Publication 1075 *Tax Information Security Guidelines for Federal, State and Local Agencies*

Comparison of 2021 version to 2016 version

The purpose of this table is to provide a comparison and highlight changes made to Publication 1075 *Tax Information Security Guidelines for Federal, State, and Local Agencies.* The table focuses on changes that impact local district operations; it is not inclusive of all changes made to Publication 1075 - see *Highlights for November 2021 Revision* for additional information. Please note, Publication 1075 *Tax Information Security Guidelines for Federal, State, and Local Agencies* contains extensive changes to computer security requirements and the Division of Child Support Services (DCSS) strongly recommends that local district staff work with IT and information security resources to ensure compliance with all requirements.

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
1.8.1.1 Data Incident	Pg. 34-35.	Data Incident: A data incident is an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. Incidental and inadvertent accesses are considered data incidents. An incident involving the loss or theft of an IRS asset containing FTI, or the loss or theft of a physical document that includes FTI, or the inadvertent disclosure of FTI, is known as a data breach. See the Data Breach definition below. Often, an occurrence may be first identified as an incident, but later identified as a data breach once it is determined that the incident involves FTI. This is often the case with a lost or stolen laptop or electronic storage device.	N/A	N/A	N/A	N/A
1.8.1.2 Data Breach	Pg. 34-35.	Data Breach: A data breach is a type of incident involving a loss, theft, or inadvertent disclosure of FTI. A data breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any a similar occurrence where: • a person other than an authorized user accesses or potentially accesses FTI or, • an authorized user accesses or potentially accesses FTI for any unauthorized purpose. A data breach is not limited to an occurrence where a person other than an authorized user potentially accesses FTI using a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A data breach may also include the loss or theft of physical documents that include FTI and portable electronic storage media that store FTI, the inadvertent disclosure of FTI on a public website, or an oral disclosure of FTI to a person who is not authorized to receive that	N/A	N/A	N/A	N/A

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
		information. It may also include an authorized user accessing FTI for an unauthorized purpose. Some common examples of a data breach include: • A laptop or portable storage device storing FTI is lost or stolen. • An email containing FTI is inadvertently sent to the wrong person. • A box of documents with FTI is lost or stolen during shipping. • An unauthorized third party overhears agency employees discussing FTI. • A user with authorized access to FTI sells it for personal gain or disseminates it. • An IT system that maintains FTI is accessed by a malicious actor. • FTI is posted inadvertently on a public website.				
N/A	N/A	N/A	Section 3.1 General	Pg. 15.	The agency must establish, maintain, and update at least annually, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing FTI. Provide each update of the FTI inventory to the Chief Information Officer or information security official at least annually to support the establishment of information security requirements for all new or modified information systems containing FTI.	The district is no longer required to maintain and or update an inventory list.
Section 2.B.2 Minimum Protection Standards	Pg. 44-45.	Per NIST guidelines, policies and procedures must be developed, documented, and disseminated, as necessary, to facilitate implementing physical and environmental protection controls. Multifunction Devices (MFDs) or High-Volume Printers must be locked with a mechanism to prevent physical access to the hard disk or meet MPS. For additional guidance, see NIST Control PE-3, Physical Access Control.	N/A	N/A	N/A	Districts are required to have Multifunction Devices (MFDs) or High-Volume Printers that meet the MPS barriers. Districts should consider building or purchasing lockable containers to ensure compliance. Districts are encouraged to consult with information Security resources for additional guidance.
Section 2.B.3.2 Authorized Access List	Pg. 46.	To facilitate the entry of employees/vendor/contractor/non-agency personnel who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area, an Authorized Access List (AAL) can be maintained so long as MPS are enforced. See Section 2.B.2, Minimum Protection Standards. The AAL must contain the following: • Name of employee/vendor/contractor/non-agency personnel • Agency or department name • Name and phone number of the agency POC authorizing access	Section 4.3.1 Use of Authorized Access List	Pg. 20.	An AAL for Vendor/Non-Agency personnel was recommended for staff who have a frequent and continuing need to enter a restricted area. This AAL was required to be reviewed monthly. An AAL for Agency personnel was recommended for staff who have a frequent and continuing need to enter a restricted area. This AAL was required to be reviewed annually, or when employee access changes.	The Vendor/Non-Agency AAL and the Agency AAL may now be combined into one list. However, the AAL(s) must be reviewed monthly or upon the occurrence or potential indication of an event such as a possible security breach or personnel change.

