# IT Security Procedural Guide:

# Termination and Transfer

# CIO-IT Security-03-23

**Revision 7**

April 18, 2025

Office of the Chief Information Security Officer

## VERSION HISTORY/CHANGE RECORD

| Change Number | Person Posting Change | Change | Reason for Change | Page Number of Change |
|---|---|---|---|---|
| | | **Initial Release and Revision 1** | | |
| 1 | Klemens | There is no record of the dates or changes for the initial release or Revision 1 of this guide. | Document reason initial release and Revision 1 changes are not listed. | Version History |
| | | **Revision 2 – January 29, 2008** | | |
| 1 | Scott/ Heard | Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1B requirements. | Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1B requirements. | Various |
| 2 | Scott/ Heard | Changes throughout the document to correspond with revisions made to CIO-IT Security-01-09, CIO-IT Security-01-03 and CIO-IT Security-01-04. | Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents | Various |
| 3 | Windelberg | Changes throughout the document to correspond with update of the current version of GSA CIO P2100 and other updates | The most current version of GSA CIO P2100 and more detailed guidance on implementing policy | Various |
| | | **Revision 3 – April 28, 2017** | | |
| 1 | Wilson/ Nussdorfer/ Klemens | Changes made throughout the document to reflect current NIST SP 800-53 and GSA CIO 2100.1 versions and other GSA processes. | Updated NIST control parameters, GSA policy statements, GSA process descriptions, and resources available to facilitate processes. | Various |
| | | **Revision 4 – June 4, 2019** | | |
| 1 | Dean/Klemens | Changes made include:<br>• Updates to reflect current GSA policies.<br>• Updates to align with current GSA processes. | Biennial update. | Throughout |
| | | **Revision 5 – May 25, 2021** | | |
| 1 | Dean/Klemens | Changes made include:<br>• Updates to reflect current GSA policies.<br>• Updates to align with current GSA processes.<br>• Updates to align with NIST SP 800-53, Revision 5 controls and parameters. | Updated to reflect current GSA policies and processes. | Throughout |
| | | **Revision 6 – April 7, 2022** | | |
| 1 | Dean/Klemens | Changes made include:<br>• Updated to current GSA process for notifying the Insider Threat team of offboarded personnel.<br>• Updates to align with current GSA format. | Updated to reflect current GSA processes and guide formatting. | Throughout |
| | | **Revision 7 – April 18, 2025** | | |
| 1 | Normand/ Peralta/ Klemens | Revision included:<br>• Updated section 4.1: Monthly Reviews (GSA Employees)<br>• Updated controls to add leading zeros and to align with the CTW. | Updated to reflect current GSA processes and guide formatting. | Throughout |

| | | | | |
|---|---|---|---|---|
| | | - Moved policy, references, and roles and responsibilities to appendices. | | |

# Approval

IT Security Procedural Guide: Termination and Transfer, CIO-IT Security 03-23, Revision 7, is hereby approved for distribution.

Signed by:
Dovarius Peoples
34793F3A1E88420...

Dovarius Peoples
Acting GSA Chief Information Security Officer

**Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.**

# Table of Contents

**Note:** Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix) or a webpage. Hyperlinks for external documents and GSA policies and guides will only be provided in Appendix B.

# 1 Introduction

This document provides guidance for individuals with the responsibility to modify, disable, or remove access for terminated or transferred General Services Administration (GSA) Federal employees, including contractors who have access privileges to GSA information technology (IT) resources, data, and facilities.

A termination occurs when an individual departs their organization and ends their association with the GSA. A termination may be considered friendly (voluntary) or unfriendly (involuntary). In either case, the individual must be denied access to all GSA resources in the timeframes specified in Section 6.1.

A transfer occurs when an individual's job position or duties change, yet they maintain an association with the GSA. An individual's access privileges to certain GSA IT resources may need to be maintained, reduced, or expanded based upon changes in their work responsibilities. For example, someone changing organizations within the GSA would retain a gsa.gov email address but their organizational affiliation should be changed.

