FIU | Office of Internal Audit

FLORIDA INTERNATIONAL UNIVERSITY

Audit of Media Sanitization Guidelines and Controls

Report No. 20/21-12
June 30, 2021

FIU | Office of Internal Audit

Date: June 30, 2021

To: Robert Grillo, Vice President and Chief Information Officer
Helvetiella Longoria, Chief Information Security Office

From: Trevor L. Williams, Chief Audit Executive

Subject: **Audit of Media Sanitization Guidelines and Controls – Report No. 20/21-12**

We have completed an audit of Media Sanitization Guidelines and Controls. The primary objective of our audit was to determine whether the technology controls in place provide reasonable assurance that media sanitization processes are compliant with the State of Florida regulations, University policies and procedures, and the National Institute of Standards and Technology (NIST) guidelines, to minimize the risk of unauthorized University data disclosure upon the transfer or disposal of media.

The Division of Information Technology is responsible for validating that any information systems equipment used for University business are erased using clearing, purging, or destruction techniques prior to the media being sent to surplus, reused, donated, and/or discarded.

Our observations and recommendations pertaining to reportable conditions found are detailed on the following pages of this report. We have also included management's response to our observations and recommendations, along with their implementation dates.

Overall, our audit identified areas where FIU has opportunities to strengthen the media sanitization processes. Those include:

- Incorporating specific repeatable sanitization procedures for media type in a formal operations manual.
- Leveraging important additional capabilities of the media sanitization tools currently in use or being offered by other tools.
- Finalizing and communicating an organization-wide data classification policy and aligning Media Sanitation Guidelines with current practices.
- Improving the recordkeeping pertaining to sanitized devices by applying an MSCID sticker to all such devices and electronically documenting the details required by NIST upon their sanitization.

- Establishing and implementing procedures for the verification of sanitization results.
- Defining the frequency for testing and calibrating sanitization equipment and establishing a log to record equipment testing activity.
- Updating the Media Sanitation Guidelines to include defining circumstances requiring the sanitization of portable media and dual authorization, media sanitization equipment and types of media, and the approval required for any exceptions to the guidelines, among other enhancements.
- Developing, in collaboration with Surplus, training content specific to FIU media sanitization protocol.

The audit resulted in 13 recommendations, which management has agreed to implement, and 10 of which have already been implemented.

We take this opportunity to express our appreciation to you and your staff for the cooperation and courtesies extended to us during the audit.

Attachment

C: FIU Board of Trustees
Mark B. Rosenberg, University President
Kenneth G. Furton, Provost, Executive Vice President, and Chief Operating Officer
Kenneth A. Jessell, Senior Vice President and Chief Financial Officer
Javier I. Marques, Vice President and Chief of Staff, Office of the President

TABLE OF CONTENTS

OBJECTIVES, SCOPE, AND METHODOLOGY

Pursuant to our approved annual plan for the 2020-2021 fiscal year, we have completed an audit of the University's Media Sanitization Guidelines and Controls. The primary objective of our audit was to determine whether the technology controls in place provide reasonable assurance that media sanitization processes are compliant with the State of Florida regulations, University policies and procedures, and the National Institute of Standards and Technology (NIST) guidelines, to minimize the risk of unauthorized University data disclosure upon the transfer and disposal of media.

The audit was conducted in accordance with the ISACA IS Audit and Assurance Standards and the *International Standards for the Professional Practice of Internal Auditing* issued by The Institute of Internal Auditors and included tests of the supporting records and devices and such other auditing procedures, as we considered necessary under the circumstances. To accomplish specific IT control objectives, we applied a governance, risk, and compliance framework, which utilizes the NIST Special Publications 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*,[1] and the NIST Special Publications 800-88, Revision 1, *Guidelines for Media Sanitization*.[2] Audit planning and fieldwork was conducted from January 2021 to April 2021.

To satisfy our objective, we:

- Reviewed the University policies and procedures, applicable Florida Statutes, and federal laws,
- Observed the current practices at FIU's Division of Information Technology's (DoIT) Department of Enterprise Information Security ("DoIT Enterprise Security"), Property Control, and Surplus Warehouse current practices,
- Interviewed responsible personnel,
- Tested selected devices, and
- Consulted with other State University System (SUS) internal auditors.

Sample sizes and items selected for testing were determined on a judgmental basis applying a non-statistical sampling methodology.

As part of our audit, we reviewed other internal and external audit and review reports issued during the last three years and determined that there was a prior recommendation related to the scope and objectives of this audit. This recommendation was included in the Crowe LLP ("Crowe") report titled, Florida Board of Governors State University System - Florida International University Internal Management and Accounting Control and Business Process Assessment, issued in November 2019. Crowe recommended that the University implement a system for classifying data which is a critical component of media sanitization. The recommendation has been partially implemented and is addressed in this report.

[1] NIST Special Publication 800-53A, Revision 4 provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations.
[2] NIST Special Publication 800-88, Revision 1 assists organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.

BACKGROUND

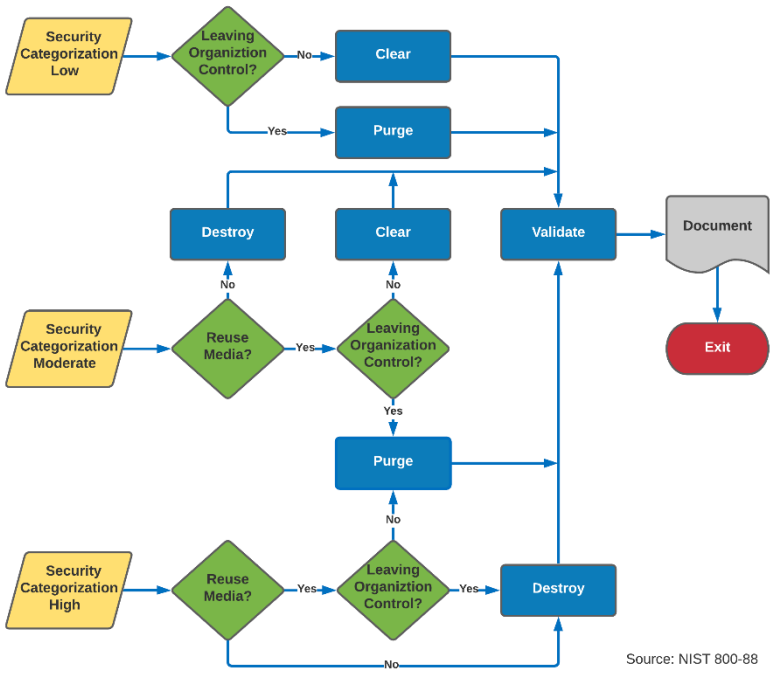
Prior to reusing, donating, or disposing of storage media, organizations should apply media sanitization techniques to erase, destroy, and prevent the recovery of any data residing on the media. This process is known as media sanitization. The application of effective media sanitization techniques and controls significantly reduces the likelihood of inadvertent data disclosure upon the release of storage media.

