Selkirk College | SELKIRK INNOVATES

Research Data Security: Risk Determination

Risk Level	Definition	Storage Requirements	IT Requirements
No Risk	The project has no identifiable risk associated with the research data. The data may be non-descriptive general data or the product of research not related to a company, human or animal. e.g. gathered through standard open access method. *Example: Initial literature review of a well-known subject with no IP consequences and no human involvement.*	Simple storage in a responsible manner is sufficient i.e. data are not negligently or carelessly mishandled. The data are handled and stored in a responsible manner, with no specific handling or storage techniques or protocols required.	• Non-encrypted desktop or laptop drive • Non-encrypted USB drive • Cloud Storage (OneDrive, Microsoft Teams)
Low Risk	Data that contains, or could contain, sensitive information. However, there are no identifiers in the data set to link the participants to the collected data. *Example: The data gathered from an anonymous survey where no identifiers were collected.*	• Physical documents must be kept in a locked office or storage room with a general lock on it. • Digital storage is on a computer that is password protected. • Proper data backup protocol is followed with emphasis on security. • For low risk data storage, a flash drive or cloud service is acceptable as long as the data are accounted for at all times.	• Non-encrypted desktop or laptop drive • Non-encrypted USB drive • Cloud Storage (OneDrive, SharePoint, Microsoft Teams)
Medium Risk	Data that bear some risk to the participants or company involved if there were a data security breach. The data may, for example, contain identifying information and technical data that can be linked to the participants. Or the data may reveal a company's technological approach. The data may include company-sensitive information that does not include identifiers. *Example: Interview transcripts collected by a researcher investigating community perspectives on public transportation where participant identifiers are included.*	Physical storage will require a locked cabinet within a locked institutional space. Digital data needs to be kept secure as well. The data should not be unnecessarily duplicated or stored on unsecure devices. Unsecure devices can include flash drives or portable hard drives and cloud storage devices that are not encrypted.	• Encrypted desktop or laptop drive • Encrypted USB drive • Cloud Storage (OneDrive, SharePoint, Microsoft Teams)
High Risk	Data that carry a significant risk of harm or loss to the participants or company involved if there were a data security breach. *Example: Video recordings of participants involved in a therapeutic intervention. Or, experimental data that are used for a patent.*	Physical storage requires a locked cabinet within a locked institutional space. Electronic storage and research data transfer over the Internet require encryption or use of denominalization software to prevent access or interception by unauthorized individuals, or other risks to data security. Identifiable data obtained through research that are kept on a computer or transferred through the Internet must be encrypted.	• Encrypted desktop or laptop drive • Encrypted USB drive • Encrypted Cloud Storage (SharePoint, OneDrive, Microsoft Teams)