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
		• Address of agency/vendor/contractor • Purpose and level of access AAL must be reviewed monthly or upon the occurrence or potential indication of an event such as a possible security breach or personnel change.				
Section 2.B.3.3 Controlling Access to Areas Containing FTI	Pg. 47.	The agency must maintain a policy addressing the issuance of appropriate authorization credentials, including badges, identification cards, or smart cards. The agency must establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.	Section 4.3.2 Controlling Access to Areas Containing FTI	Pg. 21.	The agency shall issue appropriate authorization credentials, including badges, identification cards, or smart cards. In addition, a list shall be maintained that identifies those individuals who have authorized access to any systems where FTI is housed. Access authorizations and records maintained in electronic form are acceptable. Whenever cleaning and maintenance personnel are working in restricted areas containing FTI, the cleaning and maintenance activities must be performed in the presence of an authorized employee.	The district must now implement a policy and process that addresses authorization credentials.
Section 2.B.4.1 Security During Office Moves	Pg. 48.	When an office must move to another location, plans must be made to protect and account for all FTI properly. FTI must be in locked cabinets or sealed packing cartons while in transit. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents. FTI must remain in the custody of an agency employee and accountability must be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move.	N/A	N/A	N/A	N/A
Section 2.B.7 Alternate Work Sites	Pg. 49.	If the confidentiality of FTI can be adequately protected, telework sites such as employees' homes or other non-traditional work sites can be used. FTI remains subject to the same safeguard requirements and the highest level of attainable security. All the requirements of Section 2.B.5, Physical Security of Computers, Electronic and Removable Media, apply to alternate work sites.	Section 4.7 Telework Location	Pg. 24.	The agency must conduct periodic inspections of alternative work sites during the year to ensure that safeguards are adequate. The results of each inspection shall be fully documented, and the IRS reserves the right to visit alternative worksites while conducting safeguard reviews.	Periodic inspections of alternative work sites are no longer required.
Section 2.C.1 General	Pg. 50.	Auditing controls, with the capability to generate records, to detect browsing within all systems that receive, process, store, access, protect and/or transmit FTI (i.e., TDS, case management systems, etc.) must be implemented. See NIST Sections AU-6 Audit Review, Analysis and Reporting, AU-7, Audit Reduction and Report Generation, and AU-12, Audit Generation, for additional requirements.	Section 5.1 General	Pg. 26.	Agencies are required by IRC 6103(p)(4)(C) to restrict access to FTI only to persons whose duties or responsibilities require access (see Exhibit 2, USC Title 26, IRC 6103(p)(4), and Exhibit 4, Sanctions for Unauthorized Disclosure). To assist with this requirement, FTI must be clearly labeled "Federal Tax Information" and handled in such a manner that it does not become misplaced or available to unauthorized personnel. Additionally, warning banners advising of safeguarding	If FTI is stored locally, the auditing controls found in Section 2.C.1, are applicable.

