# Data Security for Data Management Plans

**Does this apply to me?**

Data security applies to every researcher. The impacts may vary depending on your project, but theft, intentional and unintentional modification, accidental disclosure, ransomware, deletion, and tampering can all derail a project. Additionally, researcher reputation and findings can be tarnished, sensitive data can be divulged, and the integrity of your past and future projects can be called into question.

If you are conducting research, you should be aware of and manage data security within your data management plan (DMP) and data environment.

**What is data security?**

Data security helps to reduce the likelihood and impact of data being lost or corrupted. There is no all-in-one solution for data security, as security processes should be established to mitigate risks related to the data classification and data availability for their corresponding data environment. Refer to the section 2 of the **Research Data Management Plan Guide and Tool Kit ("The Guide")** on MU's Data Management Planning website for details on data classification types and data availability.

To gain a better understanding of your data environment, the university suggests a researcher use the Data Security and Privacy Checklist within the Research Data Management Plan Guide and Tool Kit. The checklist requires the researcher to understand:

- Receiving and collecting data
- Data information types and formats
- Data storage, access, collection, and security
- Data sharing and data transport
- Data retention and destruction

**Areas of Data Security**

While Marquette has preferences, there are no university required standards for data security. Instead, a researcher should address data security in three different areas of the project per the questions below:

Area 1: Data Management Plan development (The Guide**,** section 2)

- Data classification: What type of data is being handled and does this increase my risk to the data environment?
- Data availability: How will the data be managed to meet the researcher's needs of timeliness and access?

Area 2: During Analysis (The Guide, Section 3.8)

- What is the sensitivity of the data and does sensitive data need to be anonymized?
- What is the data format and average size of a file?
- How long is data required to be retained prior to publication?
- What is the data destruction process, including naming convention, to easily identify when to purge files?
- What are the known costs for current data analysis storage?

- Who should have access to the data and how will this be managed / maintained?
- What is the backup plan for data (i.e., what is deemed an acceptable loss of data that does not compromise the research)?

Area 3: End of Project: (The Guide, Section 3.8)

- If data is sensitive, can it be anonymized to reduce the risk if data is lost?
- Does the data need to be shared and if so, how will it be shared? (i.e. MU Data repository)
- How long does the data need to be stored after the completion of research and does all the data from the research need to be stored or only what is needed to support the publication?
    - Note: if data is stored longer than 7 years, what is the value of the data after 7 years?
- What is the review process to remove/destroy data?
- What format will the data be stored in?
- What is the cost for project data storage?
- Who should have access to the data and how will this be managed / maintained?
- What is the backup plan for storage of data that supports the research findings?

**MU Data Security Preferences**

While the guidance below is preferred to reduce data risk, the university is aware that every research project may not be able to meet all these preferences for a variety of reasons. When necessary, IT Services should be contacted to discuss any questions about managing data risk within the researcher's data environment.

Data Environment:

- Leverage common university supported tools (refer to DMP Tools and Resource List)
- Data should be contained and reviewed in an environment that has a known security management process, such as the university network
- Data transferring should be completed in a secure manner, such as SharePoint/Teams
- Third party data storage sites should not be used unless data is Category 1: Publicly available data as the security environment is unknown.
- Data should be stored in a location that allows for a data back-up process, such as Teams or SharePoint

User access:

- Access should be granted to users based on their role and responsibility
- Access should be limited to only data that is required for them to perform their role or responsibility (i.e., least privileged access)
- Access should be reviewed at an appropriate interval (i.e. quarterly) by a person who can determine if their access is appropriate.
    - Note: In some cases, access may need to be removed immediately after a person leaves the project if a person has administrative rights or access to highly sensitive data.
- Access should be reviewed by a person who can determine if access is appropriate on a standard frequency or at a minimum when a user is gone.
- If data is stored on SharePoint, the site should be established as private, not public, to restrict unauthorized access to data

Data tracking/management

- Version control management should be used for data files; This is a standard function in Teams or SharePoint

Data Storage, retention, and destruction

- Data should be stored in an environment that properly mitigates the risk of the data type. If data is deemed sensitive, it should be stored in a known secure environment. The university prefers:
    - OneDrive if there is no data collaboration needs
    - SharePoint or Teams is data collaboration is required
- Data should be retained for the purpose of the data, which usually is 7 years. Data retained beyond that time frame should be assessed for the value of the data and how it will be used in the future. Please note there may be some incidents where data should be stored based on a different time threshold. Refer to the Data Retention guidelines within the IT Services Policies and/or leverage your guidance from the Office of Research Compliance or grant sponsor.
- Data should be destroyed in accordance to the destruction guidelines within the IT Services Policies
- All final data should be stored within the MU repository: ePublications or linked to ePublications if data is stored in another repository due to research or funding requirements.

Data transmission:

- Ensure sensitive data is either encrypted and/or transmitted through secure means (such as private sharing within Teams or SharePoint)
- Sensitive data should never be sent through email or stored on a third-party storage site without being encrypted.