Office of the Chief Information Security Officer

Digital Asset Classification Standard

Effective March 28, 2024

UNIVERSITY OF TORONTO

Overview

Purpose

This standard defines classification of digital assets. It establishes an expectation for the University to follow. It builds upon the Data Classification Standard and includes availability considerations for digital asset classification. This standard accompanies and does not replace the Data Classification Standard.

Preamble

The University defines levels of classification for data, but data is stored, processed and transmitted by information systems of various sorts, collectively referred to as digital assets.

A digital asset is the collection of data, information systems, applications and equipment that contain and process the intellectual property of the University and of the members of its community, and the mechanisms for storage, information processing and distribution of these data. Digital assets can include, among other things, information protected by academic freedom, personal information, proprietary information and confidential information.

All digital assets must be protected in accordance with information risk management programs and U of T's Information Security Control Standard. Digital assets need to meet the standard for the highest level of data they handle.

Scope

This standard is authorized under the Policy on Information Security and the Protection of Digital Assets and inherits the scope. The policy applies to all academic and administrative units, third-party agents of the University, as well as any other University affiliate that is authorized to access institutional data, services and systems.

Standard

Digital asset classification

The classification levels (level 1, level 2, level 3 and level 4) defined within the Data Classification Standard not only apply to data but also to information systems, applications and equipment that handle data (including storage, processing and transmission) belonging to the University and the members of its community.

When applying classification levels to digital assets, you must consider the availability, integrity and confidentiality of the data it handles. As the Data Classification Standard already addresses integrity and confidentiality, this document outlines availability considerations as shown in the table below.

Availability level	Impact	Examples (not exhaustive)
A4	Loss of availability would result in major impact to the overall operation of a unit and/or essential services. Loss of availability would incur significant financial losses. Digital assets that are required to be highly available by statutory, regulatory, contractual and legal obligations.	• Industrial control systems affecting life and safety • Campus-wide active directory
A3	Loss of availability would result in moderate financial losses and/or moderate reduced operations.	• Time reporting system • Departmental website
A2	Loss of availability may cause minor losses or inefficiencies.	• Student club website • Personnel contact directory
A1	Loss of availability poses minimal impact or financial losses.	• Music streaming system • Personal webpage

Related standards

- Data Classification Standard
- Information Security Control Standard

Endorsed by the Information Security Council on March 28, 2024.