Information Risk Classification Framework

Version: 1.0
Published: Dec. 20, 2022
First Published: Dec. 20, 2022
Published By: Information Security Office, Information Services

1. Introduction

Risk considers two aspects: the degree of harm caused by an event occurring, and the likelihood of an event occurring. Consider the loss of sensitive information, harm, whether reputational or financial would result. Neither the university nor its community could afford this unnecessary consequence. Similarly, well protected information is less likely to be lost than poorly protected information. Therefore, this framework uses risk to categorize information into classifications for the purpose of safeguarding it against risk.

2. Definitions

LOW RISK	MODERATE RISK	HIGH RISK
Information and systems are classified as **Low Risk** if they are not considered to be **Moderate** or **High Risk**, and: 1. The information is intended for public disclosure, or 2. The loss of confidentiality, integrity, or availability of the information or system would have no adverse impact on our mission, research, safety, finances, or reputation.	**Moderate Risk** Information and systems are classified as Moderate Risk if they are not considered to be **High Risk**, and: 1. The information is not generally available to the public, or 2. The loss of confidentiality, integrity, or availability of the information or system could have a mildly adverse impact on our mission, research, safety, finances, or reputation.	Information and systems are classified as **High Risk** if: 1. Protection of the information is required by law/regulation, 2. University of Regina is required to self-report to provincial or federal government and/or provide notice to an individual if the information is inappropriately accessed, or 3. The loss of confidentiality, integrity, or availability of the information or system could have a significant adverse impact on our mission, research, safety, finances, or reputation.

2.1. Information Risk Classification with examples. This set of classifications have been established and are in effect for University of Regina information:

Use the examples below to determine which risk classification is appropriate for a particular type of information. When mixed information falls into multiple risk categories, use the highest risk classification across all.

LOW RISK	MODERATE RISK	HIGH RISK
• Published research information (at information owner's discretion) • U of Regina user IDs and email addresses • Information authorized to be available on or through the University's website without University authentication • Policy and procedure manuals designated by the owner as public • Job postings • University contact information not designated by the individual as "private" • Information in the public domain • Publicly available campus maps • Classroom Schedules • Information/data with no legal risk no legal restriction to access and use. • Information posted on the University’s public facing websites. • University-wide policies. • University offered programs/courses. • Faculty and staff information directory. • Published annual report/ minutes of meeting. • University of Regina’s publication/press release. • Telephone Directory • Released Patents or awards.	• Unpublished research information (at information owner's discretion) or Identifiable personal research data. • Student records and admission applications • Faculty/staff employment applications, personnel files, benefits, salary, Age, birth date, personal contact information • Non-public University Administration • Non-public contracts • University internal memos and email, non-public reports, budgets, plans, financial info • Internal project information • Engineering, design, and operational information regarding University infrastructure	• Health Information, including Health Information designated by provincial legislation • Sensitive personal information ○ Social Insurance Numbers(SIN) ○ Individual financial account information ○ Driver's license numbers ○ Passport and visa numbers ○ Biometric data • Financial account numbers • Credit card information including PCI-DSS • Export controlled information according to Federal law • Donor contact information and non-public gift information • Intellectual property proprietary to University of Regina. • Authentication credentials for systems and applications (i.e. Passwords, Private encryption keys, Tokens, Fobs, Passcodes or PINs) • Student, faculty or staff disciplinary records. • Information that is subject to special government requirements in the interests of national security.

• Published marketing materials. • Public announcements. • Any code contributed to Open Source. • Board meeting information, including agendas, materials and minutes.		• Contractual agreements. • Details of campus security threats or incidents. • Vulnerabilities in the University of Regina's processes or systems. • Solicitor-client privilege information/Legal advice.

3. Data Handling Standards

3.1 Provided the information classifications above, information custodians understand the risk associated with their information. Information Services provides the appropriate safeguards required to protect information of each risk classification. These data handling standards provide a list of essential, required, and recommended controls for each data classification (high, medium, low).

Related Information

- Data Handling Standards

Revision History

Version	Version Date	Status	Summary of Change	Author
1.0	Dec. 20, 2022	Final	First Published	R. Jesse