Data Governance & Classification Policy 9.1.1.B – Minimum Safeguards

Background

The various units and departments at the university have a multitude of types of documents and data. To the extent particular documents or data types are not explicitly addressed within this document, it is the responsibility of the Data Trustee to classify data by considering the potential for harm to individuals or the university in the event of unintended disclosure, modification or loss. Departments must be particularly mindful to protect sensitive personal information, such as social security numbers, Driver's license numbers and financial account numbers; the disclosure of which may create risk of identity theft.

Minimum Safeguards by Classification Level

This document describes the actions necessary to secure and protect university-owned data classified as Export Controlled data, Restricted data, Controlled data and Public data.

Export Controlled

As a means to promote national security, the U.S. Government controls export of sensitive data, equipment, software and technology, this data is labeled **Export Controlled**. Users of Export Controlled data must follow all the safeguards for Restricted data plus additional safeguards as directed by Export Controls Office. The Data Trustees, Stewards, Custodians and Users of systems that have Export Controlled data are responsible to work with the Export Controls Office to identify appropriate additional safeguards. The Export Controls office must be contacted for information on proper disposal of electronic equipment that contains Export Controlled data.

Restricted

Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates. Users of Restricted data must follow all the safeguards for Controlled data plus additional safeguards. High levels of security safeguards must be applied to Restricted data.

Controlled

Data should be classified as Controlled when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. By default, all institutional data that is not explicitly classified as Export Controlled, Restricted, or Public data must be treated as Controlled data. A reasonable level of security safeguards should be applied to Controlled data.

The table on the next 4 pages contain safeguards for Restricted and Controlled data.

Data Classification		General Safeguards
Controlled	**Restricted**	
Recommended	**Mandatory**	Security software must be installed, enabled and kept up to date to protect against malicious applications, viruses, spyware and malware-based attacks.
Recommended	**Recommended**	Encrypt via full disk encryption, university owned desktop computers.
Recommended	**Mandatory**	Encrypt via full disk encryption, university owned laptop computers.
Mandatory	**Mandatory**	Users must have unique and individual user credentials such as a user id and password per the Password Policy.
Recommended	**Mandatory**	Desktop and Laptop computers must be configured to utilize a pattern-hiding display lockout after an inactivity period of 30 minutes or less. Users must utilize session lockout for temporary absences.
Recommended	**Mandatory**	Laptop computers must be secured via cable locks if not stored in a locked office or locked desk when left unattended.
Recommended	**Mandatory**	A local firewall must be installed and enabled.
Mandatory	**Mandatory**	Servers, data storage devices and other IT equipment must be kept within secure areas with an appropriate level of physical and environmental controls to protect these resources.
N/A[1]	**Mandatory**	Internal forms must be revised to eliminate unnecessary references to SSN.
N/A[1]	**Mandatory**	SSNs should not be stored or used whenever possible, UCID's should be used instead.
Recommended	**Mandatory**	Data stored, used or accessed by an external service provider or agent must have contractual agreement to provide appropriate protection to the same standards as applied at the university. The contract must implement the Data Security Rider and undergo a Security Review.
Recommended	**Mandatory**	Data must not be discussed outside of the workplace or with anyone who does not have a specific "need to know".
Recommended	**Mandatory**	Electronic equipment containing Restricted or Controlled data must be securely sanitized, transferred or disposed of in a secure manner before leaving possession of the responsible university department.
		• University owned equipment removed for off-site maintenance must be sanitized of any restricted data.
		• The Electronic Media Sanitization Standard: http://www.uc.edu/content/dam/uc/infosec/docs/Standards/Electronic_Media_Sanitization_Standard_9.1.8.pdf
		• The Asset Disposition Policy 2.1.15 governs the disposition of all university owned assets and is located at: http://www.uc.edu/content/dam/uc/af/financialpolicies/Docs/assetdisp_pol.pdf