When an individual terminates or transfers, management personnel, security personnel, and human resources (HR) personnel are responsible for ensuring the individual's access privileges are updated in accordance with the time frames identified in Section 6.1 and Section 6.2. Initial responsibility lies with the individual's supervisor and the Information System Security Manager (ISSM) or Information System Security Officer (ISSO) of each IT resource to which the individual has access.

Termination or revision of access rights for individuals includes access to GSA IT systems (e.g., computers, networks, applications, mobile devices) and physical locations (e.g., buildings, rooms, etc.), whether they are owned or operated by the GSA or vendors/contractors.

**Note:** Consistent with CIO-IT Security-01-07: Access Control, system/network administrators, in conjunction with System and Data Owners, ISSMs and ISSOs are responsible for establishing, maintaining, and removing access rights to GSA systems. All allowed accounts must be documented and defined and include group and role memberships and access authorizations.

Any deviations from the security requirements established in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy" must be coordinated by the ISSO through the appropriate ISSM and authorized by the system's Authorizing Official (AO) and Chief Information Security Officer (CISO) concurrence.

## 1.1 Purpose

The purpose of this guide is to describe the processes appropriate personnel must follow when an individual's access requirements to GSA IT resources have changed due to employment termination or transfer. This guide also documents procedures for regular review of access privileges to ensure that no one who has been terminated or transferred inappropriately retains access to GSA IT resources.

## 1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the processes and procedures for modifying, disabling, or removing access to GSA systems and information. Per CIO 2100.1, a GSA system is a system used or operated:

- by the GSA; or
- on behalf of the GSA by a contractor of GSA or by another organization.

### 1.3 Policy

Appendix A contains the CIO 2100.1 policy statements regarding termination and transfer at the GSA.

### 1.4 References

Appendix B provides links to references used throughout this guide.

## 2 Roles and Responsibilities

Appendix C provides a listing of the roles and responsibilities related to termination and transfer at the GSA.

## 3 Termination and Transfer Procedures

To maintain the security of logical and physical resources, access privileges must be denied within the timeframe specified in Section 6.1 for termination, or Section 6.2 for transferring, whenever an individual's employment status changes, whether through friendly termination, unfriendly termination, or transfer.

The following sections provide an overview of the procedures for denying and deleting access privileges of an individual who terminates or transfers. Involuntary separations such as death, removal, and other similar unscheduled separations will be addressed on a case-by-case basis by consulting the servicing human resources office.

**Note:** Disgruntled employees or contractors, whether or not they have been fired, can do significant resource-related damage. Of particular concern are those employees or contractors who have resource administrative access (such as system administrator, database administrator, telecom administrator, developers, etc.) and/or are in a significant position of trust, including managers. Extra care should be taken by supervisors to ensure access privileges of potentially disgruntled employees are removed within the timeframe specified above.

**Note:** For contractors, the Government Manager or Contracting Officer's Representative (COR) is the contractor responsible for performing the procedures and processes in the following sections.

### 3.1 Offboarding

When it has been determined that a GSA employee will have a friendly termination or transfer the process described for Offboarding Employees will be followed.

Consistent with GSA Order HRM 7800.14, "Pre-Exit Clearance Guidance and Procedures for All Separations," the GSA employee must complete a GSA Form 1655, Pre-Exit Clearance

Checklist. This checklist outlines the necessary tasks to be completed for the termination or transfer. The individual's supervisor has overall responsibility for certifying that all checklist items have been acceptably completed prior to the final termination or transfer date.

**Note:** Service and Staff offices and Regional offices have established internal procedures for clearing employees using GSA Form 1655, Pre-Exit Clearance Checklist. The procedures should provide a list of issuing offices and locations for employees to use in obtaining appropriate clearances.

## 3.2 Account Deactivation

Upon notification of a pending termination, the supervisor of the GSA employee or contractor will initiate the termination procedures by submitting a request via the GSA IT Service Desk request as follows:

1) Select “GSA IT Self-Service Catalog”
2) Expand “Account Services”
3) Select “On-Boarding/Off-Boarding”
4) Select “Delete GSA Network Accounts”
5) Input the name of the individual being terminated in the “Requested For” field.
6) Input the expected departure date in the “Planning Date” field.
7) Input the name of the person who will be taking over responsibilities of the terminating person's Google folder in the “Who should google documents be transferred to?” field. **Note:** If no other person can be identified, the supervisor's name may go in this field.
8) Input the reason for the request in the “Please provide a business justification for this request.” field.
9) Submit the request.

