

Internal Revenue Service (IRS)  
Office of Safeguards



New Publication 1075  
Computer Security Changes

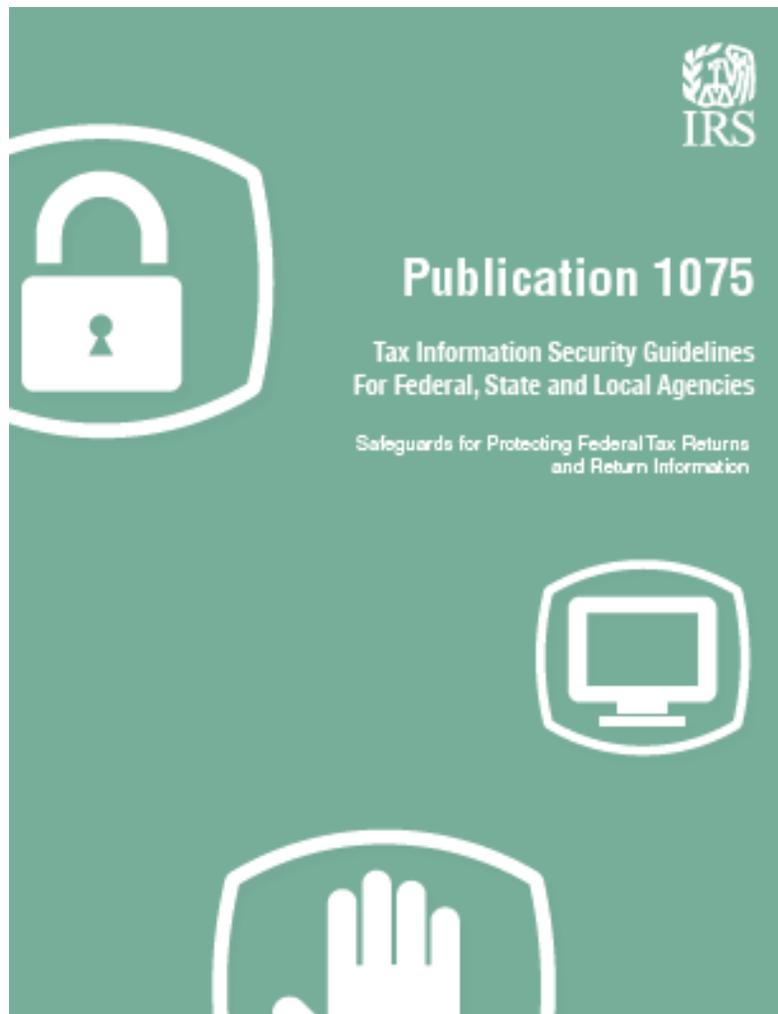
Effective January 2014

Version 0.9

February 18, 2014

## Introduction

The IRS Publication 1075 was updated and released with an effective date of January 1, 2014. This document identifies highlights which impact agency safeguarding procedures to protect information systems that receive, process, store or transmit FTI. Changes identified are a result of new guidance issued in NIST SP 800-53 Revision 4, IRS IT Security Policy, Safeguards Technical Memo requirements and feedback provided to the IRS Office of Safeguards in 2013. The new Publication 1075 also provides additional guidance on targeted topics with the goal of increasing awareness and clarity on requirements to protect FTI.



## IRS Publication 1075 Computer Security Changes

ID	Pub1075 Old Req.	Pub1075 New Requirement (Effective Jan. 2014)	Section	Change Type	Comments
1	None	NIST SP 800-53 Control Enhancements (CE) are added to the Publication 1075. Identified by CE indicator. Only significant and new CE requirement additions are noted in this list of changes.	Described in 9.1 and impacts all of Section 9.	New	As already required in existing SCSEM and technical memo releases, the majority of CE requirements have already been in place.
2	Frequency was not specified	Policy documentation required to be reviewed and updated at least every 3 years.	All Policy Sections (X-1)	Refinement	SCSEMs required annual review & updates but it was never clearly defined in the Pub1075
3	Frequency was not specified	Procedure documentation required to be reviewed and updated at least annually	All Procedure Sections (X-1)	Refinement	SCSEMs required annual review & updates but it was never clearly defined in the Pub1075
4	Frequency was not specified	AC-2: Review accounts for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts	9.3.1.2	Refinement	
5	None	AC-2: The information system must automatically disable inactive accounts after 120 days of inactivity.	9.3.1.2	New	Not to be confused with password expiration requirements.
6	None	AC-6: Require that users of information system accounts, or roles, with access to FTI, use non-privileged accounts or roles when accessing non-security functions.	9.3.1.6	New	
7	Frequency was not specified	AC-7: Enforce a limit of three consecutive invalid logon attempts by a user during a 120-minute period.	9.3.1.7	Refinement	
8	Explicit action was not specified.	AC-8: Systems must retain warning banners on the screen until users acknowledges the usage conditions and take explicit actions to log on to or further access the information system.	9.3.1.8	Refinement	
9	None	AC-17: The agency must Authorize and document the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs only.	9.3.1.12	Refinement	Particularly noteworthy considering the number of agencies that are allowing remote access.
10	None	AC-18: New wireless network intrusion detection monitoring requirement.	9.3.1.13	New	
11	None	AC-19: New requirements added for mobile device security (e.g. purging data after 10 unsuccessful device logon attempts).	9.3.1.14	New	
12	None	AC-20: Explicit approval is now required for access to FTI from external information systems or devices	9.3.1.15	Refinement	

