Security Classification Guideline for Records, Data and/or Information

Policy reference: AD.1.1 Privacy, AD.3.2 Records Management and AD.3.3 Data Governance

Identifying and applying the correct security classification to records, data and/or information at SAIT is an important tool in protecting access to personal information, protecting confidential and restricted information from unauthorized access, protecting intellectual property and supporting routine disclosure and active dissemination of information. As data or information moves through the information management lifecycle, or as the context in which it exists changes, the applied security classification may need to be re-assessed.

This guideline applies to all records, information or data, regardless of format or state (paper or electronic). Retention and disposition must comply with SAIT's Classification and Retention Schedule.

Security Classification	Description	Examples	Risk Impacts
Unrestricted Not Sensitive	Records, data and/or information created in the normal course of business, that are unlikely to cause harm. Information in the public domain. Unrestricted records are available to the public, employees, contractors, subcontractors and agents working for SAIT.	Information intended for general or public sharing with minimal risk when disclosed, such as job titles, SAIT business email addresses, course/program descriptions, etc.	**Little** or no impact.
Protected Moderately Sensitive	Records, data and/or information that are sensitive and that could affect service levels or performance, which should not be circulated outside of SAIT. Authorized access (to employees, contractors, sub-contractors and agents) is on a need-to-know basis for business-related purposes.	Information intended for limited sharing; disclosure may cause minor inconvenience or embarrassment, such as dates of birth, grades, personal contact information other than SAIT email addresses, sensitive business information, etc.	**Moderate,** potential for spam or targeted marketing. Disruption of business if not available.
Confidential Highly Sensitive	Records, data and/or information that are sensitive within SAIT and could cause serious loss of privacy, competitive advantage, loss of confidence in SAIT programs and/or damage to partnerships, relationships and/or reputation. They are available only to a specific function, group or role.	Third party business information submitted in confidence or sensitive personal information whose unauthorized disclosure could cause significant harm, such as personnel files, including salary data, passport number, medical records, tax information, gender identity, sexual orientation, gender expression, etc.	**High,** potential for identity theft, financial loss, legal implications or personal privacy violations and/or loss of confidence in SAIT's programs.
Restricted Highly Sensitive	Records, data and/or information that are highly sensitive and that could cause extreme damage to SAIT's integrity, image or effective service delivery. They are available only to specific, named individuals (or specific positions).	Information which disclosure could result in severe personal, legal, or financial damage to an individual or to SAIT, such as restricted areas, budget prior to public release, extremely sensitive personal information including, but not limited to, credit card numbers, social insurance numbers, personal medical records/test results, criminal records/investigations, biometrics, full financial records of individuals, etc.	**Very high,** severe financial loss, legal consequences, identity theft, loss of public safety, extreme or serious injury, destruction of partnerships and relationships and a real risk of significant harm to an individual.

Service Alberta, Enterprise Information Management (2026), Data and Information Security Classification: *https://manuals.alberta.ca/imt-policy-instruments-portal/standards/content-management/data-and-information-security-classification/*