Data Classification		General Safeguards - continued
Controlled	**Restricted**	
Recommended	**Mandatory**	Office doors must be closed and locked when away from your office, or desk/cabinet drawers/doors must be closed and locked when away from your desk.
Mandatory	**Mandatory**	A robust authentication process consistent with the level of risk associated with unauthorized access is required for access to all Restricted and Controlled data.
Recommended	**Mandatory**	Limit Information system access to the types of transactions and functions that authorized users are permitted to execute.
Recommended	**Mandatory**	Limit access to Restricted data to only those who require access to perform their job functions.
Recommended	**Mandatory**	Separate high-risk business functions across multiple users/roles as appropriate.
Mandatory	**Mandatory**	User access and login information must be maintained. Security logs must be enabled to maintain a complete, tamper-proof audit trail of all processes initiated by the system and should be forwarded to the central log management system.
Recommended	**Mandatory**	All portable storage devices must be encrypted (i.e. USB drives, hard drives, CD's, DVD's and other portable media.)
Recommended	**Mandatory**	Data must be encrypted when in transit, both inside and outside of the university network.
Recommended	**Mandatory**	Scans of university owned systems must be completed quarterly, as well as real-time scans of files from external sources.
Recommended	**Mandatory**	Configure system to end a user session after a predetermined time based on duration and/or inactivity of session.
Recommended	**Mandatory**	Data Stewards must maintain an updated listing of all systems supported and listing of data types stored and processed.
Recommended	**Mandatory**	Data at rest, outside of an enterprise supported, institutional, university system, must be encrypted.
Recommended	**Mandatory**	FIPS-validated cryptography must be used to secure university data.
		Data Access
Mandatory	**Mandatory**	Data access will be granted only when specifically authorized and warranted based on job function. The supervisor of the employee is responsible for reviewing access need.
Mandatory	**Mandatory**	Once data access is approved, Data Stewards are responsible for notification of the following information specific to the data being requested: • Data documentation and usage guidelines. • Data classification including information on associated state and federal regulations. • Required minimum safeguards for protected data.
Mandatory	**Mandatory**	Data access authorizations must be reviewed on an annual basis by each Data Steward to ensure that access remains appropriate.
Mandatory	**Mandatory**	Access must be deactivated after a period of inactivity not to exceed 12 months.
Mandatory	**Mandatory**	The supervisor of a transferred employee has 48 hours to confirm that access to applications and resources that need to follow an employee remain in place and that access to applications and resources that do not need to follow an employee are removed.

Data Classification		Data Access - Continued
Controlled	**Restricted**	
Mandatory	**Mandatory**	Separated employees and affiliates shall lose all employee/affiliate level access as of their separation date unless it is necessary to remove access prior to separation date.
Mandatory	**Mandatory**	Access Control Lifecycle (creation, maintenance, removal) and Business Workflow (adding/removing access) must be documented.
N/A[2]	**Mandatory**	Anyone accessing or having access to Restricted data must have passed a background check as defined by the university prior to authorization of access to Restricted data. This includes all faculty, students, staff, student workers and affiliates.
Mandatory	**Mandatory**	Any non-university employee accessing Restricted or Controlled data must be sponsored by an employee of the university. The approval process for granting such access must follow the policy of the appropriate Data Trustee. Any non-university individuals accessing university data at the University of Cincinnati are required to comply with federal and state laws and university policies and procedures regarding data security. Sponsorship of access must be reviewed and renewed every 6 months. Access approval records must be maintained according to the appropriate Record Retention schedule.
Recommended	**Mandatory**	If accessing restricted data or if required by compliance regulation, logon banner or similar communication must be implemented and display appropriate notices.
Recommended	**Mandatory**	Other than email, only university owned devices may access Restricted data.
Recommended	**Mandatory**	Unpublished research information may only be accessible by those with a "need-to-know".
		Cloud Based File Storage
Mandatory	**Mandatory**	Users must utilize approved cloud-based file storage for university data.
Recommended	**Mandatory**	Restricted data is only permitted in secure folders where syncing is disabled.
Recommended	**Mandatory**	Sharing is permitted only on a "need-to-know" basis and needs to be approved by the appropriate Data Trustees or Data Stewards for any sharing outside of UC.
		Paper Documents, Printers & Fax Machines
Mandatory	**Mandatory**	"Clean desk practices" must be in place. Paper documents containing Restricted or Controlled data must not be left unattended and must be protected from the view of passers-by or office visitors. It is recommended that confidential documents contain a cover sheet.
Mandatory	**Mandatory**	Paper documents must be shredded when discarded.
Recommended	**Mandatory**	Lock file cabinets containing Restricted or Controlled data before leaving the office each day. Utilize a controlled key system for the file cabinets keys or appropriately secure the area.
Mandatory	**Mandatory**	Store paper documents that contain information that is critical to the conduct of university business in secure file cabinets and keep copies in a secure alternate location.
N/A[1]	**Mandatory**	Paper copies of all documents with SSN must be stored in locked filing cabinets and must be shredded when discarded.
Mandatory	**Mandatory**	Printers and fax machines must be located in a low traffic area that is not accessible to those not authorized to receive the information.
Mandatory	**Mandatory**	Immediately retrieve or secure documents containing university data as they are printed on copy machines, fax machines or printers. Use “Secure Print” if available.