The categories of actions that can be taken to sanitize media are defined as follows:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through Read and Write commands or using a menu option to reset the device to the factory state (where rewriting is not supported).
- **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
- **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for the storage of data.

The decision to clear, purge, or destroy media should be applied based on the security classification of the data on the media. Figure 1 illustrates the NIST compliant sanitization decision making process based on security categorization.

Figure 1 - Sanitization and Disposition Decision Flow



The term storage media refers to any physical devices or components of computing systems capable of receiving and storing electronic data. Hard drives, printers, network routers, universal serial bus (USB) flash drives, and solid-state drives (SSDs) are all examples of storage media. A listing of media types is illustrated in Figure 2.

Florida Statute Chapter 282, section 318 requires state agencies to abide by the information technology security framework. Florida Administrative Code (F.A.C.) 60GG-2.003 - *PR.DS-3 Data Security* of the framework states that agencies must "formally manage assets managed throughout removal, transfers, and disposition."

The State University System of Florida Board of Governors (BOG) Regulation 3.0075, *Security of Data and Related Information Technology Resources* requires each university to establish a security plan based upon best practices and recognized industry standards such as NIST and ISACA.

The Florida International University IT Security Plan addresses the requirements of both mandates. The IT Security Plan's *FIU Media Sanitation Guidelines* requires DoIT to validate that any information systems equipment used for University business are erased using clearing, purging, or destruction techniques prior to media being sent to surplus, reused, donated, and/or discarded.

Figure 2 - Types of Media

Hard Copy Storage	
	• Microfilm, microfiche, or other reduced image photo negatives
Networking Devices	
	• Routers and switches (home, office, enterprise)
Mobile Devices	
	• iPhone, Blackberry, Android, Windows • All other mobile devices (Smart phones, PDAs, tablets, etc.)
Office Equipment	
	• Copy, print, fax, and multifunction machines
Magnetic Media	
	• Floppies, Reel, and Cassette • ATA Hard disks [PATA, SATA, eSATA] • SCSI
Peripherally Attached Storage	
	• External Locally Attached Hard Drives (USB, Firewire, etc.)
Optical Media	
	• CD, DVD, BD
Flash Memory-Based Storage	
	• ATA Solid State Drives (SSDs) • SCSI Solid State Drives (SSSDs) • NVM Express SSD's • USB Removable Media • Memory Cards (SD, SDHC, etc.)
Source: NIST 800-88	

Media Sanitization Tools

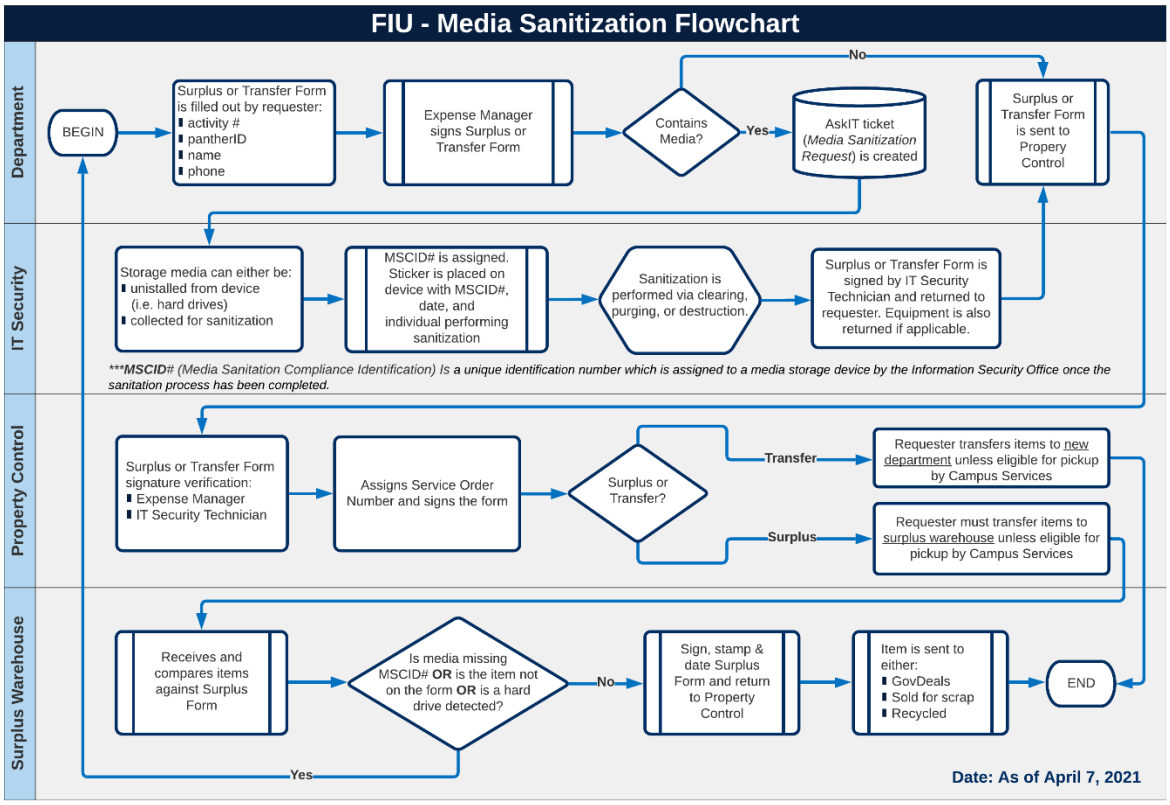
DoIT Enterprise Security has an array of tools available to perform sanitization actions as highlighted in Figure 3 below.