## 3.3 Transfer Request

Upon notification of a pending transfer, the GSA employee, contractor, or his/her supervisor will initiate the transfer procedures by submitting a Service Catalog request as follows:

1) Select “GSA IT Self-Service Catalog”
2) Expand “Client and User Services”
3) Select the appropriate subsection:
   a. “Employee Change Requests” – if changing organizations
   b. “General Requests” -> “GSA Generic Request” – if the transfer does not involve changing organizations
4) Input the name of the individual being transferred in the “Requested For” field.
5) Input the remaining required fields for the request selected in Step 3.
6) Submit the request.

## 3.4 Out Brief/Debriefing

The supervisor of the terminated or transferred personnel is responsible for ensuring that all applicable tasks are completed prior to the individual's last official day in his/her current GSA position. This includes ensuring that all items issued by the Government are returned to the issuing offices before the individual is transferred or terminated from GSA. Individuals no longer having a working relationship with GSA must not remove GSA information.

As necessary, based upon the individual's GSA access, a security debriefing will also be performed. During this debriefing the individual will be reminded that when their relationship with GSA is terminated the requirement not to disclose confidential and/or privacy data based on work-related duties is still effective.

**Note:** GSA employees will leverage GSA Form 1655, Pre-Exit Clearance Checklist, to ensure all required tasks are completed at the time of the final debrief.

## 3.5 Physical Facilities Protection

When a GSA employee or contractor terminates or transfers, it is also important to protect facilities, which may contain sensitive or critical information. Physical access encompasses buildings, doors to protected rooms, and locks on cabinets or desks. Physical access control may also be tied to IT access control.

The individual being terminated or transferred must be denied physical unescorted access to all facilities following the out brief. The individual's supervisor is responsible for working with appropriate personnel to deny access to physical facilities to prevent or limit access by the terminating or transferring individual, in accordance with GSA CIO-IT Security-12-64: Physical and Environment Protection. Denying access should include the following:

- Notifying personnel responsible for any physical access to facilities to deny access.
- Collecting all access cards (e.g., Personal Identity Verification (PIV) card).
- Deactivating codes/identification numbers on access cards.
- Changing all codes, cipher locks, combination locks, or passwords known by or available to the individual.
- Collecting all keys in the individual's possession.
- Updating access control lists, mailing lists, etc.

## 3.6 Work Product Retrieval

Individuals may not retain, give away, or remove from GSA any GSA information other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of employment. All other GSA information in the custody of the departing individual must be provided to the individual's supervisor before the time of departure. For example, as required in the ServiceNow ticketing process, an individual's Google drives, folders, files, etc. must be reassigned to an individual still supporting GSA. To ensure the collection, dissemination and/or deletion of all work products for the individual being terminated or transferring, the supervisor is responsible for:

- Providing instructions on the proper disposal of information as well as whether or not to "clean up" the assigned resource before the individual leaves.
- Ensuring cryptographic keys are obtained when cryptography is used to protect data.
- Reviewing both resource-resident files and paper files to determine who should be given possession of the files and/or the appropriate methods to be used for file disposal or destruction.
- Reassigning the individual's duties as well as specifically delegating responsibility for information (e.g., files, folders, etc.) formerly in the individual's possession.

Transferring custodian responsibilities ensures security measures are maintained in acceptable ways. The reassignment of duties process is especially important if the files contain sensitive, critical, or valuable information.

## 3.7 Special Considerations for Unfriendly Terminations

Unfriendly termination involves the removal of an individual under involuntary or adverse conditions. This may include termination for cause, reduction in force (RIF), involuntary transfer, and situations with pending grievances. The Office of Human Resources Management (OHRM) coordinates with the Insider Threat Program regarding unfriendly terminations as necessary.

A termination of this type for GSA employees occurs only after the supervisor consults with the OHRM. An evaluation of the circumstances is conducted, including the reasons for the request, the supporting documentation, and potential alternatives. Procedural requirements for evaluating performance and deciding on termination are outside the scope of this guide.

