agency regulation and applicable Federal law | Violator guilty of a felony and, upon conviction, punished by a fine not exceeding $10,000 for each violation occurrence, or by imprisonment not exceeding 5 years, or both. |
| 5 U.S.C. 552a(i) – Governing disclosure of PII protected by the Privacy Act or agency privacy regulations | Violators guilty of a misdemeanor and fined not more than $5,000 if they: willfully disclose in violation, willfully maintain a system of records without required notice, or knowing and willfully request or obtain records under false pretenses |
| 26 U.S.C. 7213, 7214A – Governing unauthorized disclosure (7213) and inspection (7214A) of tax return information protected under 26 U.S.C. 6103 | 7213 - Violators guilty of felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both; plus dismissal or discharge from federal employment<br>7214A – Violators fined not exceeding $1,000, or imprisonment of not more than 1 year, or both; plus dismissal or discharge from federal employment |
| 20 C.F.R. Part 401 Appx A – Governing improper disclosure of Privacy Act records | Disciplinary action plus criminal prosecution under the law |

# Legal Questions

- Contact the Office of General Law Division 1, Disclosure Law
  - You can email controls: [redacted]
  - Contacts:
    - Acting General Counsel
      - Grace Kim
    - Acting Associate General Counsel (AGC) and Deputy AGC, Office of General Law Division 1 (advising in fiscal and disclosure law):
      - Terri Daniel ([redacted]@ssa.gov)
    - Supervisory Attorney for Disclosure Law:
      - Jessica Vollmer ([redacted]@ssa.gov)
    - Senior Attorney Contact for Disclosure Law:
      - [redacted]@ssa.gov)

# Information Security and Privacy Awareness / Rules of Behavior

## Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

## Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

## Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI) -** Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI) -** Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

## Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

## Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

## Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

## Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

## Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

## Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

## Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

## Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

## Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

## Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

## Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

**SSA Employees -** Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: [redacted] Employee 2

Last Name: [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

Signature: [redacted] Employee 2 Date: 2/18/25

*If your n[redacted]mitted or illegible, or if your signature is omitted, this form will not be proce*