Figure 3 - DoIT Media Sanitization Tools		
Sanitization Equipment	**Comments/Description**	**Image**
Dari's Boot and Nuke (DBAN) (Clear) -Magnetic Media	Open-source software designed to securely erase a hard disk until its data is permanently removed and no longer recoverable. This is achieved by overwriting the data with pseudorandom numbers generated by Mersenne Twister or ISAAC. The Gutmann method, Quick Erase, DoD Short (3 passes) and DOD 5220.22-M (7 passes) are also included as options to handle data remanence.	
Garner Data Eliminator HD-3WXL (Purge) -Magnetic Media	A continuous duty capacitive discharge degausser. The HD-3WXL is designed to erase hard drives and tape cartridges that fit within the opening of the Media Entrance Door.	
Bow Industries MHDD-N (Destroy) -Magnetic Media -Flash Storage	NSA/CSS Approved Hard Drive destroyer capable of destroying 1-inch, 0.65-inch, 1.65-inch, Laptop Drives (HDD and SSD).	
MediaClone SuperWiper 8'' T3 Field i7 (Clear/Purge) -Magnetic Media -Flash Storage -Peripherally Attached Storage	NIST 800-88 compliant SuperWiper 8" T3 SAS/SATA and USB3.0/3.1 ports is an extremely fast, efficient, and secure portable dedicated SAS/SATA and USB3.0/3.1 eraser unit. Device can generate erase log files and erase certifications (option to save to NIST 800-88 format). The unit supports many erase protocols and different digital storage devices, such as SSD, HDD, and USB storage devices.	
Intimus 600 671-6s (Destroy) -Optical Media	5.8mm strip cut shredder. Currently used to destroy CD's, DVD's, and Blu-ray.	
Miscellaneous. Scissors/Drill (Destroy) -Microform -Floppy -Mobile Devices	Scissors are used to destroy floppy disks. Tape cassettes can be broken and the tape destroyed with scissors. Drills are used to destroy SSD's.	

Media Sanitization Process Flows

Although FIU does not have a finalized graduated data classification policy, DoIT Enterprise Security noted that the security categorization of all media is considered highly sensitive for the purposes of media sanitization and that media are destroyed in most instances.

While DoIT Enterprise Security remains responsible for the sanitization of all media, the media sanitization process is a collaborative model involving the following departments: DoIT Enterprise Security, Property Control, and Procurement's Surplus Warehouse. Figure 4 below depicts the sanitization flow of a storage medium from an individual department to the Surplus Warehouse, and the information system controls in place.



After a department identifies all media requiring sanitization and creates a *Media Sanitization Request*, DoIT Enterprise Security must visit the department to collect the media and verify there are no other surplus items requiring sanitization. A single request could include multiple devices, and each device could contain multiple hard drives. There were 238 such requests during the 2019 calendar year, 70 in 2020 due to COVID-19, and 52 sanitization requests received by DoIT as of May 2021.

Once sanitization is complete, Property Control verifies that the appropriate approvals have been obtained prior to granting permission to send the media to the Surplus Warehouse. When the media arrives at the warehouse, Surplus personnel perform one final verification step as depicted in the flowchart above to ensure that media is not transferred to another department or leaves University property without proper sanitization.

OBSERVATIONS AND RECOMMENDATIONS

Overall, our audit identified areas where FIU has opportunities to strengthen the media sanitization processes. Those areas include sanitization procedures, classifying data for sanitization, tracking media removed, verifying results, testing equipment, defining circumstances for utilizing non-destructive techniques, requiring dual authorization, and training for personnel involved in the sanitization process. Our observations and recommendations pertaining to reportable conditions found are detailed on the following pages of this report. We have also included management's response to our recommendations, along with their implementation dates. Our evaluation of FIU's controls that fall within the scope of our audit is summarized in the following table:

CRITERIA	SATISFACTORY	OPPORTUNITIES TO IMPROVE	INADEQUATE
Process Controls		**X**	
Policy & Procedures Compliance		**X**	
Effect	**X**		
Information Risk	**X**		
External Risk	**X**		

INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**OPPORTUNITIES TO IMPROVE**	**INADEQUATE**
Process Controls (Activities established mainly through policies and procedures to ensure that risks are mitigated and objectives are achieved.)	Effective	Opportunities exist to improve effectiveness	Do not exist or are not reliable
Policy & Procedures Compliance (The degree of compliance with process controls – policies and procedures.)	Non-compliance issues are minor	Instances of non-compliance are evident	Non-compliance issues are pervasive, significant, or have severe consequences
Effect (The potential negative impact to the operations, financial, reputational, social, etc.)	Not likely to impact operations or program outcomes	Impact on outcomes contained	Negative impact on outcomes
Information Risk (The risk that information upon which a business decision is made is inaccurate.)	Information systems are reliable	Data systems are mostly accurate but need to be improved	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions
External Risk (Risks arising from events outside of the organization's control, e.g., political, legal, social, cybersecurity, economic, environment.)	None or low	Potential for damage	Severe risk of damage

SUMMARY OF OBSERVATIONS AND RECOMMENDATIONS – NIST FRAMEWORKS

The areas tested during the audit and our observations and recommendations related to the internal processes currently in place to perform media sanitization as outlined in the NIST 800-53 and 53A, as well as NIST 800-88 standards are presented on the following pages.

