DATA CLASSIFICATION *Cheat Sheet*

What is data classification?

Assigning a **sensitivity level** to **research data** to **identify and implement** the **appropriate controls** for **handling** and **protecting** data based on sensitivity.

Who does this apply to?

Anyone responsible for collecting, classifying, handling, sharing, or protecting research data at the University. This can include Principal Investigators, Research Facilitators, Graduate Students, Office of Research (ORS), and Technology Services (IT).

Research Data Classification Levels

	Confidential / Sensitive	Internal / Private	Public
Definition	Data **only available** to **limited authorized users**; unauthorized disclosure could result in **severe harm** to an individual or the University.	Data **available to authorized users** for research purposes; **unauthorized disclosure** could result in **minor harm** to an individual or the University.	Data **deemed public** by legislation or through a University policy; **disclosure** would **not result in any harm** to an individual or the University.
Examples	❖ Human participants' name, address, health & medical information, income ❖ Intellectual property ❖ Unpublished research data & library transactions	❖ Research team meeting minutes & correspondence ❖ Contracts between researchers & community partners ❖ Project funders' contact information	❖ Published research data ❖ Researchers' name and business contact information ❖ Aggregated human subject data (where re-identification is not possible)

Principal Investigator (PI) & Research Team (RT) Responsibilities

Data Identification	✓ **Understand research data** collected and used and **identify sensitivity of data** ✓ **Inventory sensitive data** and its flow through the information lifecycle ✓ **Identify technologies** involved and **verify** the ones **within scope** of the **IT Team's support** (**University-provided** or **IT-approved** technologies)
Data Classification	✓ PI: **Assign a classification level** to all research data and **identify** the **appropriate controls** for handling and protecting research data based on the **classification assigned** ✓ RT: **Understand the classification level assigned and apply the appropriate controls** for handling and protecting the data **based on the classification**
Data Collection	✓ **Obtain voluntary** and **informed consent** from research participants before or at the time of data collection. ✓ **Limit collection of data** only to **what is necessary** and to the **identified purposes**
Data Storage & Transmission	✓ **Manage** and **limit access to research data** on a **role-based** and **need-to-know** basis ✓ **Implement controls** to protect data **in-storage** and **in-transit** based on sensitivity ✓ Confidential data should not be shared through email; in cases of **exception**, **removable media** should be **encrypted,** and **password protected** before use
Data Usage	✓ **Obtain fresh consent** for **secondary use** of data ✓ **Limit use of data** only to **identified purposes** at the time consent was provided
Data Sharing	✓ **Obtain consent** from research participants before **disclosing 'Confidential'** data and ensure **data sharing agreement is in place** before **disclosure to 3rd parties**
Data Retention	✓ **Retain all research data** for a **minimum of 7 years** after the completion of research activities, as defined by the LUFA Collective Agreement, **or based on separate retention requirements** the data may be subject to
Data Disposal	✓ **Ensure all research data** is **securely disposed of** through destruction or archival **in accordance with** the **applicable disposal requirements – return University devices** to **Facilities** for secure disposal; **engage IT for guidance** if needed

ℹ For questions or support on data classification, connect with the Office of Research or IT Helpdesk

DATA CLASSIFICATION *Cheat Sheet*

What is data classification?

Assigning a **sensitivity level** to **research data** to **identify and implement** the **appropriate controls** for **handling** and **protecting** data based on sensitivity.

Who does this apply to?

Anyone responsible for collecting, classifying, handling, sharing, or protecting research data at the University. This can include Principal Investigators, Research Facilitators, Graduate Students, Office of Research (ORS), and Technology Services (IT).

Research Data Classification Levels

	Confidential / Sensitive	Internal / Private	Public
Definition	Data **only available** to **limited authorized users**; unauthorized disclosure could result in **severe harm** to an individual or the University.	Data **available to authorized users** for research purposes; **unauthorized disclosure** could result in **minor harm** to an individual or the University.	Data **deemed public** by legislation or through a University policy; **disclosure** would **not result in any harm** to an individual or the University.
Examples	❖ Human participants' name, address, health & medical information, income ❖ Intellectual property ❖ Unpublished research data & library transactions	❖ Research team meeting minutes & correspondence ❖ Contracts between researchers & community partners ❖ Project funders' contact information	❖ Published research data ❖ Researchers' name and business contact information ❖ Aggregated human subject data (where re-identification is not possible)

Office of Research Services & Research Facilitators Responsibilities

Develop & maintain the Research Data Guidelines & Standard; **periodically review** & **make updates** as changes are required

Monitor changes to **privacy legislation, regulations**, & **University requirements** that may impact the management of research data.

Communicate these changes to Researchers & **incorporate updates** to the Guidelines & Standard.