Data Classification		Paper Documents, Printers & Fax Machines
Controlled	**Restricted**	
Mandatory	**Mandatory**	A UC fax cover sheet must be used. The cover sheet must contain a confidentiality statement and contact information for the recipient in the event the fax is received in error.
Mandatory	**Mandatory**	The fax number of the recipient should be confirmed prior to sending a fax by calling the person or office to which the fax will be sent. Programmed fax numbers should be checked regularly for accuracy.
University Owned Mobile Device		
Mandatory	**Mandatory**	A minimum four-digit PIN, passcode, fingerprint biometric or pattern must be used to access the device.
Mandatory	**Mandatory**	An inactivity timeout to automatically lock the device after a maximum of 5 minutes. (A one minute timeout is recommended.)
Mandatory	**Mandatory**	Device encryption must be enabled.
Mandatory	**Mandatory**	Automatic data wiping after ten failed PIN, passcode, or pattern attempts must be enabled.
Mandatory	**Mandatory**	The ability to remotely remove university-owned data from a lost/stolen device upon user or department request or advisement of the Office of General Counsel must exist.
Mandatory	**Mandatory**	Unapproved file sharing applications must not be installed or must be disabled.
Mandatory	**Mandatory**	Physical control of mobile devices must be maintained. Users and departments must know of location at all times to limit the risk of unauthorized use.
Mandatory	**Mandatory**	Users must ensure adequate security and utilize university approved VPN to send or receive university data over public Wi-Fi networks.
Mandatory	**Mandatory**	Users and departments must delete all stored university data before reusing, repurposing or discarding the mobile device. See Electronic Media Sanitization Standard for guidance.
Non-University Owned Mobile Device Accessing UC Exchange Servers		
Mandatory	**Mandatory**	It is understood that some users may inadvertently have email that contains Restricted or Controlled data from the UC Exchange email server on a non-university owned device. Before a user can access the UC Exchange email servers with a non-university owned mobile device, the device must meet the following minimum standards:
		• A minimum four-digit PIN, passcode, fingerprint biometric or pattern to access the device
		• An inactivity timeout to automatically lock the device after a maximum of 5 minutes. (A one minute timeout is recommended.)
		• Device encryption enabled.
		• Automatic data wiping after ten failed PIN, passcode, or pattern attempts.
		• Enable the ability to remotely remove university-owned data from lost/stolen devices upon user's request or advisement of the Office of General Counsel.

Non-University Owned Computer Accessing UC Exchange Server Email			
Mandatory	**Mandatory**	It is understood that some users may inadvertently have email that contains Restricted or Controlled data from the UC Exchange email server on a non-university owned computer. Before a user can access the UC Exchange email server with a non-university owned laptop, the device must meet the following minimum standards:	
		•	Password that complies with university Password Policy
		•	An inactivity timeout (screen saver) to automatically lock the device after a maximum of 5 minutes. (A one minute timeout is recommended.)
		•	Virus Protection must be installed, up to date and running. Faculty, students and staff of the university can download virus protections at http://www.uc.edu/infosec/antivirus.html
		•	Firewall must be enabled

N/A[1] data with social security number is Restricted data, safeguard is not applicable for Controlled data classification.
N/A[2] Access to Controlled data does not require background check.

Public

Public data is information that may be disclosed to any person regardless of their affiliation with the university. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original source documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the university community and no steps need to be taken to prevent its distribution.

Related Links

Data Governance & Classification Policy

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History

Issued: 07/01/2009
Revised: 05/30/2014
Revised: 01/25/2017
Revised: 10/25/2017
Revised: 09/26/2018
Reviewed: 09/25/2019