1. Sanitization Governance – Guidelines			
NIST 800-53 & 53A Criteria	**NIST 800-88 Criteria**	**FIU Controls**	**Audit Procedures**
MP-6(a)[1] The organization defines information system media to be sanitized prior to disposal, release out of organizational control, or released for re-use.	**4.1 – Information Decisions in the System Life Cycle** Organizations should take care in identifying media for sanitization. Many items used will contain multiple forms of media that may require different methods of sanitization. For example, a desktop computer may contain a hard drive, motherboard, RAM, and ROM, and mobile devices contain on-board volatile memory as well as non-volatile removable memory.	**FIU Media Sanitation Guidelines** Before disposal, donation, or recycling, DoIT Enterprise Security must validate that sensitive information has been removed from any information systems equipment that has been used for University business. This validation process must take place before releasing such equipment to a third party.	**Test Criteria:** Determine if FIU has established policies and procedures that defines information system media to be sanitized. **Audit Procedures:** Reviewed applicable FIU procedures: • *FIU Media Sanitation Guidelines* • *FIU Media Sanitation Procedures*
Observation			
No Exceptions Noted: FIU *Media Sanitation Guidelines* require that "before disposal, donation, or recycling, DoIT Enterprise Security must validate that sensitive information has been removed from any information systems equipment that has been used for Florida International University business. This validation process must take place before releasing such equipment to a third party."			

1. Sanitization Governance - Techniques			
NIST 800-53 & 53A Criteria	**NIST 800-88 Criteria**	**FIU Controls**	**Audit Procedures**
MP-6(a)[2] The organization defines sanitization techniques or procedures to be used for sanitizing organization-defined information system media prior to disposal, release out of organizational control, or released for re-use.	**2.5 - Types of Sanitization** Clear, Purge, and Destroy are actions that can be taken to sanitize media. The categories of sanitization are defined as follows: • Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). • Purge applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques. • Destroy renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.	**FIU Media Sanitation Guidelines** Storage media may be sanitized using several methods: • Data Overwriting Applications • Magnetic Degaussing • Physical Destruction	**Test Criteria:** Determine if FIU has established policies and procedures that defines sanitization techniques or procedures to be used for sanitizing organization-defined information system media. **Audit Procedures:** Reviewed applicable FIU procedures: • *FIU Media Sanitation Guidelines* • *FIU Media Sanitation Procedures*
Observation			
No Exceptions Noted: FIU has established *Media Sanitation Guidelines* requiring the sanitization of storage devices using one of the following techniques: a repeated overwrite operation, purging, degaussing, or destroying prior to storage media being sent to surplus, reused, donated, or discarded.			

1. Sanitization Governance - Process

NIST 800-53 & 53A Criteria	NIST 800-88 Criteria	FIU Controls	Audit Procedures
MP-6(a)[3] The organization sanitizes organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques or procedures in accordance with applicable federal and organizational standards and policies.	**1.1 - Purpose and Scope** The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization to prevent unauthorized individuals from gaining access to and using the information contained on the media.	**FIU Media Sanitation Guidelines** In order to protect University data, especially Highly Sensitive Data, from inadvertent or unauthorized use or disclosure, a University department or unit disposing of equipment with storage devices must ensure that the storage devices are erased using a repeated overwrite operation, purged, degaussed, or destroyed prior to storage media being sent to surplus, reused, donated, or discarded.	**Test Criteria:** Determine if FIU's sanitization techniques are compliant with minimum sanitization standards of NIST Special Publication (SP) 800-88, Revision (Rev.) 1. **Audit Procedures:** Reviewed applicable FIU procedures: • *FIU Media Sanitation Guidelines* • *FIU Media Sanitation Procedures* Evaluated techniques used by DoIT Enterprise Security to sanitize hard copy storage, networking devices, office equipment, magnetic media, peripherally attached storage, optical media, flash memory-based storage devices. Evaluated tools used by DoIT Enterprise Security to sanitize Media (see Figure 3, on page 4).

Observations, Recommendations, and Management Response

Observations:

Exceptions Noted: We were not provided with an adequate operations manual defining sanitization procedures per media type that could be conducted in a defined and repeatable manner. However, based on the interviews, walk-throughs, and research performed on sanitization techniques used by the DoIT Enterprise Security Office, we determined that the techniques used are NIST compliant, except for those used on microform and optical media. NIST 800-88 requires microform to be burned to white ash and optical media to be shredded to particles of .25mm^2. Since DoIT destroys microform with scissors, albeit a minimal currently, and shreds optical media with a strip-cut shredder, the resulting particles do not meet the compliance requirements.

In examining the sanitization tools, we observed the successful overwrite operation of an SSD using the MediaClone SuperWiper whereby the drive remained undamaged upon sanitization. We conducted additional research that found that the MediaClone SuperWiper can sanitize magnetic, peripherally attached, and flash memory-based media in accordance with NIST standards. Although a certificate of sanitization was not observed during our walk-through, the device specification indicates that the application can generate a log file and an erase certificate and export the files to a USB flash drive in a NIST compliant format.

Recommendations and Management Response:

The Division of IT should:

No.	Recommendations	Management Response	Complexity	Implementation Date
1.1	Include specific sanitization procedures per media type that can be conducted in a defined and repeatable manner in a formal operations manual.	Completed. Media types have been added to the Media Sanitation SOP [Standard Operating Procedures].	1 - Routine	Immediately

No.	Recommendations	Management Response	Complexity	Implementation Date
1.2	Investigate and capitalize on the additional capabilities offered with current media sanitization tools already in use or other tools.	Completed. The IT Security Office has reviewed the documentation and manuals for our sanitation tools. Our normal sanitation process is to destroy the devices; however, we have reviewed the documentation for other features we can use for sanitation in the event we need to reuse a drive. Additional fields will be added to the surplus form that will provide information regarding the sanitation process, data type, and serial number.	1 - Routine	Immediately

1. Sanitization Governance - Data Classification			
NIST 800-53 & 53A Criteria	**NIST 800-88 Criteria**	**FIU Controls**	**Audit Procedures**
MP-6(b) The organization employs sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.	**4.2 - Determination of Security Categorization** Early in the system life cycle, a system is categorized using the guidance found in FIPS 199, NIST SP 800-60 Rev. 1, or CNSSI 125318, including the security categorization for the system's confidentiality. This security categorization is revisited at least every three years (or when significant change occurs within the system) and revalidated throughout the system's life, and any necessary changes to the confidentiality category can be made. Once the security categorization is completed, the system owner can then design a sanitization process that will ensure adequate protection of the system's information. Much information is not associated with a specific system but is associated with internal business communications, usually on paper. Organizations should label these media with their internal operating confidentiality levels and associate a type of sanitization described in NIST 800-88.	None noted.	**Test Criteria:** Interview DoIT Enterprise Security Office personnel with information security responsibilities to gain an understanding of how data is classified and whether specific procedures exist to correspond with the data classification level. **Audit Procedures:** Reviewed applicable FIU procedures: • *FIU Media Sanitation Guidelines* • *FIU Data Stewardship Policy 1930.020a.* • *Crowe Report* Interviewed NIST and DoIT personnel.

