Industry	Regulation	Paragraph Number	The Verbage	Explanation
Financial	**GDPR**	**Recital 87**	A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay."	The 72-hour notification rule for breaches only is viable if the company has a current inventory of their data bearing devices through the storage server system itself and a means to track loose (failed) or decommissioned media. Failure to track and contain loose media that is no longer monitored makes it capable for a critical hard drive to be stolen and years to pass before discovery.
		Recital 85	"[87] It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."	In many data centers, when new storage servers have spun up and data installed, the older storage server is shut down. The monitoring systems on the old storage servers are now turned off, leaving this system vulnerable to subterfuge. Also, the data bearing devices are no longer tracked to protect the EU citizen's data. (12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
	FFEIC Handbook	**II.C.5 Inventory and Classification of Assets**	Inventory and Classification of Assets requires management to "maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections."	Loose media that contains all the data written to it while in a computer of storage server becomes a critical asset.
		II.C.7 User Security Controls	User Security Controls requires "establishing and administering a user access program for physical and logical access".	
		II.C.7(b) User Access Program	User Access Program requires management to "develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology.	
		II.C.7(c) Segregation of Duties	Segregation of Duties requires "segregation of duties, or job designs that require more than one person to complete critical or sensitive tasks, can help mitigate risk."	
		II.C.7(e) Training	Training "ensures personnel have the necessary knowledge and skills to perform their job functions."	
	NIST 800-53	**MP-6(1) MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY**	The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions. Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal.	

		MP-6(2) MEDIA SANITIZATION | EQUIPMENT TESTING	The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved. Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).	
		MP-6(3) MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES	The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices]. This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable	
		MP-6(7) MEDIA SANITIZATION | DUAL AUTHORIZATION	The organization enforces dual authorization for the sanitization of [Assignment: organization-defined information system media]. Organizations employ dual authorization to ensure that information system media sanitization cannot occur unless two technically qualified individuals conduct the task. Individuals sanitizing information system media possess sufficient skills/expertise to determine if the proposed sanitization reflects applicable federal/organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, both protecting against errors and false claims of having performed the sanitization actions. Dual authorization may also be known as two	
	NIST 800-88	**NIST SP 800-88 R1 Section 4.4 Control of Media**	A factor influencing an organizational sanitization decision is who has control and access to the media. This aspect must be considered when media leaves organizational control. Media control may be transferred when media are returned from a leasing agreement or are being donated or resold to be reused outside the organization. The following are examples of media control: Under Organization Control: Media being turned over for maintenance are still considered under organization control if contractual agreements are in place with the organization and the maintenance provider specifically provides for the confidentiality of the information. Maintenance being performed on an organization's site, under the organization's supervision, by a maintenance provider is also considered under the control of the organization. Not Under Organization Control (External Control): Media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the organization are considered to be out of organizational control.	Section 4 requires management to control the media and no data bearing device can be sent to an outside agency unless they contractually agree to take responsibility for the device (financially) dur to a breach.
		NIST SP 800-88 R1 Section 4.7.2 Verification of Personnel Competencies	Another key element is the potential training needs and current expertise of personnel conducting the sanitization. Organizations should ensure that equipment operators are competent to perform sanitization functions.	

		NIST SP 800-88 R1 Section 4.8 Documentation of the Data Eradication Process	Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. A certification of media disposition may be a piece of paper or an electronic record of the action taken. For example, most modern hard drives include bar codes on the label for values such as model and serial numbers. The person performing the sanitization might simply enter the details into a tracking application and scan each bar code as the media is sanitized. Automatic documentation can be important as some systems make physical access to the media very difficult. The decision regarding whether to complete a certificate of media disposition and how much data to record depends on the confidentiality level of the data on the media. For a large number of devices with data of very low confidentiality, an organization may choose not to complete the certificate. When fully completed, the certificate should record at least the following details: Manufacturer, Model, Serial Number Organizationally Assigned Media or Property Number (if applicable) Media Type (i.e., magnetic, flash memory, hybrid, etc.) Media Source (i.e., user or computer the media came from) Pre-Sanitization Confidentiality Categorization (optional) Sanitization Description (i.e., Clear, Purge, Destroy) Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.) Tool Used (including version) Verification Method (i.e., full, quick sampling, etc.) Post-Sanitization Confidentiality Categorization (optional) Post-Sanitization Destination (if known) For Both Sanitization and Verification: o Name of Person o Position/Title of Person o Date	99% of Certificate of Destructions in the United States do not meet NIST requirements.