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
					requirements must be used for computer screens (see Exhibit 8, Warning Banner Examples). To understand the key terms of unauthorized disclosure, unauthorized access, and need-to-know, see Section 1.4, Key Definitions.	
Section 2.C.2 Policies and Procedures	Pg. 51.	The new section provides a reference list of policies and procedures that must be developed to comply with federal requirements.	N/A	N/A	N/A	Please note the following policies/procedures are new requirements: <u>Insider Threat Program</u>– See NIST Control PM-12, Insider Threat Program The policy/procedures must address an insider threat program that includes a cross-discipline insider threat incident handling team and designate a senior official as the responsible individual to implement and provide oversight for the program. <u>Privacy Program Plan3</u> – See NIST Control PM-18, Privacy Program Plan A privacy program plan is a formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program and the program management and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
Section 2.C.3 Background Investigation Minimum Requirements	Pg. 53.	State agencies must ensure a reinvestigation is conducted within five (5) years from the date of the previous background investigation for each employee, contractor, and sub-contractor requiring access to FTI.	Section 5.1.1 Background Investigation Minimum Requirements	Pg. 26, 27.	State agencies must ensure a reinvestigation was conducted within 10 years from the date of the previous background investigation for each employee and contractor requiring access to FTI.	The district background investigation policy must be updated and submitted to OTDA for approval.

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
Section 2.C.3.1 Background Investigation Requirement Implementation	Pg. 54.	Agencies must establish a written background investigation policy that conforms to the standards of Section 2.C.3. Agencies must also identify all employees, contractors, and sub-contractors who currently have access to FTI and have not completed the required personnel security screening and initiate a background investigation that meets these standards. Agencies must initiate a background investigation for all newly hired employees, contractors, and sub-contractors who will require access to FTI to perform assigned duties. All adjudications must be done by the agency, or another state agency delegated to perform, such as an Office of Administration or HR agency. Federal agencies that completed a Moderate-Risk Background Investigation (MBI) or higher for individuals with access to FTI, before the October 2014 implementation date of the FIS Tier 2 standard investigation, have met the minimum standard and no further investigation is needed so long as reinvestigation is timely scheduled. Individuals granted access to FTI based on a National Agency Check with Inquiries (NACI) is not sufficient and a Tier 2 investigation must be initiated for continued access to FTI.	Section 5.1.2 Implementing the Background Investigation Requirement	Pg. 28.	The requirements of Section 5.1.1 pertaining to initial and periodic background investigations for individuals before authorizing access to FTI is effective upon date of this publication. Implementation of the new standards, including the development of written policies and verification that all individuals with access to FTI have an appropriate level of investigation and initiating new required investigations to comply with the requirement may occur within one year.	The one-year implementation period has been removed.
Section 2.C.4.1 Personnel Transfer	Pg. 54.	When reassignments or transfers of individuals are permanent or of such extended durations certain actions are warranted. Agencies must define actions appropriate for these types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example, returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and access to official records to which individuals had access at previous work locations and in previous system accounts. See NIST Control PS-5, Personnel Transfer.	Section 9.3.13.5 Personnel Transfer	Pg. 89-90.	In the 2016 Publication 1075, examples of actions that need to be taken are not provided. a. Review and confirm the ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the agency b. Initiate transfer or reassignment actions following the formal transfer action. c. Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer. d. Notify designated agency personnel, as required.	Districts must review and update existing policies related to personnel transfers as needed.
2.C.4.2 Personnel Sanctions	Pg. 55.	Agencies must document in policy and procedure a formal sanctions process for individuals failing to comply with established information security policies and procedures. Agencies must notify designated agency personnel within 72 hours when a formal employee sanction process is initiated, identifying the individual sanctioned and any required administrative actions. See NIST Control PS-8, Personnel Sanctions. When the formal sanction is a proposed disciplinary or adverse action involving unauthorized access or disclosure	Section 9.3.13.8	Pg. 91.	The agency must: a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures. b. Notify designated agency personnel when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Districts must now notify designated agency personnel within 72 hours when a formal employee sanction process is initiated and provide written notification to the designated person that the sanctions process has been initiated.