Observations, Recommendation, and Management Response

Observations:

Exceptions Noted: The University does not have a graduated system for classifying data. A data classification system should drive the media sanitization process and impact the organization's decision making on implementing the additional NIST control enhancements addressed later: MP-6(1), MP-6(2), MP-6(3), MP-6(7), MP-6(8).

FIU's Data Classification policy is currently in draft, and the FIU *Media Sanitation Guidelines* do not reference a data classification system to perform sanitization actions. Notwithstanding, we were informed that all media are currently treated as "highly sensitive" during sanitization. Although less stringent (and perhaps less costly) techniques could be applied if devices were classified as low or moderate, the organization has decided to err on the side of caution and is making intentional risk response decisions. However, as it pertains to Tracking and Documenting, and to Verify, addressed in the subsequent sections, when classifying systems as HIGH, NIST imposes additional controls during the sanitization process. For example, "Non-Destructive Techniques" would require that prior to connecting any removable media to any system, a user must use sanitization software to wipe the drive clean first. Although the decision to default to the HIGH baseline could result in increased costs and burden, the risk of any unintended disclosure of data would be reduced. Management has implemented mitigating and compensating controls to offset the risks of not fully implementing the media sanitization control enhancements.

Recommendation and Management Response:

The Division of IT should:

No.	Recommendation	Management Response	Complexity	Implementation Date
1.3	Finalize and communicate an organization-wide data classification policy, while aligning *Media Sanitation Guidelines* with current practices.	In Progress. This does not apply to our Media Sanitation process. We have made an operational decision to treat all drives high and do not need to classify the data in order to determine the sanitation method. Even though, the type of data stored in the devices does not drive the media sanitation process we will collect information on the surplus form on type of data stored on the device just for documentation purposes. The FIU Remote Access Guidelines containing a Data Classification Appendix was shared and communicated to all members of the University on several occasions throughout 2020. A data classification policy has been drafted and it will be finalized through the established policy process. In addition, the Media Sanitation Guidelines has been updated to state that all media will be treated as high regardless of data stored on the media for sanitization purposes.	2 - Moderate	September 30, 2021

2. Reviewal and Approval of Sanitization Disposal Actions			
NIST 800-53 & 53A Criteria	**NIST 800-88 Criteria**	**FIU Controls**	**Audit Procedures**
MP-6(1)[1] **MP-6(1)[2]** The organization reviews and approves media sanitization and disposal actions to ensure compliance with records retention policies.	**4.6 – Sanitization and Disposal Decision** Once an organization completes an assessment of its system confidentiality, determines the need for information sanitization, determines appropriate time frames for sanitization, and determines the types of media used and the media disposition, an effective, risk-based decision can be made on the appropriate and needed level of sanitization.	**Request for Surplus Form Section A** In accordance with the FIU *Media Sanitation Guidelines* and *Data Stewardship Procedures*, the University requires that ALL media storage devices be sanitized prior to being surplus, donated, transferred, or discarded. This applies even if the storage medium is missing from the equipment, physical inspection still must occur. All media storage devices require a MSCID number be assigned for proof of sanitation compliance. **FIU Policy No. 2350.065, Records Retention Schedule for Sponsored Project Documents Policy and Procedure** Destruction of any records must be done in accordance with the policy established by the State of Florida, which is available at recordsmanagement.fiu.edu.	**Test Criteria:** Obtain supporting documentation for steps taken to review media disposal actions. **Audit Procedures:** Reviewed applicable FIU procedures: • *FIU Media Sanitation Guidelines* • *FIU Media Sanitation Procedures* • *Data Stewardship Procedures* • *FIU Policy No. 2350.065* • *Request for Surplus Form*
Observations			
No Exceptions Noted: FIU *Media Sanitation Guidelines* require that all media storage devices be sanitized using approved sanitization mechanisms of overwrite, degauss, or destroy. In addition, any destruction of information must be done in accordance with FIU Policy 2350.065 Records Retention Schedules.			

2. Tracking and Documenting

NIST 800-53 & 53A Criteria	NIST 800-88 Criteria	FIU Controls	Audit Procedures
MP-6(1)[3] **MP-6(1)[4]** The organization tracks and documents media sanitization and disposal actions.	**4.8 - Documentation** Records are maintained when the media is introduced to the environment, when the media leaves the place it was last used, and when it reaches the sanitization destination. Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. [When fully completed, the certificate should at a minimum record the criteria found in Appendix I.]	**FIU Media Sanitation Procedures** • User submits a request for media sanitization by completing the *Media Sanitation Request* form found under Security/Media Sanitation at https://security.fiu.edu. • An AskIT service request is assigned to the DoIT Enterprise Security Office. • The surplus or transfer form is signed by the DoIT Enterprise Security Office. The original is retained by the user to be provided to Property Control and a copy is retained by the DoIT Enterprise Security Office. • The signed surplus or transfer form is stored in a filing cabinet in PC534A and attached to the AskIT service request. **FIU Media Sanitation Guidelines** Upon completion of media sanitation procedures, the equipment must display an official sticker from the DoIT Enterprise Security Office indicating the name of the person who performed the sanitization, the date of compliance, and the MSCID. DoIT Enterprise Security will be responsible for the performance and documentation of all media sanitation.	**Test Criteria:** Obtain supporting documentation for tracking media sanitization action. **Audit Procedures:** Reviewed documents • FIU surplus or transfer form • Query of *Media Sanitation Service Requests* from July 2020 to January 2021 Interviewed: • DoIT Enterprise Security, Property Control, and Surplus Warehouse Personnel • College of Arts, Sciences & Education (CASE) IT personnel regarding Asset Management System tracking ability We visited the FIU Surplus Warehouse, selected a judgmental sample of surplus equipment to be disposed of or released for reuse, and traced the equipment to the respective FIU Surplus Forms.

