# INSTRUCTIONS: How to use these Guidelines

## Layout

- The following charts are laid out into three categories:
    1. Administrative Storage Options
    2. Research Storage Options
    3. Teaching Storage Options
- The second row in each table labeled “Administrative/Research/Teacher Data Needs” shows a use case in each column for that table’s type of data.
- The third row are the available or future services that meet the need of each use case for each type of data being stored.
- The first (far left) column, refers to the U of A’s institutional data categories, or rather, levels of sensitivity, as defined by the institution in Institution Data Management and Government Procedure.
- There are three symbols that indicate IST’s recommendation for what level of sensitive data can be stored in each storage service:

✓ **Approved**: Limited risk associated with storing this level of sensitive data in this storage service

! **Not Advised**: Refer to **Information Security policies** for guidance before proceeding with storing this level of sensitive data in this storage service

✖ **High Risk**: Requires **Chief Information Security Officer** approval via the **Privacy and Security Review Checklist** before proceeding with storing this level of sensitive data in this storage service

## How to read each table

1) Determine the **type of data** you are trying to store: research data, administrative data (financial, HR, marketing, communications, forms, etc.), and/or teaching and learning data

2) **Find the table** that **fits** your type of data, and **review the “needs”** row that describes the **unique storage need** for each type of data

3) If a storage service is **underlined**, it means that it *links* to an information page about that service; **click on the link to learn about the service**

4) Use the information provided to **determine where you can move the data** that you have

## In development

IST is in the process of **developing a “storage finder” application** that will enable a user to **filter available storage services** based on **their requirements**. The intent is to eventually replace the below guidelines with this storage finder application. Many universities currently utilize a tool like this to help users determine which storage services best fit their needs. (i.e. https://umanitoba.ca/libraries/finder)

# Data Management and Storage Guidelines

The University of Alberta's data classifications help members of the university community to identify, understand, manage and use university data appropriately. The data classes described below are meant to be used as recommendations in conjunction with any applicable compliance requirements, such as PARIS, Freedom of Information (FOIP), and Protection of Privacy Act or Copyright Act.

| **University Storage Options for Administrative Purposes** | | | | |
|---|---|---|---|---|
| **Administrative Data Needs** | Institutional administrative data | Administrative data that supports your team/unit | Individual use data | Person-to-person or team communication platforms |
| ****Available Solutions** | EDRMS, PeopleSoft, SupplyNet | Google Shared Drives, Department Network Drives | Google My Drive, Department Network Drives | U of A Gmail,<br>Google Chat, Jabber Softphone application, Zoom |
| **Restricted** | ✓ | ! | ! | ✖ |
| **Confidential** | ✓ | ✓ | ✓ | ! |
| **Protected** | ✓ | ✓ | ✓ | ✓ |
| **Unrestricted** | ✓ | ✓ | ✓ | ✓ |

**Personal Devices at Work Disclaimer:** It is **highly discouraged** to purchase and/or use removable storage devices, personal mobile devices or non-sanctioned cloud services for work purposes. These include, but are not limited to: USB flash drives, External Hard Drives, External SSD drives, CDs, DVDs, mobile phones, computers, Dropbox, Slack, M365 OneDrive, Apple iCloud, Box, etc.

! **Not Advised: Refer to Information Security policies**

✖ **High Risk: Requires Chief Information Security Officer approval via the Privacy and Security Review Checklist**

*Google MyDrive **should not be used** for any long term storage and retention practices.

| **University Storage Options for Research Purposes** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Research Data Needs** | Active individual research | Active collaborative research | Archival | Archival | Active Sensitive Health Data | External Advanced Research Computing | Secure research storage | Sensitive Research Data High Performance Computing (HPC) |
| ****Available Solutions** | ***Google MyDrive** | **Google Shared Drive** | **Library Storage Archive** | **U of A Library Borealis-Dataverse** | **Data Analytics Research Core (DARC)** | **Access to National Digital Research Infrastructure (DRI)** | **Research Data Storage Service (RDSS)**<br>**Live Now** | **Sensitive Data Research Environment**<br>**Coming 2025** |
| **Restricted** | ❗ | ❗ | ❗ | ❗ | ✓ | ✖ | ✓ | ✓ |
| **Confidential** | ✓ | ✓ | ✓ | ✓ | ✓ | ✖ | ✓ | ✓ |
| **Protected** | ✓ | ✓ | ✓ | ✓ | ✓ | ❗ | ✓ | ✓ |
| **Unrestricted** | ✓ | ✓ | ✓ | ✓ | ❗ | ✓ | ✓ | ✓ |

