**INSTRUCTIONS** (delete once editing is complete)

* This Template is intended to support researchers in meeting the expectations outlined under requirement U12 (“Confidentiality and security training”) in the [WEBPAGE Data Security Requirements Guidance](https://www.washington.edu/research/hsd/guidance/data-security/#5a) . Existing departmental policy(ies) that satisfy this requirement may be used in lieu of developing a study-specific policy. **You are not required to use this template.**
* This document should be edited for your specific study.
* [Text in brackets] indicates there is a choice to be made about what information to provide. Delete anything that is not relevant and remove brackets after editing is complete.
* Complete the Training Requirements section based on what training will be required for your study. Recommended training options and considerations are listed. Add or remove information as needed.

# Confidentiality and Security Training Policy

Effective Date: [Insert Date]

Study Title: [Insert Study Title]

Principal Investigator(s): [Insert Name(s)]

## 1. Purpose

The purpose of this policy is to outline the requirements for confidentiality and security training for all personnel involved in the handling of research data. This ensures that all individuals understand their responsibilities in maintaining the confidentiality and security of sensitive information.

## 2. Scope

This policy applies to all members of the research team, including principal investigators, co-investigators, research assistants, IT administrators, and any other personnel who have access to research data.

## 3. Training Requirements

All personnel must complete the following training requirements before being granted access to research data:

* [[HSD Data Security Protections Online Tutorial](https://www.washington.edu/research/hsd/training/hsd-tutorials-and-videos/#datasecurity)]
* [[UW IT Security 101 Online Training](https://it.uw.edu/guides/security-authentication/overview-of-security/security-101/)]
* [UW Medicine Compliance - Protecting Patient Information (HIPAA) Training: If applicable, this training provides an overview of the Health Insurance Portability and Accountability Act (HIPAA) regulations and how to handle protected health information (PHI) securely. The course may be accessed from [UW Medicine’s Learning Hub](https://lms.uwmedicine.org/) (UW NetID required) and searching for the title in Library or by registering for the module in the [Compliance Learning Portal](https://uwmedicinecompliance.uw.edu/clp_main/).]
* [Department-Specific Data Handling Training: Any additional training specific to the department or study, focusing on the proper handling and protection of research data.]
* [Review the following information and policy regarding reporting actual or suspected information security and privacy incidents:
	+ [UW IT Reporting an Incident or Breach](https://it.uw.edu/guides/privacy/take-action/report-an-incident-or-data-breach/)]

Regular refresher training: All personnel will complete any required refresher courses to ensure ongoing compliance with institutional confidentiality and security standards.

## 4. Documentation of Training

A centralized log will be maintained listing all individuals who have completed the required trainings, including:

* Name
* Role
* Date training completed
* Training type
* Approver name

Logs will be stored securely and reviewed quarterly.

## 5. Review Schedule

This policy will be reviewed annually to ensure that it remains up-to-date with current confidentiality and security standards. Any changes to the policy will be communicated to all personnel involved in the handling of research data.