Observations, Recommendations, and Management Response

Observations:

Exceptions Noted: Tracking and documenting of sanitization actions is required for any media categorized as HIGH. FIU currently designates all media undergoing sanitization as HIGH. During our walk-through of the Surplus Warehouse from the media on hand, we examined two of the 14 Panasonic digital recording systems, two of the nine Dell servers, two of the 19 desktop computers, and one switch from a lot of 29 Cisco Networking Equipment. We verified that the sampled media were appropriately sanitized and found that all but the networking devices had the MSCID tag appropriately attached. While serial numbers, date of sanitization, and MSCID number were documented on the FIU surplus forms, we were unable to determine the sanitization methods and destination of hard drives removed from the sampled media, where applicable. NIST 800-88 requires this information to be recorded in the form of Certificates of Sanitization. These certificates provide an audit trail for sanitization activities. Additional details required per NIST's minimum certificate requirements were also omitted:

- media type
- media source
- pre-sanitization confidentiality categorization (optional)
- sanitization description (i.e., clear, purge, or 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: (name, position, date, contact information, signature of the attending personnel).

Exceptions Noted: Records of sanitization can be identified in two ways. DoIT can perform a query of Media Sanitation Requests, which features the name of the requester, the assigned technician, and a link to an uploaded pdf of the Surplus Form. However, the system relies on information about the assets being recorded on the Surplus Form and does not provide search capabilities. Alternatively, a physical search can be conducted through the Surplus Forms in Property Control for an items' serial number or MSCID number (if available). Neither method can produce a reliable count of the quantity of media sanitized as all storage media removed from devices containing multiple media are not accounted for.

During a walk-through of CASE's Asset Management system, we observed that the system features over 1,500 of the organization's assets. The system contains a field for MSCID's and allows users to upload attachments. It allows for asset status changes such as "Ready to Deploy" and "Sent to Surplus." The system is scalable, allowing for the introduction of additional fields not currently in the system. In addition, the system allows for the searching of assets by identifiers such as MSCID, Serial Number, etc. If sanitization records need to be referenced in the future, electronic records stored via the Asset Management system could provide the more efficient and reliable search capabilities. In order to keep better tracking of the assets from decentralized units, DoIT could proactively leverage the tool for University-wide application.

Recommendations and Management Response:

The Division of IT should:

No.	Recommendations	Management Response	Complexity	Implementation Date
2.1	Apply MSCID stickers to all devices sanitized.	Completed. MSCID stickers will be applied to all devices sanitized including network devices. The Media Sanitation Guidelines and Media Sanitation SOP have been updated to reflect the process for network devices.	1 - Routine	Immediately
2.2	Collaborate with Surplus to develop a tool to electronically document the details required by NIST upon sanitization. Continue to promote the use of the Enterprise Asset Management system.	In Progress. The IT Security Office will work with others in the Division of IT to help Surplus develop an electronic form to replace the current paper form for surplus. In addition, the new surplus form will be updated to include fields such as sanitation description, serial number, method used, media type, and verification method. The IT Security Office will continue to promote the use of the Enterprise Asset Management System.	3 - Complex	September 30, 2021

2. Verify

NIST 800-53 & 53A Criteria	NIST 800-88 Criteria	FIU Controls	Audit Procedures
MP-6(1)[5] The organization verifies media sanitization and disposal actions.	**4.7.3 - Verification of Sanitization Results** The goal of sanitization verification is to ensure that the target data was effectively sanitized. Full verification or representative sampling can be conducted.	**FIU Media Sanitation Guidelines** Facilities Department [Surplus Warehouse] It is the responsibility of the Facilities Department through the Surplus Warehouse to ensure that no media that has been submitted for surplus, disposal or donation is permitted to be transferred to another department or leave university property without proper sanitation of storage media. The Facilities Department must ensure that all equipment that is submitted for surplus, disposal or donation bears the compliance sticker indicating that media sanitation procedures have been completed and MCSID number has been assigned.	**Test Criteria:** Obtain supporting documentation for media disposal actions related to verification. **Audit Procedures:** Reviewed applicable FIU procedures: • *FIU Media Sanitation Guidelines* • *FIU Media Sanitation Procedures* Interviewed: • DoIT Enterprise Security, Property Control, and Surplus Warehouse personnel Performed a walk-through and observed DoIT personnel performing the sanitization of a SSD using MediaClone SuperWiper 8'' T3 Field i7.

Observations, Recommendation, and Management Response

Observations:

Exceptions Noted: It is important for organizations to periodically verify that data is sanitized from all media categorized as HIGH prior to re-use or disposal. We did not observe any policies or procedures addressing the verification of sanitization results. According to DoIT, most of the media received for sanitization are destroyed. Most destroy techniques do not support practical verification for each sanitized piece of media. However, verification can be performed when clearing and purging techniques are applied. During our walk-through, we did observe sanitization equipment with built-in verification abilities and a demonstration of verification conducted for an SSD. However, logs do not exist to show occurrences of verification. Additionally, most surplus networking equipment received by the Surplus Warehouse arrives from the Network Services department. Network Services performs the sanitization of the equipment. However, the DoIT Enterprise Security department is not currently verifying network equipment sanitization.

During a walk-through of the Surplus Warehouse, we observed that upon receiving surplus items, Surplus Warehouse personnel checks items for MSCID tags and physically opens the items to verify that storage media has been removed.

Recommendation and Management Response:

The Division of IT should:

No.	Recommendation	Management Response	Complexity	Implementation Date
2.3	Establish and implement procedures for the verification of sanitization results.	Completed. The Media Sanitation SOP was updated with the following: Equipment Testing and Validation: Media Sanitation equipment is used at least once a week. After every batch of drives sanitized, one is connected to a computer to confirm that the information on the drive was successfully erased.	1 - Routine	Immediately

3. Equipment Testing

NIST 800-53 & 53A Criteria	NIST 800-88 Criteria	FIU Controls	Audit Procedures
MP-6(2)[1] **MP-6(2)[2]** The organization defines the frequency for testing sanitization equipment and procedures and tests sanitization equipment and procedures with the organization-defined frequency to verify that the intended sanitization is being achieved.	**4.7.1 - Verification of Equipment** If the organization is using sanitization tools (e.g., a degausser or a dedicated workstation), then equipment calibration, as well as equipment testing, and scheduled maintenance, is also needed.	None noted.	**Test Criteria:** Obtain FIU Media Sanitization Procedures and observe if the document addresses a frequency for testing and calibrating sanitization equipment. **Audit Procedures:** Reviewed applicable FIU procedures: • FIU Media Sanitation Guidelines • FIU Media Sanitation Procedures Interviewed DoIT Enterprise Security personnel regarding equipment testing.