**Personal Devices at Work Disclaimer:** It is **highly discouraged** to purchase and/or use removable storage devices, personal mobile devices or non-sanctioned cloud services for work purposes. These include, but are not limited to: USB flash drives, External Hard Drives, External SSD drives, CDs, DVDs, mobile phones, computers, Dropbox, Slack, M365 OneDrive, Apple iCloud, Box, etc.

❗ **Not Advised: Refer to Information Security policies**

✖ **High Risk: Requires Chief Information Security Officer approval via the Privacy and Security Review Checklist**

*Google MyDrive **should not be used** for any long term storage and retention practices.
**Department/College based solutions exist outside of these solutions (i.e.HRDR, Cirrus)

| **University Storage Options for Teaching Purposes** | | | |
|---|---|---|---|
| **Instructor Data Needs** | Digital teaching materials used in course presentations, assignments | Collaborative work | Media files for Teaching |
| ****Available Solutions** | **Google My Drive**, **Department Network Drives** | **Google Shared Drives**, **Department Network Drives** | **YuJa & Canvas Studio** |
| **Restricted** | ❗ | ❗ | ❌ |
| **Confidential** | ✅ | ❗ | ❗ |
| **Protected** | ✅ | ✅ | ✅ |
| **Unrestricted** | ✅ | ✅ | ✅ |

**Personal Devices at Work Disclaimer:** It is **highly discouraged** to purchase and/or use removable storage devices, personal mobile devices or non-sanctioned cloud services for work purposes. These include, but are not limited to: USB flash drives, External Hard Drives, External SSD drives, CDs, DVDs, mobile phones, computers, Dropbox, Slack, M365 OneDrive, Apple iCloud, Box, etc.

❗ **Not Advised: Refer to Information Security policies**

❌ **High Risk: Requires Chief Information Security Officer approval via the Privacy and Security Review Checklist**

*Google MyDrive **should not be used** for any long term storage and retention practices.

**Institutional Data Categories**

### Restricted Data

This classification is for information that is extremely sensitive and could cause extreme damage to the integrity, image or effective service delivery of the University of Alberta. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship and major economic impact. Restricted information is available only to named individuals or specified positions. (Examples include restricted spaces, credit card numbers, social insurance numbers and personal medical records).

### Confidential Data

This is for information that is sensitive within the University of Alberta and could cause serious loss of privacy, competitive advantage, loss of confidence in university programs or damage to partnership, relationships and/or reputation. Confidential information includes highly sensitive personal information. Confidential information is available only to a specific function, group or role. (i.e.. personnel files, including personal salary data and third party business information submitted in confidence).

### Protected Data

This is for information that is sensitive outside the University of Alberta and could impact service levels or performance, or result in low to medium levels of financial loss to individuals or enterprises, loss of privacy, loss of confidence in university programs or damage to partnerships, relationships and/or reputation. Protected information includes personal information, financial information or details concerning the effective operation of the university of Alberta. Protected information is available to employees and authorized non-employees (contractors, sub-contractors and agents) possessing a need to know for a business-related purpose. (i.e.., grades, dates of birth and personal contact information other than university email addresses). These definitions and classifications reflect the Government of Alberta information security classification standard.

### Unrestricted Data

This is for information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information includes information deemed public by legislation or through routine disclosure or active dissemination. Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the university. Or, where the information has not been made available to the public, if it were, it would not have any harmful or negative effect. (i.e.. university email addresses, accounting chart of accounts).

Excerpt from: https://policiesonline.ualberta.ca/PoliciesProcedures/Procedures/Institutional-Data-Management-and-Governance-Procedure.pdf

Links & Resources

*Institutional Data Management and Governance Procedure*

https://policiesonline.ualberta.ca/PoliciesProcedures/Procedures/Institutional-Data-Management-and-Governance-Procedure.pdf

*Mobile Device Encryption Policy*
https://www.ualberta.ca/information-services-and-technology/security/encryption/index.html#:~:text=Any%20mobile%20or%20portable%20personal,information%20must%20also%20be%20encrypted.