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

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 sJ 0 Thuc nformation.

Eamples of IJ 08 (n)fe9rn(t)a5ti3 (e)20 Tl.rnal include:

- Employmet Iformation,

- 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
  -

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