REDISTRIBUTION OF UNIVERSITY COMPUTER EQUIPMENT

Policy Statement

All data on computers or electronic storage devices (including, but not limited to, desktop, laptop, tablets, servers, or handheld devices) must be cleaned and the device reimaged prior to transfer to another user.

Reason for Policy/Purpose

This policy is intended to prevent the inadvertent release of confidential, protected, or personally identifiable information (PII) contained on electronic storage devices when physical possession or stewardship is changed. Furthermore, it seeks to promote compliance with federal and state data protection regulations as it pertains to personally identifiable information and financial records.

Who Needs to Know This Policy

All members of The University of Southern Mississippi (USM) community.

Website Address for this Policy

www.usm.edu/institutional-policies/policy-ACAF-IT-025

Definitions

Cleaning - A process used to assure that data is erased permanently.
Device – An instrument used to process or store digital records and data; including, but not limited to, personal computers, workstations, laptops, tablets, externally connected hard drives, flash drives, removable media, and any other equipment or media capable of electronically storing data. The policy applies to university-owned electronic equipment (including those devices purchased with grant funds).

Personally Identifiable Information (PII) – Information that can be directly related to an individual.

Reimage – Is the process of overwriting or installing an entire storage device with a new operating system and selected software.

Removable media – Includes but is not limited to floppy diskettes, compact disks (CD), magnetic tapes, digital video disks (DVD), Zip media, flash media, and all other similar storage devices that are easily removed from a device.

User – Any individual that has been given the authority to use a USM owned device.

---

**Policy/Procedures**

1.0 **Policy**

1.1 When the responsible party for a University device changes, the data stored on the device must be cleaned. Users must initiate the data cleaning process, as appropriate for each case listed below:

1.1.1 For a “Device Transfer” (the responsibility and possession of a device is being transferred from one department, business unit, administrative area, or individual to another), the user of the device must contact the iTech Help Desk and arrange to have the device cleaned and reimaged.

1.1.2 For a “Computer Exchange Program (CEP) transaction” (a device is either exchanged with, or returned to, the CEP program), the user of the device must contact itcep@usm.edu. A valid, complete backup of all necessary data should be completed prior to contracting IT CEP (see item 2.3).

1.1.3 For a “User Status Change” (the employment status of a user changes. Changes can include, but are not limited to: resignation, retirement, position elimination, termination, or death), the user’s supervisor must contact the iTech Help Desk and arrange to have the device cleaned and reimaged (see item 2.3).

1.1.4 For a “Surplus device” (when a device is to be released from the University inventory), the user will follow the Disposition of Surplus Property Process as defined in the following policy: https://www.usm.edu/institutional-policies/policy-adma-pur-017.
1.1.5 For any other case involving the change of parties responsible for a device, please contact the iTech Help Desk for guidance.

1.2 With the exception of iTech employees, no one should attempt to clean the device. Any attempt to do so will not satisfy the policy requirements.

1.3 Exceptions
1.3.1 An exception of this policy can be considered in cases when the cleaning of the device would have a significant negative impact on business processes.
1.3.2 The chair, director, or unit manager must submit a request to the Help Desk through a work order for an exemption, which must include:
   1.3.2.1 The reason for the exemption
   1.3.2.2 A description of compensating actions to address the removal of information
   1.3.2.3 A specific deadline for the completion of any compensating actions
1.3.3 The exemption request will be reviewed by the Chief Information Officer, Technology Security Officer, and General Counsel.
1.3.4 Once the request has been reviewed, it may either be allowed or denied. For either outcome, the requester will be notified by email about the decision.
1.3.5 For requests that have been denied, the specific reason will be cited with the request and the device must be cleaned per the requirements of this policy.

2.0 Retention of Data
2.1 If the University owned device contains University data which should be retained by the University /department /administrative unit, this information should be properly saved and backed up prior to the cleaning and reimaging performed by iTech.

2.2 It is the responsibility of the department to ensure that such University data files necessary to be retained are properly backed up prior to the cleaning and reimaging performed by iTech.

2.3 A backup must be obtained of any University device that is being reassigned due to separation of its assigned user from University employment, either through resignation, retirement, death, termination, position elimination or any other means. The employing department of the separating employee must immediately notify iTech of such separation by placing a work order through the Help Desk to initiate the computer backup process and subsequent cleaning and reimaging of the device. This device backup may be accessed for future business use by the University at its sole discretion and without notice.

2.3.1 Data captured by the backup will be retained for 180 days, unless direction is given by University General Counsel, University Police Department, or Human Resources to hold the data backup for a time period beyond 180 days.
2.3.2 Once a data backup has been held for 180 days, the data backup will be purged and information from that device will no longer be available, with exception of data backups directed to be held for longer than 180 days.

2.4 iTech can archive files for the user, but it will be the user’s responsibility to explicitly indicate which files and data must be retained.

2.5 USM, iTech, its agents and employees cannot be held responsible for data lost due to the cleaning process.

2.6 If you have particular concerns about the data on a device, contact the iTech Security Team at infosec@usm.edu for recommendations and assistance.

3.0 Devices Taken Out of Service

3.1 When the University device is being taken out of service and sent to surplus (the device is to be released from the University inventory), the user will follow the Disposition of Surplus Property Process as defined in the following policy: https://www.usm.edu/institutional-policies/policy-adma-pur-017.

4.0 Enforcement

4.1 Any faculty or staff found to have violated this policy will be subject to disciplinary action, up to and including suspension, expulsion and/or termination of employment in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.

4.2 Violations of any provision of this policy may result in civil liability and/or criminal penalties as prescribed by federal and state laws.

Review

The Chief Information Officer is responsible for the review of this policy every four years (or whenever circumstances require immediate review).

Forms/Instructions

N/A

Appendices

See Appendix A for Flowchart
Related Information

See ADMA-PUR-017 Property Accounting – Policies and Procedures

History

Amendments: Month, Day, Year – summary of changes

10/28/13 – Creation

1/9/14 – Added Flowchart as Appendix A

3/3/14 – minor changes to Flowchart

9/26/15 – Updated policy references and minor additions related to security for legal compliance
Authorization

RECOMMENDED BY:

Responsible University Administrator

Responsible University Officer

REVIEWED BY:

Director of Compliance

Date

Office of General Counsel

Date

APPROVED:

President

Date