Disgruntled or upset employees must be removed from positions where serious damage to agency property may occur (including information and communication resources). In the event an employee must be removed or involuntarily separated, or when an employee notifies an organization of a resignation and it can be reasonably expected that it is on unfriendly terms, the following actions must be completed immediately:

- Deny access to resources. If an individual is terminated, resource access should be removed at the same time (or just before) the individual is notified of dismissal.
- Relieve the individual of all duties. During the “notice of termination” period, it may be necessary to assign the individual to a non-sensitive position. This may be particularly true for individuals capable of changing programs or modifying the resource or an application.
- Require the return of all GSA equipment and information. Ensure all Government property in the custody of the terminated individual is returned to the issuing office before the individual is separated from GSA.
- Ensure the individual is escorted out of the GSA facility. In some cases, physical removal from GSA facilities may be necessary. While the individual packs belongings, careful supervision must be maintained to prevent malicious activities.

## 3.8 Special Considerations for Contractors

Contracting Officers and CORs must include wording in contracts that assignment changes in contractor personnel will be communicated to GSA IT security personnel. It must be a contractual requirement that the contractor’s company notify the GSA COR of any terminations or changes in the contracting employee’s responsibilities that support the specified timeframe in Section 6.1 for terminating or Section 6.2 for transferring. Additional information regarding contractors is available on the Contractor Offboarding InSite webpage.

In the event the individual terminated is a contractor, it is the responsibility of the contractor’s supervisor to notify the appropriate ISSO and to coordinate denying access to GSA IT resources with the ISSO and appropriate administrators. The contractor must provide and maintain an updated list of the names of contractor personnel who have approved access to GSA resources.

# 4 Monthly Processes

## 4.1 Monthly Reviews (GSA Employees)

Monthly reviews are done to ensure that the access privileges have been revoked for any GSA employee who has been terminated. The monthly review procedure provides a measure of quality control, with the ISSM verifying the activities of the ISSOs. The ISSM will coordinate with each ISSO for the systems under their purview to ensure that former employees identified through the monthly review are denied access to all resources by the ISSOs coordinating with appropriate administrators to remove access.

**Note:** There is no corresponding monthly process from the OCISO for GSA employees who transfer.

## 4.2 Monthly Offboarding Report (all personnel)

A monthly report of offboarding tickets from the GSA IT Service Desk for all GSA users is sent to the Insider Threat team in support of GSA's Insider Threat Program.

# 5 Annual Reviews

Annual reviews of user access privileges are required by CIO 2100.1 and CIO-IT Security-01-07. Performing these reviews ensures that GSA IT resources remain protected from unauthorized access and promotes the security of GSA information and information resources. The annual review provides a quality control check on access to GSA resources.

System Owners are required to review user accounts to ensure that individuals who have accounts are not just currently employees or contractors of GSA but also that access is appropriate based on their job functions and need-to-know.

Data Owners are required to review access authorization listings to ensure that the type or types of access remains appropriate.

## 5.1 Annual Review of User Accounts: Procedure and Responsibilities

1) The System Owner will review the entire list of user accounts for each system for which he or she is responsible. The review must verify that:
    a. Each named user is still associated with GSA; and
    b. Access to the system is appropriate to each individual's job function and need-to-know.
2) If the System Owner determines that a user account exists but access is not appropriate, the System Owner must notify the ISSM and ISSO.
3) The System Owner/ISSO must coordinate with the appropriate administrators to have a user account that no longer requires access to the system removed as well as any associated files or information, as appropriate.
4) The ISSO then must notify the ISSM and the System Owner that the account has been removed.
5) The System Owner must then document any action taken and update the list of user accounts.

**Note:** If the System Owner and Data Owner disagree on the level of authorization given to an individual, they will consult with their management, and the ISSO/ISSM if applicable, to determine the suitable level of authorization.

