



Information Security Classification Standard

<i>Classification</i>	<i>Definition</i>	<i>Minimum Safeguards Required</i>			
		<i>Access Restrictions</i>	<i>Transmission</i>	<i>Storage</i>	<i>Disposal</i>
Public	<p>Information deemed to be public by legislation or policy. Information in the public domain.</p> <p>Examples include annual reports, public announcements, the telephone directory, and specific categories of employee and student information.</p> <p>Confidentiality: not applicable* Availability: low to medium* Integrity: low to crucial*</p>	No restrictions on access.	No special handling required.	No special safeguards required.	Can be recycled.
Internal Use	<p>Information not approved for general circulation outside the University of Calgary or a University faculty or department.</p> <p>Loss would inconvenience the organization or management;</p>	Access limited to employees and other authorized users.	No special handling required.	Stored within a controlled access system (eg. password protected file or file system or locked file)	Shredded, erased.

Classification	Definition	Minimum Safeguards Required			
		Access Restrictions	Transmission	Storage	Disposal
	<p>disclosure is unlikely to result in financial loss or serious damage to credibility.</p> <p>Examples include internal memos, minutes of meetings, internal project reports.</p> <p>Confidentiality: medium* Availability: varies from low to high* Integrity: varies from low to high*</p>			cabinet).	
Confidential	<p>Information that is available only to authorized persons.</p> <p>Loss could seriously impede the organization's operations; disclosure could have a significant financial impact or cause damage to the organization's reputation.</p> <p>Examples include specific categories of employee and student information, unit budgets, accounting information, and information protected by legal privilege.</p> <p>Confidentiality: high* Availability: high* Integrity: high*</p>	Access limited to those with a demonstrated need to know.	<p>Encryption mandatory for public networks.</p> <p>Encryption optional on internal networks.</p>	Stored within a controlled access system (eg. password protected file or file system or locked file cabinet).	Shredded, degaussed (removal of magnetic information).

<i>Classification</i>	<i>Definition</i>	<i>Minimum Safeguards Required</i>			
		<i>Access Restrictions</i>	<i>Transmission</i>	<i>Storage</i>	<i>Disposal</i>
Highly Confidential	<p>Confidential information that is so sensitive that it is entitled to extraordinary protections.</p> <p>Loss would seriously impede the organization's operations; disclosure would have a significant impact on finances, reputation, and competitiveness and could have legal repercussions.</p> <p>Examples include specific categories of employee and student information such as legal suits, medical/health information, appeals, and grievances as well as clinical patient data.</p> <p>Confidentiality: crucial* Availability: crucial* Integrity: crucial*</p>	Access limited to those with a demonstrated need to know.	<p>Encryption mandatory for public networks.</p> <p>Encryption optional on internal networks.</p>	Stored within a controlled access system (eg. password protected file or file system or locked file cabinet). Additional controls implemented as necessary to comply with relevant legislation.	Shredded, degaussed (removal of magnetic information).

* Confidentiality, Availability, and Integrity are categorized as 'not applicable', 'low', 'medium', 'high', or 'crucial'.

Policy Reference: **Information Asset Identification and Classification Policy** (relevant sections)

4.1 Business Information Assets owned by and/or in the custody of the University will be identified and classified by the Data Custodian in accordance with the University Classification System (UCLASS) and the Information Security Classification Standard.

4.4 Scholarly Information Assets, stored in systems that are operated or managed by the University, will be identified and classified by the Data Custodian in accordance with the University Classification

System (UCLASS) and the Information Security Classification Standard.

4.6 Health Information Assets, stored in systems that are operated or managed by the University, will be identified and classified by the Data Custodian in accordance with the University Classification System (UCLASS) and the Information Security Classification Standard.

Please see published policy for definitions of terms.

History: Developed in the Fall 2007 by:
Jo-Ann Munn Gafuik, Information Management Program Compliance Officer, University Legal Services
Dennis Tracz, Information Security Officer, Information Technologies
Bonnie Woelk, Information Management Program Manager, University Archives

Approved By: Harold Esche, Chief Information Officer
Jo-Ann Munn Gafuik, Information Management Program Compliance Officer, University Legal Services

Effective Date: January 31, 2008