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

* This template is intended to support researchers in meeting requirement D9 (“Device management and monitoring”) in the [WEBPAGE Data Security Requirements Guidance](https://www.washington.edu/research/hsd/guidance/data-security/#5b). 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 table in section 4 based on devices in use for your study. Remove the example text and add as many rows to the table as needed.

# Device Management & Monitoring Policy

Effective Date: [Insert Date]

Study Title: [Insert Study Title]

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

## 1. Purpose

This policy outlines the procedures for managing and monitoring devices used in the above referenced research. It ensures compliance with UW data security requirements and protects study participants from potential harm due to data breaches or unauthorized access.

## 2. Scope

This policy applies to all devices used to collect, process, store, or transmit research data, including but not limited to:

- Desktop and laptop computers
- Smartphones and tablets
- USB drives and external hard drives
- Audio/video recording devices

## 3. General Requirements

For all devices used in support of this research, the study team will ensure that:

* **Secure Configuration:** Devices are configured for secure operation and access is limited to authorized users.
* **Timely Updates:** Operating systems and applications used on devices are regularly updated with security patches.
* **Inventory & Tracking:** Devices are inventoried and tracked to prevent loss or theft.
* **Acceptable Use:** Devices are used in accordance with the [UW Acceptable Use Policy](https://policy.uw.edu/directory/aps/section-40-personnel/aps-47-2-personal-use-of-university-facilities-computers-and-equipment-by-university-employees/) and any applicable data use agreements.

## 4. Device Inventory and Researcher Plans

The following table summarizes all devices used in the study and how the general requirements of this policy are met:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Type** | **Owner (UW/Personal)** | **Device Management/Custodian** | **User(s)** | **Purpose in Study** | **Security Configuration** | **Update Plan** | **Tracking Method** | **Notes** |
| [e.g., Laptop] | [UW] | [Dept IT] | [Dr. Smith] | [Data analysis] | [Encrypted, MFA enabled] | [Auto-updates enabled] | [UW asset tag + logbook] | [Used off-site] |
| [e.g., iPhone] | [Personal] | [RA Team] | [RA Team] | [Audio recording] | [Passcode, encrypted storage] | [Manual weekly check] | [Numbered + signed checkout] | [Data uploaded daily] |
| [e.g., USB Drive] | [UW] | [Dr. Lee] | [Dr. Lee] | [Temporary data transfer] | [AES-256 encryption] | [N/A] | [Stored in locked cabinet] | [Wiped after use] |

## 5. Compliance and Review

This policy will be reviewed annually or when significant changes to the study or devices occur.

Any suspected or actual data loss or device theft will be reported immediately to the IRB and relevant UW offices per the [HSD Data Security Requirements Guidance](https://www.washington.edu/research/hsd/guidance/data-security/#3).