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
		of FTI, the agency must provide written notification to the taxpayer whose FTI was subject to unauthorized access or disclosure. The required written notification must include the date the unauthorized access or disclosure of FTI occurred and the rights of the taxpayer under IRC § 7431 (see Section 1.8.5, Incident Response Notification to Impacted Individuals).				
Section 2.C.4.3 Personnel Termination	Pg. 55.	In personnel termination situations, certain actions are required. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, agencies must consider disabling the system accounts of individuals that are being terminated before the individuals are notified. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. The system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. See NIST Control PS-4, Personnel Termination.	Section 9.3.13.4 Termination	Pg. 90.	The agency, upon termination of individual employment must: a. Disable information system access b. Terminate/revoke any authenticators/credentials associated with the individual c. Conduct exit interviews, as needed d. Retrieve all security-related agency information system–related property e. Retain access to agency information and information systems formerly controlled by the terminated individual f. Notify agency personnel upon termination of the employee	Exit interviews are now required to ensure that terminated individuals understand the security constraints imposed by being a former employee.
Section 2.C.7 Offshore Operations	Pg. 57.	FTI cannot be accessed by agency employees, agents, representatives, contractors, or subcontractors located outside of the legal jurisdictional boundary of the United States (outside of the United States, its territories, embassies, or military installations). FTI must not be received, processed, stored, accessed, or transmitted to (IT) systems located offshore nor may FTI be sent offshore for disposal. Systems containing FTI must be located, operated, and maintained by personnel physically located within the United States (this prohibits foreign remote maintenance, foreign call centers, help desks, and the like) and should follow Publication 1075 requirements including the Background Investigation Requirements in Section 2.C.3. Some agencies may need their employees to travel internationally for business purposes. As such, agencies must develop procedures to follow during foreign travel. When agency employees travel abroad, they must not: • Bring IT equipment containing stored FTI (e.g., laptop computers, tablets, phones, removable media); or • Access agency systems that receive, process, store, protect and/or transmit FTI. During international travel, batteries of agency-managed or	N/A	N/A	N/A	N/A

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
		Bring Your Own Device (BYOD) mobile devices and laptops must be removed from battery-powered mobile devices and stored separately from the device when left unattended. SIM cards must be removed and stored separately from devices that employ them when entering non-U.S. customs. Once agency employees return from abroad, agencies need to ensure the continued security of networks where FTI resides. Agencies must sanitize all devices taken abroad before allowing them to connect to their trusted network. Additionally, agencies must disable wireless connectivity options until devices have been sanitized and may wish to provide additional security training for employees traveling abroad.				
Section 2.C.9 Service Level Agreements (SLA)	Pg. 58-59.	Agencies using support functions, including, but not limited to, consolidated data centers, shared print facilities, and disaster recovery sites, must implement appropriate controls to ensure the protection of FTI. This includes a service level agreement (SLA) between the agency authorized to receive FTI and support functions. The SLA must cover the following: • The agency with authority to receive FTI is responsible for ensuring the protection of all FTI received. The state support function shares responsibility for safeguarding FTI. • The Exhibit 7 language must be included in the SLA between the recipient agency and support functions and in all contracts involving contractors or sub-contractors hired by the state support function. • The SLA provides written notification to the state support function's management that they are bound by the provisions of Publication 1075, relative to protecting all FTI within their possession or control. • The SLA shall detail the IRS's right to inspect state support function facilities and operations receiving, processing, storing, accessing, protecting and/or transmitting FTI under this agreement to assess compliance with requirements defined in IRS Publication 1075. The SLA shall specify that IRS's right of inspection includes the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. • The SLA shall detail the state support function's responsibilities to address corrective action recommendations to resolve findings of noncompliance identified by IRS inspections.	Section 5.4.2.2 Consolidated Data Centers	Pg. 32-33.	Agencies using consolidated data centers must implement appropriate controls to ensure the protection of FTI, including a service level agreement (SLA) between the agency authorized to receive FTI and the consolidated data center. The SLA must cover the following: • The agency with authority to receive FTI is responsible for ensuring the protection of all FTI received. The consolidated data center shares responsibility for safeguarding FTI. • The SLA provides written notification to the consolidated data center management that they are bound by the provisions of Publication 1075, relative to protecting all FTI within their possession or control. • The SLA shall detail the IRS' right to inspect consolidated data center facilities and operations accessing, receiving, storing, or processing FTI under this agreement to assess compliance with requirements defined in IRS Publication 1075. The SLA shall specify that IRS' right of inspection includes the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. • The SLA shall detail the consolidated data center's responsibilities to address corrective action recommendations to resolve findings of noncompliance identified by IRS inspections. • The agency will conduct an internal inspection of the consolidated data center every 18 months, as described in Section 6.4, Internal Inspections. Multiple agencies sharing a consolidated data center may partner together to conduct a	The IRS changed the name of this section from Consolidated Data Centers to Service Level Agreements (SLA). In addition, this now includes shared print facilities and disaster recovery sites. The IRS now requires a formal sanction process for individuals covered by the SLA for failure to comply with FTI policies and procedures.

