Data Classification Policy

Purpose

The purpose of the data classification policy is to define different classifications of data and to describe principles for access, use, and safeguards of data based on classification.

Scope

This policy applies to all members of the East Stroudsburg University community (staff, faculty, students, contractors, consultants, visitors, etc.) while using East Stroudsburg University's computing or networking resources. All users are expected to be familiar with and comply with this policy.

Policy

Data and information assets are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection. Three levels of data classification will be used to classify University Data based on how the data are used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

East Stroudsburg University Data Classifications:

Confidential - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Disclosure requires the information custodian's approval for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the University or affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations or University contracts. Confidential data has a very high level of sensitivity. Examples include:

- Social Security Number
- Driver's License Number
- Passport number or other identification number issued by the United States Government
- Individual Taxpayer Identification Number
- Financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account
- Personnel records
- Medical records Any other Personal identity information (PII) as defined by State Government.

Internal Use Only- Data intended for internal University business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal Use Only data is generally not made available to parties outside the East Stroudsburg University community. By default, any data that is not explicitly classified as Confidential or Public data should be treated as Internal Use Only. Internal Use Only data generally has a low to moderate sensitivity. Examples include:

- Financial accounting data that does not contain confidential information
- Departmental intranet
- Information technology network diagrams
- Employee or Student ID number
- Student educational records
- Budget information

- Research and manuscripts
- Payroll and employment documentation
- Strategic or differentiating documentation unique to East Stroudsburg University
- Directory information for students, faculty, and staff who have requested non-disclosure

Public - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the University, affiliates, or individuals. Public Data may be publicly accessible but does not require public access. Public data generally has a very low sensitivity. Examples include:

- East Stroudsburg University's public website
- Directory information for students, faculty, and staff (except for those who have requested non-disclosure)
- Course descriptions
- Schedules and Calendars
- Marketing material
- Press releases
- Social Media
- Maps

Revision History

Version Number	***Date***	***Author***	***Description***
1.0	*June 20, 2022*	*Robert E. Smith, Ed.D.*	*Initial Document*