Media Disposal, Destruction and Redeployment Protocol

ITS Protocol

Pursuant to the University at Albany Information Security Policy, this protocol is established as part of the Infrastructure Management Security Domain.

Security Domain

Infrastructure Management Security: Protocols, standards and procedures to create and maintain prioritized, reasonable, and appropriate safeguards and controls for the University’s information infrastructure (databases, storage media, workstations, PDAs, mobile and handheld devices, servers, network devices, wireless access points, firewalls, etc.), along with measures to ensure compliance.

Objective

This protocol assures that University business information, in all formats and forms of storage, is effectively removed or destroyed in compliance with the Memorandum dated June 23, 2005, issued by the Commissioner of OGS, and New York State Information Security Policy (P03-002).

Background

The University collects, produces, and shares a wide range of business information as it engages in its core operations of teaching, learning, and research. This information is augmented by collaborations and contracts with a broad spectrum of academic, commercial, and non-profit partners, both domestically and internationally. Because much of this information is regulated or sensitive in nature, it is vitally important that the University takes appropriate precautions to protect the confidentiality of this information when the media that contains the data is re-purposed, disposed of, surplused, or otherwise redistributed or removed from the control of the University’s business, academic, or research entities, and their designated partners.

As electronic storage becomes the primary method of formatting and retaining information, the proper disposal and sanitation of electronic, optical, and magnetic media must be addressed.

Business Information

Business Information should be construed to include not only sensitive, personally identifiable information such as Social Security Numbers and Credit Card Numbers, but also to include information such as letters of recommendation, personnel actions, University IDs, student grades or projects, health records, research and commercial data, and material such as software and databases licensed for use on University computers.

The University will establish formal processes for all forms of information storage, regardless of location, that will assure that the University’s sensitive information is properly sanitized, disposed of, or destroyed when the media used to store that information is earmarked for redistribution, disposal, destruction, surplus, or exchange.

The means used to sanitize or destroy media shall be in accordance with generally accepted and recommended practices designed to prevent information from being recovered from the media.

Scope

This protocol applies to all University at Albany business and academic units. Academic departments, business units, and affiliated corporations shall exercise due care in assuring that vendors and partners comply with requirements to properly remove, return, or destroy University information.

Roles and Responsibility

It is primarily the responsibility of University Data Owners, or their designates, to develop local procedures to assure that the unit is in compliance with this standard and its associated procedures governing the removal, disposal, destruction, surplus, re-distribution, or exchange of media containing sensitive institutional data.

- Each academic department, business unit, and affiliate shall designate or otherwise appoint an employee responsible for overseeing the proper removal and/or destruction of media containing University information.
- The designated employee will prepare and sign the Media Certification section of the OEM Report of Surplus Property form.
- As part of their Internal Controls activities, academic departments and business units will report to the University Internal Control coordinator on their efforts to comply with this protocol during their regular Internal Controls reviews.

Compliance

Compliance with this standard and its related procedures will be in accordance with the Compliance section of the University’s Information Security Policy.
Exceptions

Special situations may arise that prevent or make it excessively difficult for units to comply with this standard. To accommodate such situations, alternate methods of preserving the confidentiality of sensitive institutional data can be substituted.

Exceptions must be:

- Requested from the ISO
- Submitted in written form with the authorization of the employee responsible for compliance.
- Provide an explanation for the exception request that includes a comprehensive description of the information contained on the media, and why the unit cannot comply with the standard and/or its related procedures.

Notwithstanding the status of the exception request, Data Owners are responsible for assuring compliance with this standard.

Review

This protocol will be reviewed and evaluated no less than once every three years.

Location of Links to Documents for Electronic Versions of the Policy

Related Documents

Memorandum dated 06/23/2005 from OGS Commissioner Daniel Hogan

NYS Information Security Policy (P03-002)[3]

New York State legislation governing the collection, retention, and dissemination of personally identifiable information[4] (“private data”)

Standard and procedures documents detailing specific tools and techniques for sanitizing and destroying various media (https://csrc.nist.gov/publications/detail/itl-bulletin/2015/02/nist-special-publication-800-88-revision-1-guidelines-for-media/final)

--------------------------------------------------------------------------------


2. Data Owners are the business, academic, or research entities that are primarily responsible for collecting, creating, or using the data. They should not be confused with Data Custodians who are responsible for implementing the Data Owners decisions regarding access and usage.

3. Section 7: Physical and Environmental Security Policy

Secure Disposal or Re-Use of Storage Media and Equipment

There is a risk of disclosure of sensitive information through careless disposal or re-use of equipment. Formal processes must be established to minimize this risk. Storage devices such as hard disk drives and other media (e.g., tape, diskettes, CDs, DVDs, cell phones, digital copiers, or other devices that store information) or paper containing sensitive information must be physically destroyed or securely overwritten to prevent unauthorized disclosure of sensitive SE information.

4. NYS Information Security Breach and Notification Law

Last Updated September 2019

Need more help? Contact the ITS Service Desk.