Information Security Classification Standard

Purpose of the Standard: to establish a framework for:

a) classifying Information and information Assets based on Confidentiality; and

b) determining baseline security controls for the protection of Information Assets based on their Confidentiality.

This standard applies to Information Assets regardless of their location.

In this standard:

a) "Confidentiality" defines an attribute of information. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial.

b) "Data Custodian" means an employee who implements controls to ensure the security of Information and Information Assets within the College. The Data Custodian is accountable to the Data Trustee.

c) "Data Trustee" means a member of the Board of Directors. Data Trustees are there to define and approve data-related policies and standards.

d) "Information Assets" means Business Information Assets, computers, IT systems, Hard and soft copy of all forms, policies, procedures and standards (filled/unfilled)

Security Classification

Data Custodians will classify Information Assets with respect to their Confidentiality using one of the following four categories:

Classification	Definition	Examples
Level 1: Public	- Information deemed to be public by legislation and/or under College policy; - Information in the public domain.	name of employees business contact information, college programs, degree awarded, convocation date, annual reports, public announcements, telephone directory etc.
Level 2: Internal Use	- Information not approved for general circulation outside the college -Information the disclosure or loss of which would inconvenience the College	internal memos sent to all members of the college, minutes of college meetings that are circulated to all employees and students, anonymized or de-identified human subject data etc.

Level 3: Confidential	Information that is available only to authorized persons Information; the disclosure or loss of which could seriously impede the College's operations; Adversely affect the College's operation; or cause reputational damage; and obligate the College's to report to the government or other regulating body and/or provide notice to affected individuals	- staff employment applications, personnel files, date of birth, health information and personal contact information - admission applications, student enrollment status, grades etc - information commonly used to establish identity such as a driver's license or passport - intellectual property and authentication verifiers including passwords
Level 4: Restricted	- Information that is confidential; and subject to specific privacy and security safeguards under law, policy or contractual agreement. -Information the loss or disclosure of which could cause severe harm to individuals or Glenbow College; - Information the loss or disclosure of which may obligate Glenbow College to report to the government or other regulating body and/or provide notice to affected individuals	-payment card information including: PAN, cardholder name,CVV2/CVC2/CID; -health information when it can be linked to an identifiable - identifiable human subject research data; -information that is subject to special government requirements in the interests of national security.

Baselines:

1- For convenience, Data Custodians may assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection includes a student's name, program of interest and credit card number, the data should be classified as Restricted.
2- If there is any ambiguity with respect to Confidentiality, the information will be classified as Confidential until it can be definitively classified at a lower level.
3- Data Custodians will reevaluate the classification of Information and Information Assets on a periodic basis to ensure the assigned classification is still appropriate.
4- If a Data Custodian determines that the classification of certain Information and Information Assets has changed, an analysis of security controls will be performed to determine whether existing controls are consistent with the new classification.
5- If gaps are found in existing security controls, the Data Custodian will work with relevant Glenbow College Board to mitigate and/or correct the risk.

Information Asset Protection Requirements

Information Assets will be protected in accordance with the security classification. Refer to Information and Information Asset Access, Transmission and Storage Policy

Effective Date: July 30, 2019