GSA CIO Policies

The following GSA CIO Policies are relevant to contracts that may involve access to or use of GSA information or information technology (IT) resources. Not all policies apply to all contracts. Contracting activities review these policies with requiring activities and program officials to determine which apply.

The policies can be found at http://www.gsa.gov/directives.

I. GSA CIO Policies, Required For All Contracts Involving GSA IT Resources or Sensitive Data

1. CIO P 1878.1 GSA Privacy Act Program
2. CIO P 1878.2 Conducting Privacy Impact Assessments (PIAs) in GSA
3. CIO P 2100.1 GSA Information Technology (IT) Security Policy
4. CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
5. CIO 9297.1 GSA Data Release Policy
6. CIO 9297.2 GSA Information Breach Notification Policy

II. GSA CIO Policies, Required When Inside a GSA Building or Inside a GSA Firewall

1. CIO P 2100.2 GSA Wireless Local Area Network (LAN) Security
2. CIO 2100.3 Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities
3. CIO 2104.1A GSA Information Technology IT General Rules of Behavior
4. CIO P 2181.1 GSA Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification and Credentialing
5. CIO 2182.2 Mandatory Use of Personal Identity Verification (PIV) Credentials
6. ADM P 9732.1D Suitability and Personnel Security

III. GSA CIO Policies, Required When Applicable

1. CIO 2102.1 Information Technology (IT) Integration Policy
2. CIO 2105.1 GSA Section 508: Managing Information and Communications Technology (ICT) for Individuals with Disabilities

3. CIO 2106.1 GSA Social Media Policy
4. CIO 2107.1 Implementation of the Online Resource Reservation Software
5. CIO 2108.1 Software License Management
6. CIO 2160.2 GSA Electronic Messaging and Related Services
7. CIO 2160.4 Provisioning of Information Technology (IT) Devices
8. CIO 2162.1 Digital Signatures
9. CIO P 2165.2 GSA Telecommunications Policy
10. CIO 01-02 GSA IT Security Procedural Guide: Incident Response
11. CIO 04-26 GSA IT Security Procedural Guide: FISMA Implementation
12. CIO 06-29 GSA IT Security Procedural Guide: Contingency Planning
13. CIO 06-30 GSA IT Security Procedural Guide: Managing Enterprise Risk, Security Assessment and Authorization, Planning, and Risk Assessment
14. CIO 07-35 GSA IT Security Procedural Guide: Web Application Security
15. CIO 09-44 GSA IT Security Procedural Guide: Plan of Action and Milestones (POA&M)
16. CIO 09-48 GSA IT Security Procedural Guide: Security Language for IT Acquisition Efforts
17. CIO 11-51 GSA IT Security Procedural Guide: Conducting Penetration Test Exercises
18. CIO 12-66 GSA IT Security Procedural Guide: Information Security Continuous Monitoring Strategy
19. CIO 12-67 GSA IT Security Procedural Guide: Securing Mobile Devices and Applications
20. CIO 14-69 GSA IT Security Procedural Guide: SSL/TLS Implementation