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
		• The agency will conduct an internal inspection of the state support function every 18 months, as described in Section 2.D.3, Internal Inspections. Multiple agencies sharing a state support function such as a consolidated data center may partner together to conduct a single, comprehensive internal inspection. However, care must be taken to ensure agency representatives do not gain unauthorized access to other agencies' FTI during the internal inspection. • The employees from the state support function with access to or use of FTI, including system administrators and programmers, must: 1. Meet the background check requirements defined in Background Investigation Minimum Requirements and 2. Receive disclosure awareness training and sign a confidentiality statement, prior to initial access to or use of FTI, as well as annually thereafter. These provisions also extend to any contractors or subcontractors hired by the state support function that have authorized access to or use of FTI. • The specific data breach incident reporting procedures for all state support function employees, contractors, and sub-contractors must be covered. The required disclosure awareness training must include a review of these procedures. • Responsibilities must be identified for coordination of the 45-day notification of the use of contractors or sub-contractors with access to FTI. • Require a formal sanction process for individuals covered by the SLA for failing to comply with established FTI security policies and procedures. Notification of designated agency personnel is required within 72 hours when the formal sanction is a proposed disciplinary or adverse action involving unauthorized access or disclosure of FTI and must include the date the unauthorized access or disclosure of FTI occurred. Generally, consolidated data centers are operated either by a separate state agency (e.g., Department of Information Services) or by a private contractor or sub-contractor. If an agency is considering transitioning to either a state-owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision making or implementation planning process. The purpose of these discussions is to ensure the agency remains compliant with safeguarding requirements during the transition to the consolidated data center.			single, comprehensive internal inspection. However, care must be taken to ensure agency representatives do not gain unauthorized access to other agencies' FTI during the internal inspection. • The employees from the consolidated data center with access to or use of FTI, including system administrators and programmers, must: 1. Meet the background check requirements defined in IRS Publication1075 and 2. Prior to initial access to or use of FTI, as well as annually thereafter, receive disclosure awareness training and sign a confidentiality statement. These provisions also extend to any contractors hired by the consolidated data center that have authorized access to or use of FTI. • The specific data breach incident reporting procedures for all consolidated data center employees and contractors must be covered. The required disclosure awareness training must include a review of these procedures. • The Exhibit 7 language must be included in the contract between the recipient agency and the consolidated data center, including all contracts involving contractors hired by the consolidated data center. • Responsibilities must be identified for coordination of the 45-day notification of the use of contractors or subcontractors with access to FTI. Generally, consolidated data centers are either operated by a separate state agency (e.g., Department of Information Services) or by a private contractor. If an agency is considering transitioning to either a state-owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision making or implementation planning process. The purpose of these discussions is to ensure the agency remains compliant with safeguarding requirements during the transition to the consolidated data center.	

