GLENBOW COLLEGE
Inspiring Future Professionals

Information & Information Asset Access, Transmission and Storage Policy

Purpose of the Policy: to establish a framework for access, transmission and storage of information both external and internal stakeholders including but not limited to students, employees and contractors.

In this Policy: Access, Transmission and Storage Policy is based on the Information Security Classification Standard

Security Classification is as follows:

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.

Information Asset Access, Transmission and Storage Requirements:

Level	Labels	Access	Transmission	Storage
1	Public	Read - no restrictions. Write/Edit - limited to Data Trustee or delegate Access Controls - none required	**- no special safeguards required.**	**- no special safeguards required.**
2	Internal Use	Read - limited to employees and other authorized users who have a work-related need to access the information; - access privileges determined by the Data Trustee; and can be based on position or on role definition. Write/Edit - limited to Data Trustee or delegate. Access Controls - access information through the local network or VPN; - password authentication required;	**- Encryption (or similar mechanism):** recommended when transmitting information via public networks (e.g. Internet); **- encryption (or similar mechanism)** optional when transmitting via local network.	Electronic - information must be stored within a controlled access system; - the server must be on a network that is not visible to public networks; - information may be stored on a server that is: o managed and monitored internally; OR managed by a third party and when a contract with the third party is in place (G suite). - Encryption (or similar mechanism): o optional when information is stored within the Colleges IT assets Paper - store records in a locked file cabinet; - access to the cabinet restricted to those authorized by the Data Trustee or designate.

3	**Confidential**	Read - limited to employees and other authorized users who have a work-related need to access the information; - access privileges determined by the Data Trustee; based on position or on role definition. Write/Edit - limited to Data Trustee or delegate. Access Controls - access information through the Local Network or VPN; - password authentication required; - two-Factor Authentication required for remote access.	**- Encryption (or similar mechanism):** recommended when transmitting information via public networks (e.g. Internet); **- encryption (or similar mechanism)** optional when transmitting via local network.	Electronic - information must be stored within a controlled access system; - the server must be on a network that is not visible to public networks; - information may be stored on a server that is: o managed and monitored internally; OR managed by a third party and when a contract with the third party is in place (G suite). Encryption (or similar mechanism): ○ required when information is stored outside the Colleges Data Centre; ○ optional when information is stored on premise. Paper - store records in a locked file cabinet; - access to the cabinet restricted to those authorized by the Data Trustee or designate.
4	**Restricted**	Read - as above for Level 3. Write/Edit - as above for Level 3. Access Controls - as above for Level 3 unless additional controls are required under law or contract.	- as above for level 3 unless encryption (or similar mechanism) is required under law or contract when transmitting via local network.	Electronic - as above for Level 3 unless additional controls are required under law or contract; - encryption (or similar mechanism): as above for Level 3 unless encryption (or similar mechanism) is required under law or contract even when information is stored on premise. Paper - store records in a locked file cabinet; - access to the cabinet restricted to those authorized by the Data Trustee or designate.