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

* This Template is intended to support researchers in meeting the expectations outlined under requirement U10 (“Authorization and documentation of access”) 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 Roles and Responsibilities section based on your study. Add or remove rows as needed.

# SAMPLE: Research Data Access Control Policy

Effective Date: [Insert Date]

Study Title: [Insert Study Title]

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

## 1. Purpose

This policy outlines the procedures for authorizing, documenting, and managing access to research data (both digital and non-digital) to ensure compliance with institutional and regulatory data security requirements.

## 2. Scope

This policy applies to all individuals who access or manage research data for the above-named study, including study team members, IT administrators, auditors, and other affiliated personnel.

## 3. Roles and Responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Privileges** | **Criteria for Role Assignment** | **Access Approval Authority** |
| [Principal Investigator (PI)] | [Full access to all data and systems] | [Lead researcher on the study] | [Automatically assigned] |
| [e.g., Co-Investigator] | [Access to data and systems relevant to their research tasks] | [Co-investigator. Completion of data security and confidentiality training] | [PI] |
| [e.g., Research Assistant] | [Limited access to de-identified or coded data] | [Completion of data security and confidentiality training] | [PI or Co-PI] |
| [e.g., IT Administrator] | [System-level access for maintenance and security] | [Institutional IT staff with assigned duties] | [PI and Department IT Lead] |
| [e.g., External Collaborator] | [Access as defined in Data Use Agreement] | [Institutional affiliation and signed agreement] | [PI and Institutional Official] |

## 4. Access Authorization Procedures

Access requests must be submitted via the [Access Request Form or System].

The PI or designated approver will review and approve access based on role and necessity.

Access will be granted only after completion of required confidentiality and data security training.

## 5. Access Review and Revalidation

Access privileges will be reviewed every 6 months.

Individuals no longer involved in the study will have access revoked within 5 business days.

Temporary access (e.g., for auditors) will be time-limited and monitored.

## 6. Documentation of Access

A centralized log will be maintained listing all individuals with access, including:

* Name
* Role
* Date access granted
* Date access revoked (if applicable)
* Approver name

Logs will be stored securely and reviewed quarterly.

## 7. Non-Digital Data Access

Physical access to paper records or other non-digital data will be limited to authorized personnel.

Access logs for non-digital data will be maintained and reviewed semi-annually.

## 8. Policy Review

This policy will be reviewed annually or upon significant changes to the study team, data systems, or institutional requirements.