

***Security Classification and Handling Policy***

1. ***Purpose***

*This document aims to provide a simplified security handling and categorization policy for instructional purposes. Based on the categorization level of the data, this policy attempts to give precise instructions for data classification and the proper protocols for safe data transfer, storage, and transportation. Our goals in putting this policy into effect are to safeguard confidential data, uphold data integrity, and encourage awareness of information security best practices in a learning environment.*

1. ***Scope***

*This document outlines the security classification and handling policy for all information assets managed within the organization. It applies to all employees, contractors, students, and others accessing the organization’s data. The policy covers data classification into different sensitivity levels and provides guidelines for the secure storage, transmission, and handling of information based on its classification.*

1. ***Overview***

*To successfully categorize and secure any data, we must first describe the data and specify the amount of protection required. This policy defines in which all data can be leveled:*

**Level 1: Public Access**

* ***Description:*** *Data designated as "Public Access" is freely accessible to everybody and meant for wide dissemination. There is no risk to the organization if this data is published because it is not sensitive. Some examples are publicly available site information, press releases, marketing materials, and general university announcements.*

**Level 2: Restricted Use**

* ***Description:*** *Data marked as “Restricted Use" should only be used internally by authorized staff members and not be distributed outside the company without authorization. Information at this level could have a moderate impact on operations or privacy if it were made public. Internal reports, sensitive research data, staff directories, and student grades are a few examples.*

**Level 3: Confidential**

* ***Description:*** *Information deemed “confidential" must be cautiously handled and safeguarded. People with a legitimate need to know are the only ones who can access this data. Unauthorized disclosure could seriously hurt the company, the people involved, or the observance of the law. Financial documents, intellectual property, personally identifiable information (PII), and sensitive research findings are a few examples.*

1. ***Handing Procedures/Guidelines***

*Detailed instructions for processing data securely according to its classification level are given in this section. It delineates precise protocols for information storage, transmission, and physical conveyance, guaranteeing data security against unapproved access, revelation, or manipulation throughout the entire process. These processes are intended to protect the integrity and confidentiality of information per the organization’s data security goals.*

***Table1: The handling procedures/guidelines for each level of data***

|  |  |  |  |
| --- | --- | --- | --- |
| *Classification Level* | *Storage* | *Transmission* | *Transport* |
| *Level1: Public Access* | *Store in shared or public locations.* | *Transmit via unsecured channels (e.g., standard email, public file-sharing).* | *No special precautions are needed; transport freely.* |
|  | *No encryption is required.* | *- No encryption necessary.* | *- No labeling or tracking required.* |
| *Level2: Restricted Use* | *Store in secure, access-controlled environments (e.g., internal servers, restricted cloud services).* | *Use secure methods (e.g., encrypted email, SFTP, VPN).* | *Transport using encrypted USB drives or sealed, labeled envelopes.* |
|  | *Recommended encryption at rest.* | *Passwords or encryption for attachments are recommended.* | *Track transport and confirm delivery with the recipient.* |
| *Level3: Confidential* | *Store in highly secure environments (e.g., encrypted drives, dedicated servers).* | *Transmit using encrypted end-to-end methods (e.g., secure email encryption, VPNs, encrypted file transfers).* | *Transport using hardware-encrypted media or secure digital storage devices.* |
|  | *Strong encryption at rest is required.* | *Transmit passwords and encryption keys separately.* | *Seal in tamper-evident envelopes labeled "Confidential."* |
|  | *Multi-factor authentication (MFA) is required for access.* | *Only authorized recipients should receive data and maintain transmission logs.* | *Use trusted personnel or secure courier services; maintain tracking and confirmation logs.* |

1. ***Pros/Cons of Classification Levels***

*The advantages and disadvantages of putting in place a three-level data classification system within the company are discussed in this section. By weighing its advantages and potential disadvantages, you will better comprehend how this framework contributes to data protection and what obstacles might occur during its deployment.*

|  |  |
| --- | --- |
| Pros | Cons |
| *Granular Control Over Data Protection* | *Complexity and Administrative Overhead* |
| *Allows for tailored security measures based on data sensitivity.* | *Implementing and managing the system can be complex and resource-intensive.* |
| *Efficient Resource Allocation* | *Risk of Misclassification* |
| *Enables optimal use of security resources, focusing on the most sensitive data.* | *Potential for incorrect classification, leading to either over- or under-protection.* |
| *Clear Guidelines for Data Handling* | *Inconsistent Application Across the Organization* |
| *Provides clear instructions on data handling, reducing ambiguity.* | *Different interpretations may lead to inconsistent classification and handling practices.* |
| *Enhanced Compliance and Risk Management* | *Potential for Over-Classification* |
| *Helps meet legal and regulatory requirements, reducing risks.* | *Data may be classified too conservatively, resulting in excessive security measures.* |
| *Flexibility and Scalability* | *Increased Training Requirements* |
| *Adapts to organizational growth and changes in data types.* | *Ongoing training is required to ensure proper understanding and application of the system.* |