Queens College **Technology Standard**	**No: QC-ITS-CYBER-027**
Sanitization/Secure Disposal Standard	**Updated: 09/08/2023**
	Issued By: Queens College, Office of the CISO **Owner: Queens College, Information Technology Services**

1.0 Purpose and Benefits

Information systems capture, process, and store information using a wide variety of media, including paper. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These media may require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality. All computer systems, electronic devices and electronic media must be properly cleaned of data and software before being transferred outside of Queens College (QC) or if being repurposed or reused within (QC). When electronic storage devices cannot be sanitized, the media will be destroyed using Office of CIO approved vendors and processes.

The large volume of electronic data stored on computer systems and electronic media throughout the College includes confidential, FERPA-Restricted, HIPA-Restricted, and COPA-Restricted information as defined in the Data Classification Policy, such as student records, financial data, personnel records and research information. The College is subject to federal laws that set forth responsibilities for protecting this information, copyright laws and software license agreements that protect vendor rights regarding the use of software.

Unauthorized disclosure of confidential, FERPA-Restricted, HIPA-Restricted, and COPA-Restricted information may subject the College to legal liability, negative publicity, monetary penalties and loss of funding.

This policy outlines the responsibilities for carrying these protective measures.

2.0 Authority

- **Responsible Office(s):** Queens College Information Technology Services

- **Responsible Executive(s)**: Chief Information Officer (CIO)
- **Responsible Officer(s)**: Chief Information Security Officer (CISO)

3.0 Scope – College-Wide

This is a college-wide standard and includes requirements that must be followed if Queens College is to protect the information that is collected in the standard process of business. This policy is to be an additional layer of security on top of existing CUNY security policies and is not intended or able to supersede CUNY policies.

This standard applies to all departments, faculty, employees, students and contracted personnel that use or maintain (QC) information systems or media which contains confidential, FERPA-Restricted, HIPA-Restricted, and COPA-Restricted information.

The primary responsibility for sanitizing and/or disposal of data that resides on computer systems or electronic media devices rests with the units that procured, purchased, or leased the electronic media.

4.0 Information Statement

1. All computer systems, electronic devices and electronic media must be properly cleaned of data and software before being transferred outside of Queens College (QC) or if being repurposed or reused within (QC). When electronic storage devices cannot be sanitized, the media will be destroyed using Office of CIO approved vendors and processes.
2. The entity must ensure through training and/or instruction that users and custodians of information are aware of its sensitivity and the basic requirements for media sanitization and secure disposal.
3. The entity must ensure that all workforce members, including property management and custodial staff, are made aware of the media sanitization and secure disposal process in order to establish proper accountability for all data.
4. The entity must ensure that confidential material is destroyed only by authorized and trained personnel, whether in-house or contracted, using methods outlined in this standard.
5. The entity may use service providers for destruction purposes provided that the information remains secure until the destruction is completed. The service providers must follow this standard. The entity must ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the information classification standards.
6. Deans, directors and department heads are responsible for ensuring the sanitation of all College electronic devices and computer systems in their units prior to removal from the campus.

7. Software used to sanitize computer hard drives must be compliant with Department of Defense standards. Any medium that cannot be sanitized with such software must be physically destroyed.
8. The Office of Information Technology will:
    a. publish guidelines and approved software on the Information Technology Policy website. Sanitization and disposal forms and additional sanitization and data disposal information can also be found on the website.
    b. accept for destruction, any electronic data storage medium from any department.
9. Property Services is responsible for the disposition of surplus computer systems and electronic devices. Any computer system or device sent to Property Services for disposition must have an Electronic Data Disposal Verification form (available from the IT website) affixed to it indicating that the system has been sanitized, the date, the name and phone number of the person responsible for sanitizing the system.
10. Property Services will not accept any computer system without this information. If the original operating system media and certificate of license are available, they should also be sent to Property Services with the computer system.
11. Any disposal of computer systems and media must comply with all environmental regulations.
12. All confidential, FERPA-Restricted, HIPA-Restricted, and COPA-Restricted University information maintained on electronic media must be carefully removed before the media are made available for re-use within the College.

Methods of Media Sanitization

The following table depicts the three types of sanitization methods and the impact of each method.

Sanitization Method	Appropriate Use	Description
Clear	If the media will be reused and will not be leaving the entity's control.	Protects confidentiality of information against an attack by replacing written data with random data. Clearing must not allow information to be retrieved by data, disk or file recovery utilities.
Purge	If the media will be reused and leaving the entity's control.	Protects confidentiality of information against an attack through either degaussing or Secure Erase.
Physical Destruction	If the media will not be reused at all.	Intent is to completely destroy the media.

Sanitization Decision Process

The decision process is based on the confidentiality of the information, not the type of media. The entities choose the type of sanitization to be used, and the type of sanitization is approved by the Information Owner. The technique used may vary by media type and by the technology available to the custodian, so long as the requirements of the sanitization type are met. Recommended Sanitization techniques for specific types of media are outlined in Appendix A of NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Minimum Sanitization Recommendations.

Disposal without sanitization should be considered only if information disclosure would have no impact on organizational mission, would not result in damage to organizational assets, and would not result in financial loss or harm to any individuals.