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
Section 2.F.4 Other Precautions	Pg. 79-80.	FTI must never be disclosed to an agency's agents, contractors, or sub-contractors during disposal without legal authorization and destruction must be witnessed by an agency employee. The Department of Justice, state tax agencies, and SSA may be exempted from the requirement of having agency personnel witness destruction by a contractor or sub-contractor. If a contractor or sub-contractor is used: • The contract must contain safeguard language in Exhibit 7a and 7b, Safeguarding Contract Language as appropriate to the contract to ensure the protection of FTI. • Destruction of FTI must be certified by the contractor or sub-contractor when not witnessed by an agency employee. • It is recommended that the agency periodically observe the process to ensure compliance with the security of FTI until it reaches a non-disclosable state and that an approved destruction method is utilized. If the agency has legal authority to disclose FTI to a disposal contractor or sub-contractor and chooses one that is National Association for Information Destruction (NAID) certified, the agency will not be 79 required to complete an internal inspection every 18 months of that facility. However, the agency must annually validate and maintain the most recent copy of the NAID certification.	Section 8.4 Other Precautions	Pg. 54	FTI must never be disclosed to an agency's agents or contractors during disposal without legal authorization and destruction must be witnessed by an agency employee. The Department of Justice, state tax agencies, and SSA may be exempted from the requirement of having agency personnel witness destruction by a contractor. If a contractor is used: • The contract must contain safeguard language in Exhibit 7, Safeguarding Contract Language as appropriate to the contract to ensure the protection of FTI. • Destruction of FTI must be certified by the contractor when not witnessed by an agency employee. • It is recommended that the agency periodically observe the process to ensure compliance with security of FTI until it reaches a non-disclosable state and that an approved destruction method is utilized. • If the agency has legal authority to disclose FTI to a disposal contractor and chooses one that is National Association for Information Destruction (NAID) certified, the agency will not be required to complete an internal inspection every 18 months of that facility. However, it must maintain a copy of, and periodically validate the NAID certification.	The district is required to annually confirm that a valid NAID certification exists for any destruction or disposal contractor.
Section 3.3.5 Multi-Function Devices (MFDs) and High-Volume Printers	Pg. 85.	If the agency determines FTI is not permitted to be printed, a written policy must be established and distributed to: a. Prohibit FTI from being printed b. Clearly state the actions that will be taken if FTI is inadvertently printed If the agency determines FTI is permitted to be printed, a written policy must be established and distributed to: a. Prohibit printing FTI to printers outside of the agency's internal network. b. Ensure printed FTI is sent only to authorized printers (e.g., multifunction devices, standalone printers, high-volume printers) c. Require adequate labeling and protection of all printed FTI Additionally, the agency must ensure MFDs and HVPs are configured securely and included in the agency's FTI inventory.	Section 9.4.9 Multi-Functional Devices and High-Volume Printers	Pg. 112.	To use FTI in a multi-functional device (MFD) or High-Volume Printer, the agency must meet the following requirements: a. The agency should have a current security policy in place for secure configuration and operation of the MFD or High-Volume Printer b. Least functionality controls that must be in place that include disabling all unneeded network protocols, services, and assigning a dedicated static IP address to the MFD or High-Volume Printer c. Strong security controls should be incorporated into the MFD or High-Volume Printer management and administration d. Access enforcement controls must be configured correctly, including access controls for file shares, administrator and non-administrator privileges, and document retention functions e. MFDs or High-Volume Printers should be locked with a mechanism to prevent physical access to the hard disk f. Firmware should be up to date with the most current firmware	The district must determine if the printing of FTI will be allowed. If the district opts to print FTI, then a written policy must be established. Printing must be restricted to the internal network only. Each county's architecture may be different, please consult your IT resources.

2021 Publication Section	Page	2021 Publication 1075 Requirement	2016 Publication Section	Page	2016 Publication 1075 Requirement	District Impact
					available and should be currently supported by the vendor g. Devices and print spoolers have auditing enabled, including auditing of user access and fax logs (if fax is enabled), and audit logs should be collected and reviewed by a security administrator h. All FTI data in transit should be encrypted when moving across a WAN and within the LAN i. Disposal of all hardware follows media sanitization and disposal procedure requirements (see Section 9.3.10.6, Media Sanitization (MP-6), and Section 9.4.7, Media Sanitization	