Data Classification & Handling Policy for Chicago State University

Policy Statement

Chicago State University (CSU) Information Technology Division (ITD) stores, processes, and transmits sensitive data as a part of its everyday operations. To minimize the risks to the confidentiality and integrity of this data a consistent system of classification of that data and the specifications for its handling through the useful life of that data is necessary to protect all members of the CSU community.

Purpose

The purpose of the CSU Data Classification and Handling Policy is to provide a framework for classifying and handling Information Resources according to the risks associated with its storage, processing, transmission, and destruction.

Scope

This policy applies to any individual, entity, or process that interacts with any CSU Information Resource.

Definitions

Information User

- The person, organization or entity that interacts with Information for the purpose of performing an authorized task.

Information Owner

- The person responsible for, or dependent upon, the business process associated with an information asset.

Information Custodian

- Maintains the protection of Information according to the information classification associated to it by the Information Owner.
- Delegated by the Information Owner and is usually Information Technology personnel.

Responsibility

Information User

- Has a responsibility to use Information in a manner that is consistent with the purpose intended and in compliance with policy.

Information Owner

- The person responsible for, or dependent upon, the business process associated with an information asset.
- Identifies the Information Custodian and will typically be ITD personnel.

Information Custodian

- Responsible for establishing and maintaining the protection of Information according to the information classification associated to it by the Information Owner.

Policy

Information Classification

- Information owned, used, created, or maintained by CSU should be classified into one of the following three categories:
    - Public
    - Internal
    - Confidential

Public Information:

- Is information that may or must be open to the general public.
- Has no existing local, national, or international legal restrictions on access or usage.
- While subject to CSU disclosure rules, is available to all CSU employees and all individuals or entities external to the corporation.

*Examples of **Public Information** include:*

- Publicly posted press releases,
- Publicly available marketing materials,
- Publicly posted job announcements.

Internal Information:

- Is information that must be guarded due to proprietary, ethical, or privacy considerations.
- Must be protected from unauthorized access, modification, transmission, storage, or other use and applies even though there may not be a civil statute requiring this protection.
- Is restricted to personnel designated by CSU, who have a legitimate business purpose for accessing such Information.

Examples of Internal Information include:

- Employment Information,

- Business partner information where no more restrictive confidentiality agreement exists,
- Internal directories and organization charts,
- Planning documents,
- Contracts.

Confidential Information:

- Is information protected by statutes, regulations, CSU policies or contractual language. Information Owners may also designate Information as Confidential.
- Is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a "need-to-know" basis only.
- Disclosure to parties outside of CSU must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.

Examples of Confidential Information include:

- Customer data shared and/or collected during a consulting engagement,
- Financial information, including credit card and account numbers,
- Social Security Numbers,
- Personnel and/or payroll records,
- Any Information identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction,
- Any Information belonging to a CSU staff member, associate or student that may contain personally identifiable information,
- Patent information

Information Handling

All Information should be labeled according to the CSU Labeling Standard.

Public:

- Disclosure of **Public Information** must not violate any pre-existing, signed non-disclosure agreements.

Internal:

- When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords as defined in the Authentication Standard.
- Access should. Be limited based on job role or "need to know".
- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
- Must be protected by a confidentiality agreement before access is allowed.

- Must be stored in a closed container (i.e., file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Is the "default" classification level if one has not been explicitly defined.

Confidential:

- When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords as defined in the Authentication Standard.
- When stored on mobile devices and media, must be encrypted.
- Must be encrypted at rest.
- Must be stored in a locked drawer, room, or area where access is controlled by a cipher lock and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- Must not be transferred via unsecure communication channels, including, but not limited to:
    - Unencrypted email
    - Text messaging
    - Instant Messaging
    - Unencrypted FTP
    - Mobile devices without encryption
- When sent via fax, must be sent only to a previously established and used address or one that has been verified as using a secured location.
- When transmitted via USPS or other mail service, must be enclosed in a sealed security envelope.
- Must not be posted on any public website.
- CSU Management must be notified in a timely manner if Information classified as **Confidential** has been or is suspected of being lost or disclosed to unauthorized parties.

Information Retention & Destruction

- All information stored by CSU must be stored in accordance with the CSU Information Retention Schedule.
- All information maintained by CSU must include a documented timestamp or include a timestamp as part of metadata.
- Information that is no longer required to be maintained by CSU is classified as "Expired" and must be destroyed in accordance with CSU Information Reuse and Destruction Standards.
- Information owners should be consulted prior to information destruction and may have the opportunity to extend Information expiration, given business needs and/or requirements for the extended retention.
- CSU customers may have their own information retention requirements that supersede CSU's requirements. Such customer requirements should be documented in contractual language.

Policy Exceptions and Maintenance

Waivers from certain and specific policy provisions may be sought following the CSU ITD Approval Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted by ITD.

Enforcement

This Data Classification and Handling Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between CSU policies, they must be brought to the attention of CSU for immediate reconciliation.

Procedures used for Data Destruction and Device tracking

1) Use Absolut Device endpoint management to Track Windows Devices, using Absolut we can freeze lost laptops, remotely Wipe the data on them.
2) Use JAMF Mobile device management for IOS and Mac OS devices, using JAMF we can track devices, and remotely freeze them, wipe the data on them.
3) Use the Nexstar Hard drive wiping device, to perform a comprehensive format of the hard drive before disposing of any hard drive or returning to the state.
Along with this, we also use BitLocker for employee laptops for departments like Financial Aid, Bursar, Cashiers, HR and Legal to add an additional layer of encryption to confidential and sensitive data.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

References

- NIST CSF: ID.AM-5, PR.DS-5, PR.IP-6, PR-DS-7

Version History

Version	Modified Date	Next Review	Approved Date	Approved By	Comments
1.0	11/3/2022	11/1/2023	11/6/2022	Donna Hart	
1.1	09/27/2023	09/27/2024	09/27/2023	Donna Hart	