Data Identification	✓ **Work with Researchers** to **understand** the **research data** collected and used and **identify sensitive data** to be **inventoried** to capture its flow through the information lifecycle ✓ **Identify technologies** involved and **verify** the ones **within scope** of the **IT Team's support** (**University-provided** or **IT-approved** technologies)
Data Classification	✓ **Provide Researchers** with the **classification levels** and **guidelines on controls** for handling and protecting research data so they can assign a classification level to all research data and identification the appropriate controls to implement
Data Collection	✓ **Provide training** and **guidance** to Researchers on **obtaining voluntary** and **informed consent** from research participants before or at the time of data collection **and limiting collection of data** only to **what is necessary** and to the **identified purposes**
Data Storage & Transmission	✓ **Provide training** and **guidance** to Researchers on **limiting access to research data** on a **role-based** and **need-to-know** basis, **implementing controls** to protect data **in-storage** and **in-transit** based on sensitivity, and ensuring that storage of 'Confidential' data on **removable media** is **encrypted,** and **password protected** before use
Data Usage	✓ **Provide training** and **guidance** to Researchers on **obtaining fresh consent** for **secondary use** of data and **limiting use of data** only to **identified purposes** at the time consent was provided
Data Sharing	✓ **Maintain a data sharing agreement template** for Researchers' use when **disclosing Confidential' data to 3rd parties,** and **provide training** and **guidance** to Researchers on **obtaining consent** from research participants before **disclosing 'Confidential' data**
Data Retention	✓ **Provide training** and **guidance** to Researchers on **data retention requirements** as defined by the **LUFA Collective Agreement** (**retaining all research data** for a **minimum of 7 years** after the completion of research activities) or based on separate retention requirements the data may be subject to
Data Disposal	✓ **Provide training** and **guidance** to Researchers on **ensuring all research data** is **securely disposed of in accordance with** the **applicable disposal requirements** and that **University devices** are returned to **Facilities** for secure disposal

DATA CLASSIFICATION *Cheat Sheet*

What is data classification?

Assigning a **sensitivity level** to **research data** to **identify and implement** the **appropriate controls** for **handling** and **protecting** data based on sensitivity.

Who does this apply to?

Anyone responsible for collecting, classifying, handling, sharing, or protecting research data at the University. This can include Principal Investigators, Research Facilitators, Graduate Students, Office of Research (ORS), and Technology Services (IT).

Research Data Classification Levels

Definition

Confidential / Sensitive	Internal / Private	Public
Data **only available** to **limited authorized users**; unauthorized disclosure could result in **severe harm** to an individual or the University.	Data **available to authorized users** for research purposes; **unauthorized disclosure** could result in **minor harm** to an individual or the University.	Data **deemed public** by legislation or through a University policy; **disclosure** would **not result in any harm** to an individual or the University.

IT Team Responsibilities

Data Identification

Identifying the scope of IT's responsibility to implement technical controls for handling & protecting research data

In Scope

- ✓ **Research data** that is **within the Researcher's control** and **within** the **University's environment**. This can include:
  - ✓ Research data stored on University-provided or IT-approved systems, applications, and devices
  - ✓ Data hosted within on-premise and cloud systems

Not In Scope

- × Research data **stored** and **managed** in an **external third party's system** that researchers are provided access to for use in research
- × Research data stored on **systems, applications**, or **devices** that are **not University-provided** or **approved by IT**

Data Storage & Transmission

Protecting data at rest

Storage of 'Confidential' research data should be restricted to University-provided technologies (e.g., laptops, devices, databases, and authorized applications.

Ensure that University-provided **technologies have effective security controls** in accordance with **defined University standards** so Researchers can securely store research data.

Where removal media is required for storage of 'Confidential' data, **provide encrypted**, and **password protected** USBs to Researchers.

Protecting data in transit

'Confidential' research data should not be shared through email. In cases of exception, **enable email encryption capabilities** within the University's email system for Researchers' use.

Sharing of data should be done only via secure and authorized means that have been approved by IT (e.g., secure file transfer protocol).

Maintain a list of authorized sharing methods to help Researchers verify what is appropriate to use.**and Implement these capabilities** upon request

Audit Logs of Access to Data

Audit trails should be enabled for systems/applications that contain 'Confidential' research data to track user activities (e.g., access, edits, downloads).

Review audit logs to investigate user activities when there is a **suspected** or **reported privacy or security incident** and retain audit logs for at least a year with a minimum of two months immediately available for analysis.

Threat and Vulnerability Management

Systems, applications, and servers containing '**Confidential**' research data should undergo **threat and vulnerability management testing** on a **monthly basis.**

Vulnerability scans should be performed on a **monthly basis** and **rescans** should be performed after a **significant change** to the system/application/server, or to **test** and inspect that a **vulnerability identified** has been remediated

Data Disposal

Implementing the appropriate data disposal requirements using the following methods:

Electronic data

Destroy data, including backups, using a process that ensures the data cannot be recovered and used for unauthorized purposes.

University-provided physical devices

University-provided devices are to be **returned to the Facilities** team for secure disposal. **Provide guidance to Researchers** on returning physical devices upon request.