## IRS Publication 1075 Computer Security Changes

ID	Pub1075 Old Req.	Pub1075 New Requirement (Effective Jan. 2014)	Section	Change Type	Comments
13	None	AC-22: New requirements on controlling data posted onto publicly accessible systems to ensure inadvertent posting of FTI is avoided.	9.3.1.17	New	
14	None	AT-2: Added requirement for including insider threat awareness in agency training material.	9.3.2.2	New	
15	General audit event requirements for all platforms.	AU-2: Simplified audit logging requirements.	9.3.3.3	Refinement	Agency is responsible for implementing auditing per specific technology SCSEM requirements.
16	None	AU-5: Added requirement for audit record storage capacity notifications.	9.3.3.6	New	
17	None	AU-6: Added proactive auditing recommendations (not required at this time).	9.3.3.7	New	
18	None	AU-6: Added requirement that the agency must authorize access to manage audit functionality and restrict the ability to modify or delete audit log entries.	9.3.3.10	New	
19	None	AU-16: Added new cross-agency auditing requirements.	9.3.3.13	New	
20	None	CA-3: Added "deny-all" and "allow-by-exception" requirement for allowing FTI systems to connect to external systems.	9.3.4.3	New	
21	Required for alternate work locations or via agency's web portal.	IA-2: Multi-factor authentication is required for all remote network access to privileged and non-privileged accounts. One of the factors must be provided by a device separate from the system gaining access.	9.3.7.2	New	
22	Minimum lifetime was 15 days. Password reuse was 6 generations.	IA-5: Password requirements have been detailed and updated. - Minimum password lifetime restriction is now 1 day. - Password reuse must be prevented for 24 generations.	9.3.7.5	Refinement	
23	None	IR-9: New requirement added for information spillage response.	9.3.8.9	New	
24	None	PL-2: Revised SSR requirements are described.	9.3.12.2	Refinement	
25	None	PL-4: Updated rules of behavior requirements to include explicit restrictions on the use of social media/networking sites and posting agency information on public websites.	9.3.12.2	Refinement	

## IRS Publication 1075 Computer Security Changes

ID	Pub1075 Old Req.	Pub1075 New Requirement (Effective Jan. 2014)	Section	Change Type	Comments
26	Quarterly	RA-5: The frequency for performing vulnerability scanning is now monthly for all systems and when new vulnerabilities potentially affecting the system/applications are identified and reported.	9.3.14.3	Refinement	
27	None	SA-22: New requirement on unsupported systems.	9.3.15.10	New	
28	None	SC-7: New requirement to limit the number of external network connections to FTI systems.	9.3.16.5	New	
29	None	SC-7: New requirement for the agency to implement a secure managed interface for external telecommunication services.	9.3.16.5	New	
30	None	SC-8: Provided additional guidance on protecting the transmission confidentiality and integrity of FTI. Optional protections from encrypting FTI focuses on physical protections vs. virtual.	9.3.16.3	Refinement	
31	Previous 15 minutes.	SC-10: Network disconnect time is now 30 minutes.	9.3.16.7	Refinement	Note difference from session termination (AC-12) req.
32	No specific guidance provided.	SC-28: New guidance provided to protect FTI at rest.	9.3.16.15	Refinement	
33	None	SI-2 and SI-3 : New guidance provided that the agency must centrally manage the flaw remediation and malicious code protection process.	9.3.17.3	Refinement	
34	None	SI-4: New requirements added for system monitoring (e.g. Host Intrusion Prevention Systems, monitoring and notification)	9.3.17.4	New	
35	None	SI-16: New control to protect system memory from unauthorized code execution.	9.3.17.10	New	
36	None	Additional Computer Security Requirements included on the following topics: <ul style="list-style-type: none"> <li>- Cloud Computing</li> <li>- Media Sanitization</li> <li>- Mobile Devices</li> <li>- Network Protections</li> <li>- Storage Area Networks</li> <li>- System Component Inventory</li> <li>- Virtual Desktop Infrastructure</li> <li>- Virtualization</li> <li>- Web Browser Security</li> <li>- Wireless Networking</li> </ul>	9.4	New	Requirements are not new. These updates to Publication 1075 are made based on existing technical memo released on the Safeguards IRS.gov website.
37	Exhibit 4 (old)	Consolidated into NIST Moderate Risk Controls into all of Section 9.	9	Consolidation	
38	Exhibit 8 (old)	Consolidated Password Management Guidelines into Section 9.3.7.5 (IA-5)	9.3.7.5	Consolidation	

## IRS Publication 1075 Computer Security Changes

ID	Pub1075 Old Req.	Pub1075 New Requirement (Effective Jan. 2014)	Section	Change Type	Comments
39	Exhibit 9 (old)	Consolidated System Audit Management Guidelines into Section 9.3.3 (Audit Control Family)	9.3.3	Consolidation	
40	Exhibit 10 (old)	Consolidated Encryption Standards into multiple Sections addressing IA-7, SC-8, C-12, SC-13 and SC-28	Multiple Sections	Consolidation	