Observations, Recommendation, and Management Response

Observations:

Exception Noted: Apart from the minimum requirements in NIST 800-53 above, NIST 800-53b specifically requires that organizations with media categorized as HIGH should periodically test and calibrate sanitization equipment to ensure that media are appropriately sanitized. According to the DoIT Enterprise Security Office, the calibration and testing of sanitization equipment is conducted every six months to a year. However, our review of the FIU *Media Sanitation Procedures* revealed that formal documentation addressing the steps needed to test/calibrate equipment, frequency of testing, and an auditable trail of testing and calibration is missing. We did not obtain an audit trail of calibration and testing of sanitization equipment.

Recommendation and Management Response:

The Division of IT should:

No.	Recommendation	Management Response	Complexity	Implementation Date
3.1	Define a frequency for the testing and calibration of sanitization equipment and establish a log to record equipment testing activity.	Completed. The Media Sanitation SOP was updated with the following: Equipment Testing and Validation: --- Every 6 months media sanitation equipment will be tested by degaussing or sanitizing a drive and confirming that the data is erased or destroyed after that process. This action will be logged with date and name of IT Security Analyst performing the test.	1 - Routine	Immediately

4. Nondestructive Techniques for Portable Storage Devices

NIST 800-53 & 53A Criteria	NIST 800-88 Criteria	FIU Controls	Audit Procedures
MP-6(3)[1] **MP-6(3)[2]** The organization defines circumstances requiring sanitization of portable storage devices and applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under organization-defined circumstances.	**Appendix A - Minimum Sanitization Recommendations** Refer to Clear and Purge sections of the various forms of media for non-destructive techniques, if applicable. (See page 2 of this report.)	None noted.	**Test Criteria:** Evaluate FIU *Media Sanitization Procedures* and processes and determine if policies and procedures define circumstances requiring sanitization of portable storage devices. Observe if the DoIT Enterprise Security Office can apply nondestructive techniques. **Audit Procedures:** Reviewed applicable FIU procedures: • *FIU Media Sanitation Guidelines* • *FIU Media Sanitation Procedures* We interviewed DoIT Enterprise Security personnel and performed walk-throughs to observe the application of non-destructive techniques.

Observations, Recommendation, and Management Response

Observations:

Exceptions Noted: Portable storage devices include external or removable hard disk drives, optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

We performed walk-throughs and conducted research on the sanitization tools used by DoIT Enterprise Security. DoIT Enterprise Security can perform non-destructive techniques on portable media using the Departments MediaClone SuperWiper. However, we did not observe defined circumstances for the application of non-destructive techniques in the procedures obtained.

Recommendation and Management Response:

The Division of IT should:

No.	Recommendation	Management Response	Complexity	Implementation Date
4.1	Define circumstances requiring the sanitization of portable media in the *Media Sanitation Guidelines.*	Completed. We have defined the method of sanitization for various portable media types in the Media Sanitation Guidelines.	1 - Routine	Immediately

5. Dual Authorization

NIST 800-53 & 53A Criteria	NIST 800-88 Criteria	FIU Controls	Audit Procedures
MP-6(7)[1] **MP-6(7)[2]** The organization defines information system media requiring dual authorization to be enforced for sanitization of such media. The organization enforces dual authorization for the sanitization of organization-defined information system media.	N/A	**FIU *Media Sanitation Guidelines*** Information and Equipment Disposal - Department managers are responsible for the disposal of surplus property no longer needed for business activities in accordance with procedures established by the DoIT Enterprise Security Office, including the irreversible removal of sensitive information and licensed software.	**Test Criteria:** Evaluate FIU *Media Sanitization Procedures* and processes to determine if FIU defines information system media requiring dual authorization to be enforced for sanitization of such media. **Audit Procedures:** Reviewed applicable FIU procedures • *FIU Media Sanitation Guidelines* • *FIU Media Sanitation Procedures*

Observations, Recommendation, and Management Response

Observations:

Exceptions Noted: Although not a bare minimum requirement by NIST 800-53, NIST lists dual-authorization as enhanced control for organization's data sanitization's framework. We found that the University does not currently define information system media that requires dual authorization for sanitization. Dual authorization requires an organization to define circumstances where two technically qualified individuals, who possess sufficient skills and expertise, determine if the proposed sanitization of a storage medium reflects applicable federal and organizational standards, policies, and procedures. This control helps to ensure that sanitization occurs as intended, protecting against errors and false claims of having performed the sanitization actions. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Recommendation:

The Division of IT should:

No.	Recommendation	Management Response	Complexity	Implementation Date
5.1	Define circumstances requiring dual authorization.	Completed. We have other mitigating controls such as whole disk encryption deployed on all managed workstations. We do not have any circumstances which will require dual authorization.	1 - Routine	Immediately

6. Remote Purging			
NIST 800-53A Criteria	**NIST 800-88 Criteria**	**FIU Controls**	**Audit Procedures**
MP-6(8)[1] **MP-6(8)[2]** The organization defines information systems, system components, or devices to purge/wipe either remotely or under specific organizational conditions. The organization defines conditions under which information is to be purged/wiped from organization-defined information systems, system components, or devices. The organization provides the capability to purge/wipe information from organization-defined information systems, system components, or devices either remotely; or under organization defined conditions.	**Table A-3 - Mobile Device Sanitization** Refer to "Clear" sections of Table A-3 of NIST 800-88 for remote wiping techniques listing the various forms of mobile devices including Apple, Blackberry, Google Android OS, Windows and all other mobile devices.	None noted.	**Test Criteria:** Evaluate FIU Media Sanitization Procedures and processes and determine if FIU defines information systems, system components, or devices to be remotely purged/wiped. **Audit Procedures:** Reviewed applicable FIU procedures: • *FIU Media Sanitation Guidelines* • *FIU Media Sanitation Procedures* • *School of Hospitality and Tourism Management Procedures: FIU Owned Devices Management Process* Interviewed the DoIT Enterprise Security Office and the School of Hospitality and Tourism Management personnel to gain an understanding of remote purging efforts for devices located at the FIU Tianjin, China campus.
Observation			
Observation: **No Exceptions Noted**: Remote purging or wiping of data protects information on organizational systems and system components if they are obtained by unauthorized individuals. We observed University policies and procedures addressing conditions under which specified devices should be remotely purged or wiped.			