The security categorization of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. The key is to first think in terms of information confidentiality, then apply considerations based on media type.

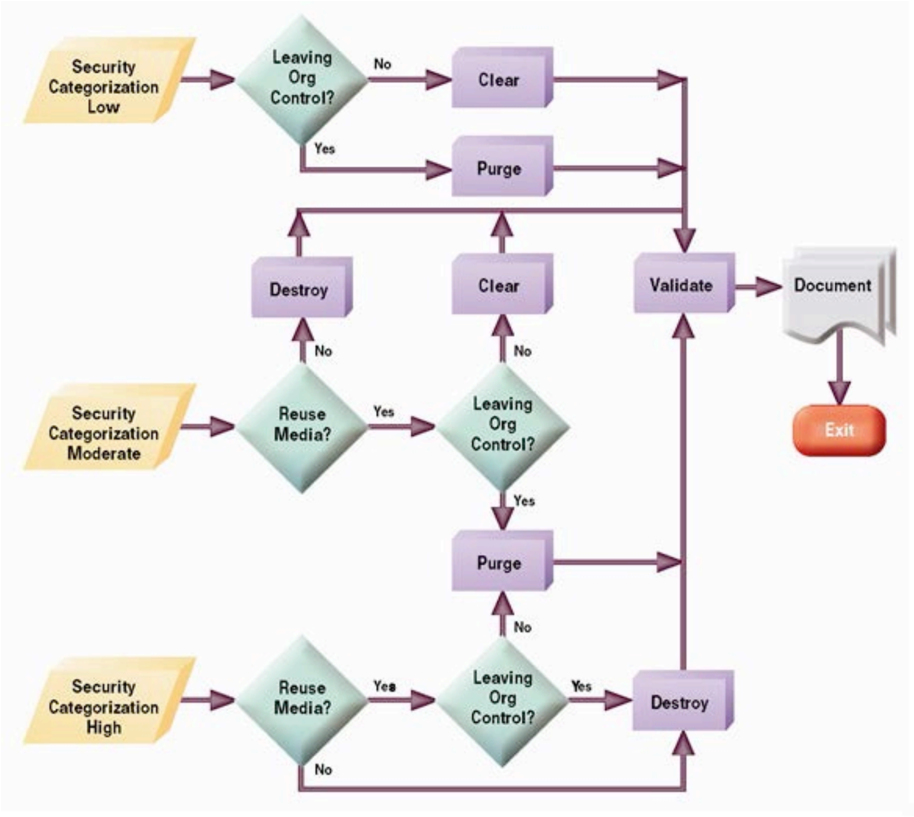

Figure 4.1- Sanitization and Disposition Decision Flow
(*from NIST 800-88, Rev. 1, Guidelines for Media Sanitization*)

The cost versus benefit of a sanitization process should be understood prior to a final decision. Entities can always increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk. For example, even though Clear or Purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options. Entities may not decrease the level of sanitization required.

Control of Media

A factor influencing a 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 SE Control:

- Media being turned over for maintenance are still considered under the entity's control if contractual agreements are in place and the maintenance provider specifically provides for the confidentiality of the information.
- Maintenance being performed on an entity's site, under the entity's supervision, by a maintenance provider is also considered under the control of the entity.

Not Under Entity Control:

- Media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the entity are considered to be out of the entity's control.

Reuse of Media

Entities should consider the cost versus benefit of reuse. It may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options.

Clear / Purge / Destroy

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite user-addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user- addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface.

	The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
Purge	Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. • *Disintegrate, Pulverize, Melt, and Incinerate*. These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • *Shred*. Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media). The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

Table 5-1 – Sanitization Methods
(*from NIST 800-88, Rev. 1, Guidelines for Media Sanitization*)

Validation

Entities must test a representative sampling of media for proper sanitization to assure that proper protection is maintained.

Verification of Equipment

If the entity is using sanitization tools (e.g., a degausser), the entity must have procedures to ensure that the tools are operating effectively.

Verification of Personnel Competencies

Entities must ensure that equipment operators are properly trained and competent to perform sanitization functions.

Document

Entities must maintain a record of their sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media.

5.0 Interpretation

The office of the CISO in conjunction with Queens College General Counsel if necessary has the authority to interpret this policy.

6.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

7.0 Definitions of Key Terms

Term	Definition
Sanitation	Sanitation of a hard drive or other electronic medium means placing the medium in a condition so that the prior data stored on it cannot be read or recovered.
Electronic Media	Electronic Media refers to any device that can store data and includes, but is not limited to, computers (servers, desktop, laptop and tablets), disk drives, portable disks, backup tapes, CD-ROMS, flash/thumb drives, portable drives, cell phones and PDAs.

8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Officer
Damon Vogel
CISO@qc.cuny.edu

9.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	**Description of Change**	**Reviewer**
9/20/22	Initial Changes to apply to Queens College	DVogel
07/12/2023	More Changes to Apply to Queens College	DVogel
09/08/2023	Added #11, Aligned to Gartner Recommendations	DVogel

10.0 Related Documents

11.0 External Documents

NIST 800-88, Rev. 1, Guidelines for Media Sanitization