### 5.2 Annual Review of Authorizations: Procedure and Responsibilities

1) The Data Owner reviews the access authorizations for which he or she is responsible. The review must verify that each user's authorization privileges are appropriate to the individual's job function, need-to-know, and least privilege.
2) If the Data Owner determines that a user account or authorization exists but access is not appropriate, the Data Owner must coordinate with the System Owner, and ISSO/ISSM if applicable, to have administrators modify, disable, or delete the account.
3) Administrators must assign the files or information associated with the user account modified, disabled, or deleted, to an existing user or remove them, as appropriate.
4) The administrators must notify the System Owner, Data Owner, and ISSO/ISSM if applicable, that the account has been modified, disabled, or deleted.
5) The Data Owner must then document any action taken and update the list of user authorizations.

**Note:** If the System Owner and Data Owner disagree on the level of authorization given to an individual, they will consult with their management, and the ISSO/ISSM if applicable, to determine the suitable level of authorization.

## 6 GSA Guidance for PS-04 and PS-05 Controls

The PS-04 and PS-05 controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations" address personnel termination and transfer. The GSA-defined parameter settings included for the control requirements in the following sections are in blue text and offset by brackets, followed by GSA's implementation guidance per the Federal Information Processing Standard (FIPS) Publication (PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems" security categorization level.

For readers' ease of use, "mini tables" (see Table 6-1) that contain control/enhancement designation and applicability information are provided at the end of control statements for each PS control. The tables allow readers to see if a control/enhancement is applicable at the system's FIPS Level/A&A process and if it is common (C), Hybrid (H), or system specific (S).

**Table 6-1. Example Mini Table**

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| Control ID | ✓ | ✓ | ✓ | C | H |

### 6.1 PS-04 Personnel Termination

**Control:** Upon termination of individual employment:

a. Disable system access within [30 days of personnel termination];
b. Terminate or revoke any authenticators and credentials associated with the individual;
c. Conduct exit interviews that include a discussion of [privacy, disclosure, and confidentiality responsibilities];

d. Retrieve all security-related organizational system-related property; and
e. Retain access to organizational information and systems formerly controlled by terminated individual.

**Control Enhancements:**

(02) Personnel Termination | Automated Actions. Use [GSA SSO or Contractor defined and GSA CISO and AO approved automated mechanisms] to [notify supervisors and ISSMs/ISSOs of individual termination actions; disable access to system resources].

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PS-04 | ✓ | ✓ | ✓ | H | H |
| PS-04(02) | | | ✓ | S | S |

**Common Control Implementation**
For PS-04, disabling GSA account(s)/information system access is initiated and facilitated by an individual's supervisor/Contracting Officer (CO)/Contracting Officer Representative (COR). GSA account access (ENT Long-Name Account [LNA] and Short-Name Account [SNA]) is disabled within 24 hours of an approved Service Catalog Request indicating personnel termination.

Terminating/revoking of all information system-related property which includes HSPD-12 cards, authentication tokens (USB for privileged access), laptops, etc. is facilitated by the supervisor and sent to GSA IT support personnel based on the Service Catalog Request.

Exit interviews are initiated and facilitated by the supervisor/CO/COR of an individual ensuring that privacy, disclosure, and confidentiality responsibilities are reviewed with the person leaving.

Retrieval of all information system-related property which includes HSPD-12 cards, authentication tokens (USB for privileged access), laptops, etc. is facilitated by the supervisor and sent to GSA IT support personnel based on the Service Catalog Request.

As part of user off-boarding, the supervisor/CO/COR is responsible for coordinating with GSA IT support personnel the transfer of organizational information and information systems based on the Service Catalog Request.

**Federal System-Specific Expectation**
For PS-04, the GSA supervisor/CO/COR is responsible for notifying the appropriate System Owner/Account Manager about a user's off-boarding so they can take appropriate action at a system/application level. The GSA supervisor/CO/COR is responsible for submitting a GSA off-boarding ServiceNow ticket required per assigned personnel.

For PS-04(02), the automated mechanisms used to notify personnel and disable access to system resources must be approved by GSA OCISO and AO, and annotated as such in the GSA Control Tailoring Workbook for the system.

**Vendor/Contractor System-Specific Expectation**
For PS-04, vendors/contractors must adhere to the personnel termination processes defined in GSA policies and guidance. They may supplement this process by conducting their own personnel termination processes.

For PS-04(02), the automated mechanisms used to notify personnel and disable access to system resources must be approved by GSA OCISO and AO, and annotated as such in the GSA Control Tailoring Workbook for the system.