OBSERVATIONS AND RECOMMENDATIONS - OTHER

During our audit, we observed the following other areas not specifically related to NIST standards, where opportunities for improvement exist:

7. Enhancement of University Guidelines

Although DoIT's *Media Sanitation Guidelines* have been established to provide instructions on the proper disposal of all FIU sensitive information, the department should enhance the Guidelines. The current Guidelines do not mention the types of media and sanitization equipment to be used, nor do they provide any wording for exceptions to the Guidelines. Additionally, there was no clear policy statement, scope, or initial effective and revision dates. Furthermore, the roles and responsibilities of each of the parties involved in the sanitization process can be more defined. Incorporating these changes will ensure the guidelines are written in accordance with best practices.

Recommendations

The Department of Information Technology should augment current guidelines by:	
7.1	Utilizing the FIU policy template to include policy statement, scope, initial effective date, revision by, responsible department, and roles and responsibilities.
7.2	Including media sanitization equipment and types of media.
7.3	Adding the wording that specifies, "any exceptions to these guidelines must be approved by the DoIT."

Management Response/Action Plan

7.1 Completed. The Media Sanitation Guidelines were updated to the FIU Policy template.

Implementation date: Immediately

Complexity rating: 1 - Routine

7.2 Completed. The Media Sanitation Guidelines and Media Sanitation SOP were updated.

Implementation date: Immediately

Complexity rating: 1 - Routine

7.3 Completed. The Media Sanitation Guidelines and Media Sanitation SOP were updated.

Implementation date: Immediately

Complexity rating: 1 - Routine

8. Continuous Training of Technology Key Contacts

DoIT conducts monthly Information Technology Administrators Committee (ITAC) meetings where the Chief Information Officer, Chief Information Security Officer (CISO), and Information Technology Administrators discuss and learn about the latest technology initiatives. We participated in the ITAC meeting that took place in May where sanitization training was provided by the CISO, DoIT Enterprise Security Technician, and Surplus Warehouse personnel.

Notwithstanding the monthly meetings, one of the biggest areas of weakness in the sanitization process lies with the Business Units' lack of understanding of types of media requiring sanitization. Upon visiting the Surplus Warehouse, Surplus personnel pointed out that in some instances, media is erroneously delivered to the Surplus Warehouse prior to sanitization. If employees do not have a great understanding of their responsibilities and the requisite knowledge and skills to properly identify media, FIU's sanitization process could be compromised.

Recommendation

The Department of Information Technology should:	
8.1	Collaborate with Surplus to develop an FIU-specific training on the surplus process that includes media sanitization.

Management Response/Action Plan

8.1 In progress. We will work with Surplus to develop FIU specific content to be shared on FIU Develop, which explains the surplus process and the media sanitation process.

Implementation date: December 30, 2021

Complexity rating: 3 - Complex

APPENDIX I – CERTIFICATE OF SANITIZATION

Minimum Certificate Details	NIST 800-88 Example Certificate of Sanitization
• 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: (Name, Position, Date, Contact Information, Signature).	**CERTIFICATE OF SANITIZATION** **PERSON PERFORMING SANITIZATION** Name: Title: Organization: Location: Phone: **MEDIA INFORMATION** Make/ Vendor: Model Number: Serial Number: Media Property Number: Media Type: Source *(ie user name or PC property number)*: Classification: Data Backed Up: ☐ Yes ☐ No ☐ Unknown Backup Location: **SANITIZATION DETAILS** Method Type: ☐ Clear ☐ Purge ☐ Damage ☐ Destruct Method Used: ☐ Degauss ☐ Overwrite ☐ Block Erase ☐ Crypto Erase ☐ Other: Method Details: Tool Used *(include version)*: Verification Method: ☐ Full ☐ Quick Sampling ☐ Other: Post Sanitization Classification: Notes: **MEDIA DESTINATION** ☐ Internal Reuse ☐ External Reuse ☐ Recycling Facility ☐ Manufacturer ☐ Other *(specify in details area)* Details: **SIGNATURE** I attest that the information provided on this statement is accurate to the best of my knowledge. Signature: Date: **VALIDATION** Name: Title: Organization: Location: Phone: Signature: Date:

APPENDIX II – COMPLEXITY RATINGS LEGEND

Legend: Complexity of Corrective Action	
1	**Routine:** Corrective action is believed to be uncomplicated, requiring modest adjustment to a process or practice.
2	**Moderate:** Corrective action is believed to be more than routine. Actions involved are more than normal and might involve the development of policies and procedures.
3	**Complex:** Corrective action is believed to be intricate. The solution might require an involved, complicated, and interconnected process stretching across multiple units and/or functions; may necessitate building new infrastructures or materially modifying existing ones.
4	**Exceptional:** Corrective action is believed to be complex, as well as having extraordinary budgetary and operational challenges.

APPENDIX III – OIA CONTACT AND STAFF ACKNOWLEDGMENT

OIA contact:

Joan Lieuw 305-348-2107 or jlieuw@fiu.edu

Contributors to the reports:

In addition to the contact named above, the following staff contributed to this audit in the designated roles:

Henley Louis-Pierre (auditor in-charge)
Brandon Andrade (assistant – student intern)
Odalys Villanueva (assistant – student intern)
Maria Rosa Lopez (IT audit manager and reviewer)
Manuel Sanchez (supervisor and reviewer)
Vivian Gonzalez (independent reviewer)

Definition of Internal Auditing

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.