[ORGANIZATION]

INFORMATION SECURITY PLAN

# PURPOSE

The purpose of this Information Security Plan (Plan) is to attest that safeguards are implemented to ensure the ongoing Confidentiality, Integrity, and Availability of [Organization]’s critical information assets in compliance with [Administrative Policy Statement 2.6](http://www.washington.edu/admin/rules/policies/APS/02.06.html).

NOTE: When filled out, this document or information therein is classified as Restricted and may be exempted from a public records request on the basis of security; pursuant to RCW 42.56.420.

# SCOPE

## Organization

|  |
| --- |
| [Include a brief description of the organization and its mission. Identify subordinate organizations and indicate if their assets are covered by this Plan or if they have their own security plans.] |

## Critical Assets

The term “critical asset” refers to any [Organization] hardware, software, or other information technology component that stores or processes **UW Confidential** or **Restricted** data. List critical assets that are in scope for the Plan below and mark the associated data classification. For more information see:[**Data Classifications**](https://privacy.uw.edu/design/data-classifications/).

|  |  |  |
| --- | --- | --- |
| **Asset Name** | **UW Confidential** | **Restricted** |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |
|  | [ ]  | [ ]  |

# CONTROLS

The following security controls demonstrate, at a high-level, how [Organization] protects its critical assets, as well as detects, responds, and recovers from incidents. Mark the controls that are performed by the organization or on behalf of the organization (e.g., by UW-IT or by a vendor). See the [**Information Security Guideline**](https://ciso.uw.edu/site/files/Information_Security_Guideline.pdf) for more details on individual controls.

|  |  |
| --- | --- |
| **General Operational Controls** | **Performed** |
| A change and configuration management process | [ ]  |
| A flaw remediation process | [ ]  |
| A malicious code and unauthorized software countermeasure process | [ ]  |
| A data protection and destruction process | [ ]  |
| Secure development practices | [ ]  |
| Backup and recovery processes for critical information and software | [ ]  |
| A business continuity and disaster recovery plan | [ ]  |
| Information security technical architecture standards | [ ]  |
| System build and maintenance standards | [ ]  |
| Acceptable use standards | [ ]  |

|  |  |
| --- | --- |
| **Technical Security and Access Controls** | **Performed** |
| Remote access process | [ ]  |
| Cryptographic controls for protecting data | [ ]  |
| An access authorization process for all users and information systems | [ ]  |
| An authentication mechanism for all authorized users and information systems | [ ]  |
| Network, system, and application-level protection measures. | [ ]  |

|  |  |
| --- | --- |
| **Monitoring Controls** | **Performed** |
| A baseline measurement process for application, system, and network activity | [ ]  |
| A monitoring capability for critical systems | [ ]  |
| An intrusion detection mechanism | [ ]  |
| Logging processes for networks, systems, and applications | [ ]  |

|  |  |
| --- | --- |
| **Physical Controls** | **Performed** |
| Physical protection and access processes for buildings that house critical information technology and systems | [ ]  |
| A physical protection process for critical information systems and institutional information | [ ]  |

|  |  |
| --- | --- |
| **Account and Identity Management Controls** | **Performed** |
| An identity and eligibility verification and registration process | [ ]  |
| A user and system account life cycle management process | [ ]  |

# Maintenance

The Executive Head of [Organization] is [Name], who approves this document and agrees that it will be used as the Plan for [Organization]. This Plan is considered to be a “living document” and is expected to change to meet the needs of the University and [Organization] This document will be reviewed annually and updated as needed.

Last reviewed: [date]

Last updated: [date]

An official copy will be stored [link].