IT Security Procedural Guide:

Termination and Transfer

CIO-IT Security-03-23

Revision 6

April 19, 2022

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: • Updates to reflect current GSA policies. • Updates to align with current GSA processes.	Biennial update.	Throughout
		Revision 5 – May 25, 2021		
1	Dean/ Klemens	Changes made include: • Updates to reflect current GSA policies. • Updates to align with current GSA processes. • 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 19, 2022		
1	Dean/ Klemens	Changes made include: • Updated to current GSA process for notifying the Insider Threat team of offboarded personnel. • Updates to align with current GSA format.	Updated to reflect current GSA processes and guide formatting.	Throughout

Approval

IT Security Procedural Guide: Termination and Transfer, CIO-IT Security 03-23, Revision 6, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas

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

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in the references in Section 1.4. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) into a web browser rather than using Ctrl-Click to access them.

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) employees and 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 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 GSA. An individual's access privileges to certain IT resources may need to be maintained, reduced, or expanded based upon changes in their work responsibilities. For example, someone changing organizations within 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 GSA or vendors/contractors.

Note: This guide assumes the existence of a documented access authorization process within Services and Staff offices (S/SO), and Regional offices, in accordance with GSA CIO-IT Security-01-07, "Access Control." This guide also assumes that records reflecting the resources to which access has been authorized are kept-up to date to ensure privileges may be expediently revoked.

The termination and transfer practices identified in this guide must be followed by all GSA Federal employees and contractors involved in operating, maintaining, and using GSA information systems. 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). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

1.1 Purpose

The purpose of this document is to provide guidance on standard procedures for modifying, disabling, or removing access to GSA logical and physical resources when GSA employees or contractors terminate their employee relationship with GSA or transfer to another position within GSA. The processes described in this guide are designed to help ensure appropriate personnel are notified and take appropriate action in a timely manner when access requirements change due to 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 information systems and information. Per CIO 2100.1, a GSA information system is an information system:

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

1.3 Policy

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.

> *d. Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of all user accounts shall be completed annually to ensure the continued need for system access*
>
> *e. Disabling and removal of user accounts supporting account management processes, to include:*
>
> > *(1) Supervisors being responsible for coordinating and arranging system access termination for all departing or resigning personnel, both Federal employees and contractors.*
> > *(2) Account removal being initiated by a user's supervisor, COR, or through the review of information provided by the OCISO (e.g., separation lists, role revisions). Data and*

system owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources.
(3) Termination and transfer procedures being incorporated into the authorization process for all information systems IAW GSA CIO-IT Security-03-23.

f. Request, including modifications, and approval routing in support of account management processes must ensure:

(1) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;
(2) Users complete and send access requests to their supervisor or COR, not directly to the data or system owner;
(3) Access requests are routed to the data or system owner by a user's supervisor, COR, ISSO, ISSM, director, or designated official.

l. Termination and transfer procedures must be followed for all information systems IAW GSA CIO-IT Security-03-23.

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

1.4 References

Note: GSA updates its IT security policies and procedural guides on independent biennial cycles which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws, Regulations, and Guidance:

- CSF, Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity"
- EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- Federal Information Processing Standard (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 Guidance:

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"
- GSA Order HRM 7800.14, "Pre-Exit Clearance Procedures for All Separations"
- Off Boarding Employees – website with instructions on offboarding employees
- GSA Form 1655, Pre-Exit Clearance Checklist
- GSA IT Service Desk

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 InSite page.

- CIO-IT Security-01-07, "Access Control (AC)"
- CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk"
- CIO-IT Security-12-64, "Physical and Environmental Protection"
- GSA Control Tailoring Workbook (template)

2 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.

2.1 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.

2.2 Information Systems 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.

2.3 Information Systems 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.

2.4 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.

2.5 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.

2.6 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.

2.7 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.

2.8 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.

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. This applies to GSA employees, contractors, and employees or contractors of other organizations using IT resources on behalf of GSA.

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.

The GSA employee will obtain and begin completing the 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 Service Catalog 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 within the specified timeframe in Section 6.1 for terminating or Section 6.2 for transferring.

