Data Elements Secure Storage & Exchange

The Data Elements Secure Storage & Exchange table lists individual data elements that must be treated as Confidential or Sensitive, due to legal, contractual, and risk-based objectives. If you are dealing with one of these data elements and evaluating new processes or storage and sharing options, then you need to contact the ITFS Office of Information Security for review and assistance.

Secure File Storage & Sharing Guidelines

About
- The data classifications listed below are recommended categories to help evaluate and differentiate university data based on associated risks.
- Note: Normal risks should be classified based on the data elements that would have the most restrictive classification.

Data Management Standards: The objective of this standard is to clearly define the role, responsibility, and specific requirements needed to provide secure and optimal management of data to support the University's mission.

Data Classification

Confidential (High Security)
- Data whose unauthorized disclosure and/or loss of control would result in significant financial losses, reputational damage, or impact to the efficient conduct of the university mission.
- Confidential data often have these attributes:
  - Protection of this data is prescribed within legal and/or contractual requirements.
  - Not considered a public record subject to disclosure (F.S. 119).
  - Handling of this data addressed by detailed data security requirements.

Examples:
- Personal identifiers: Social Security Numbers, Driver’s License Numbers, State Identification cards or Passport Numbers.
- Financial data: Credit Card Numbers, Bank Account Numbers, Checkings/Accounts Numbers.
- Authentication Data: Username, Passwords, Digital Signatures
- Health Information: Protected Health Information (PHI)

Sensible Data (Medium Security)
- Data that is considered private and must be protected, but has a lesser degree of impact associated with unauthorized disclosure or loss of control versus confidential data.
- Sensitive data often have these attributes:
  - Protection measures not prescribed by legal or contractual requirements.
  - Access and rights established around identified processes and procedures.
  - Handling of this data requires enhanced security requirements.

Approved Storage
- Application Secure Data should only be stored on authorized data sources or approved storage solutions. A list of shared services includes:
  - Share
  - Google Drive
  -Box
  - Secure Exchange

Approved Storage
- Application Secure Data should only use approved file-sharing solutions:
  - Share

Internal Data (Standard Security)
- Data that is proprietary or is highly sensitive for only users of the University community who have a legitimate purpose to access such data.
- Internal data often have these attributes:
  - Access established for fulfillment of daily business requirements.
  - Handling of this data requires general security requirements.

Approved Storage
- Internal Data should only be stored and shared via University-owned, maintained, or purchased devices, solutions, and services.

Public Data (Minimum Security)
- Institutional information that has few restrictions or is intended for public use.
- There are no security restrictions or guidelines for Public Data.