## 6.2 PS-05 Personnel Transfer

**Control:**

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiate [denial or modification of access privileges to specific information systems based on their new duties] within [30 days of personnel transfer];
c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notify [supervisor and/or ISSMs/ISSOs] within [14 days of personnel transfer].

| | Low | Mod | High | Federal | Contractor |
|---|---|---|---|---|---|
| PS-05 | ✓ | ✓ | ✓ | H | H |

**Common Control Implementation**
For PS-05, review of an individual’s ongoing operational need for current logical and physical access is initiated and facilitated by the individual’s supervisor/Contracting Officer (CO)/Contracting Officer Representative (COR). The supervisor/CO/COR is responsible for initiating transfer procedures (with the individual), such as creating a Service Catalog Request, as necessary, to ensure the user’s access is adjusted as appropriate for their new assignment.

Access is denied or modified within 3 days of an approved Service Catalog Request indicating personnel transfer.

The supervisor/CO/COR is responsible for coordinating with the user to ensure modifications to the user’s access, as appropriate, to their new assignment. If necessary, Service Catalog Request(s) can be opened to facilitate access modifications.

Supervisors are notified within 24 hours that a personnel transfer Service Catalog Request has been serviced.

**Federal System-Specific Expectation**
For PS-05, Supervisors/CO/COR are responsible for notifying the appropriate System Owner/Account Manager of a user’s transfer so they can take appropriate action at a system/application level.

**Vendor/Contractor System-Specific Expectation**
For PS-05, vendors/contractors must adhere to the personnel transfer processes defined in GSA policies and guidance. They may supplement this process by conducting their own personnel termination processes.

# 7 Summary

Termination and transfer procedures are beneficial to ensure the security of GSA’s IT resources and facilities. Vulnerabilities, threats, and risks to IT resources and facilities can be significantly reduced by employing standard individual termination and transfer guidelines.

The GSA employees, contractors, and other organizations using GSA’s IT resources on behalf of the GSA must adhere to the GSA policy regarding termination and transfer of access privileges.

Effective termination and transfer procedures established and implemented for GSA IT resources assist the GSA in complying with federal mandates and the GSA IT Security Policy. Once effective termination and transfer procedures have been established, continuous monitoring methodologies such as monthly and annual reviews assist in maintaining effective control of access to GSA IT resources and facilities to mitigate risks.

# Appendix A: CIO 2100.1 Policy Statements on Termination and Transfer

CIO 2100.1 contains many policy statements regarding access control, privilege management, and user account management. The following policy statements from it are focused on the termination and transfer of personnel and their access to GSA IT resources and facilities.

**Chapter 4, Policy for Protect Function states:**

1. Identity Management, Authentication and Access Control.

j. Information system user accounts (i.e., persons) must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing user accounts. Reviews and validations of all user accounts shall be completed consistent with the SSPP to ensure the continued need for system access. GSA user account management processes include:

(1) Supervisors, CORs, or account managers coordinating and arranging system access termination for all departing or resigning personnel, including both GSA employees and contractors.

(2) Supervisors, CORs, or account managers initiating account removal, disablement, or permission changes based on a review of information provided by the OCISO (e.g., separation lists, role revisions) for GSA users, including both GSA employees and contractors.

(3) System Owners/account managers verifying that separated GSA users, i.e., users with an ENT account, no longer maintain access to GSA IT systems or resources after 30 days of separation. Verification of non-GSA users' access removal must be performed within the time period specified in the SSPP in NIST control AC-2(3).

(4) ISSOs, ISSMs, and System Owners ensuring processes for removing or modifying access to GSA systems, based on terminations and transfers, are performed IAW procedures specified in GSA CIO-IT Security-03-23.

(5) Supervisors, CORs, or System/Data Owners submitting GSA user access requests and user permission or role changes for account manager approval based on a user's job function and need-to-know.

(6) System Owners/Data Owners, with assistance from the designated ISSO, ensuring system access is restricted to authorized users who meet GSA and system access requirements, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs.

(7) System Owners/Data Owners, with assistance from the designated ISSO, ensuring system access authorizations enforce separation of duties, see Separation of duties.

dd. User authorizations must be verified annually for all information systems to determine if they remain appropriate.