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. The ISSM then confirms to OCISO that the removal of access has been verified.

Note: There is no corresponding monthly process from the OCISO for:

- Individuals who are contractors or employees of other organizations using IT resources on behalf of GSA; or
- 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 access privileges are required by CIO 2100.1. 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:
   a. Each named user is still associated with GSA; and
   b. Authorization privileges are appropriate to each 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-4 and PS-5 Controls

The PS-4 and PS-5 controls from NIST 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 italics offset by brackets in the control text, followed by GSA’s implementation guidance. PS-4 and PS-5 are applicable at all FIPS 199 security categorization levels. PS-4(2) is only applicable for FIPS 199 High level systems.

Questions regarding these controls should be directed to the GSA Office of the Chief Information Security Officer (OCISO) at ispcompliance@gsa.gov.

6.1 PS-4 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:

(2) Personnel Termination | Automated Actions. Use [*GSA S/SO or Contractor defined automated mechanisms*] to [*notify supervisors and ISSMs/ISSOs of individual termination actions; disable access to system resources*].

GSA Implementation Guidance: Control PS-4 is applicable at all FIPS 199 levels. Enhancement PS-4(2) is applicable at the FIPS 199 High level. PS-4 and PS-4(2) are Hybrid Controls for Federal systems, shared between the GSA Enterprise, Platforms and Hosted Applications, and Hybrid Controls for Contractor systems shared between the GSA Enterprise policies and the Contractor.

Common Control Implementation: Disabling information system access is initiated and facilitated by the supervisor/CO/COR of an individual. Retrieval of all information system-related property which includes HSPD-12 cards, authentication tokens (USB devices for privileged access), laptops, etc. is a common control provided by the Office of Enterprise Infrastructure (IDI) and the Office of Mission Assurance (OMA) and facilitated by the supervisor. 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. As part of the offboarding of users, the supervisor/CO/COR is responsible for coordinating the transfer of organizational information and information systems, as appropriate, to appropriate individuals.

System Specific Expectations: The supervisor/CO/COR is responsible for notifying the appropriate ISSMs/ISSOs of a user's off-boarding so they can take appropriate action at a system/application level.

For enhancement PS-4(2)—applicable to FIPS 199 High systems, the automated mechanisms used to notify personnel and disable access to system resources must be approved by GSA OCISO and annotated as such in the GSA Control Tailoring Workbook for the system.

Additional Contractor System Considerations: Vendors/Contractors must ensure individuals working/using GSA information systems comply with the GSA policies and guides regarding personnel termination processes and procedures. They may supplement this process by conducting their own personnel termination processes.

For enhancement PS-4(2)—applicable to FIPS 199 High systems, the automated mechanisms used to notify personnel and disable access to system resources must be approved by GSA OCISO and annotated as such in the GSA Control Tailoring Workbook for the system.

6.2 PS-5 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. Notifies [*supervisor and/or ISSMs/ISSOs*] within [*14 days of personnel transfer*].

Control Enhancements: None.

GSA Implementation Guidance: Control PS-5 is applicable at all FIPS 199 levels. PS-5 is a Hybrid Control for Federal systems, shared between the GSA Enterprise, Platforms and Hosted Applications, and a Hybrid Control for Contractor systems shared between the GSA Enterprise policies and the Contractor.

Common Control Implementation: Review of ongoing operational need for current logical and physical access by individuals is initiated and facilitated by the individual's supervisor/CO/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.

System Specific Expectation: The supervisor/CO/COR is responsible for notifying the appropriate ISSMs/ISSOs of a user's transfer so they can take appropriate action at a system/application level.

Additional Contractor System Considerations: Vendors/Contractors must have individuals working/using GSA information systems comply with the GSA policies and guides regarding personnel transfer processes and procedures. They may supplement this process by conducting their own personnel transfer processes.

7 Summary

Termination and transfer procedures are beneficial to ensure the security of 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.

GSA employees, contractors, and other organizations using IT resources on behalf of GSA must adhere to 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.