## Appendix B: References

**Federal Laws, Standards, Regulations, and Publications:**

- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations

**GSA Policies, Procedures, Guidance:**

- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy
- GSA Order HRM 7800.14, Pre-Exit Clearance Guidance and Procedures for All Separations

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page. The template listed is available on the GSA internal IT Security Forms and Aids page.

- CIO-IT Security-01-07: Access Control (AC)
- CIO-IT Security-12-64: Physical and Environmental Protection
- GSA Control Tailoring Workbook

# Appendix C: Roles and Responsibilities

The termination and transfer roles and responsibilities provided in this section have been extracted from CIO 2100.1 or summarized from other GSA policies, procedures, and processes. A complete set of GSA security roles and responsibilities can be found in Chapter 2, Security Roles and Responsibilities, of CIO 2100.1. Throughout this guide specific processes and procedures for managing the termination and transfer of personnel within GSA are described.

## GSA Personnel Security Officer/Office of Mission Assurance (OMA)

Responsibilities include the following:

- Developing, promulgating, implementing, and monitoring GSA personnel security programs.
- Developing and implementing access agreements, and personnel screening, termination, and transfer procedures.
- Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.

## Information System Security Manager (ISSM)

Responsibilities include the following:

- Providing guidance, advice, and assistance to ISSOs on IT security issues, the IT Security Program, and security policies.
- Reviewing ISSO checklists submitted in the Archer Governance, Risk, and Compliance (GRC) application and coordinating with ISSOs, as necessary, for systems under their purview.
- Coordinating with System Owners and ISSOs to ensure all activities required regarding personnel terminations and transfers are performed as described in this guide.

## Information System Security Officer (ISSO)

Responsibilities include the following:

- Ensuring the system is operated, used, maintained, and disposed of IAW documented security policies and procedures. Necessary security controls should be in place and operating as intended.
- Performing the recurring activities as listed in the ISSO Checklists implemented in the Archer GRC application.
- Supporting System Owners and System/Network Administrators to ensure all activities required regarding personnel terminations and transfers are completed as described in this guide.

## System Owners

Responsibilities include the following:

- Conducting annual reviews and validation of system users’ accounts to ensure the continued need for access to a system and verify users’ authorizations (rights/privileges).

- Verifying within 30 days of personnel termination that terminated personnel no longer maintain access to GSA IT systems or resources.

### Data Owners

Responsibilities include the following:

- Reviewing access authorization listings and determining whether they remain appropriate at least annually.
- Verifying within 30 days of personnel termination that terminated personnel no longer maintain access to GSA IT systems or resources.

### Contracting Officers (CO)/Contracting Officer's Representative (COR)

Responsibilities include the following:

- Collaborating with the Chief Information Security Officer (CISO) or other appropriate official to ensure that the agency's contracting policies adequately address the agency's information security requirements.
- Ensuring Service Catalog requests are opened for terminating contractor personnel who are no longer supporting GSA and coordinating with OCISO and GSA IT personnel as necessary.

### Supervisors

Responsibilities include the following:

- Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system.
- Coordinating and arranging system access termination within 30 days of personnel termination for all terminating personnel.
- Coordinating and arranging system access modifications within 30 days of personnel transferring for transferring personnel.
- Terminating all work-related privileges within 30 days of personnel termination.
- Notifying employees that departed individuals are no longer permitted on GSA property or to use GSA resources unless escorted by an authorized person.
- Collecting or coordinating the return of all keys, badges, equipment, and other Government resources, including GSA information in accordance with GSA Form 1655, Pre-Exit Clearance Checklist.
- Ensuring all Government property in the custody of the individual is returned to the issuing office before that individual terminates or transfers.
- Ensuring Service Catalog requests are opened for terminating employees and contractors under your supervision who are no longer supporting GSA and coordinating with OCISO and GSA IT personnel as necessary.

### System/Network Administrators

Responsibilities include the following:

- Coordinating and arranging the disabling and deleting of user accounts, permissions, and privileges for system access within 30 days of personnel termination for all terminating personnel.
- Coordinating and arranging system access modifications within 30 days of personnel transferring for transferring personnel.