Unit Information Security Management Program (ISMP) Instructions

**Delete this page when filled out for a particular Unit.**

To facilitate using the “search and replace” function, repeated words and phrases are indicated in {BRACES}.

Instructions {enclosed in braces} indicate where descriptive information should be supplied.

Additional information for certain words or sections are highlighted.

**When completed, all comments and highlights should be deleted.**

Please keep in mind that all information provided should be a brief overview of your security program summarizing and describing your current state, accomplishments, gaps, action items and accepted risks. Avoid going into too much detail as this is intended to be an executive overview of your current security activities. Additional detail can be referenced in OneTrust or other locations.

If you have any questions, please contact securityrisk@uci.edu



{UNIT NAME} Information Security Management Program (ISMP)

[DATE]

## GOVERNANCE AND SCOPE

The {Unit Name} is committed to high standards of excellence for protecting the Institutional Information and IT Resources that support {Unit Name} mission to {Unit’s mission or description statement}. {Unit Name} processes, stores, and transmits an immense quantity of information to conduct its core campus functions.

This Information Security Management Program (ISMP) is established to support the implementation of the UC wide IS-3 Information Security Policy and the UCI Information Security Standard (ISS). This ISMP provides a comprehensive view of {Unit Name} security posture. This document illustrates the unit’s current state of:

1. Security controls and practices implemented
2. Existing security gaps and action items
3. Assumed security risks.

IS-3, the related standards, and other UC Systemwide IT policies can be accessed at:

* <https://security.ucop.edu/policies/>

UCI Information Security Standard is available at:

* <https://www.security.uci.edu/program/policy/iss/>

EXECUTIVE SUMMARY **{Complete this section last after documenting gaps/risks below}**

{Unit Name} has conducted an analysis of their Unit’s security posture against UCI ISS. The unit’s current security practices and control implementations are documented within this ISMP under each control section. Below is a summary of the top 3 security threats facing the unit and their high-level strategy to protect against those threats. A full list of all common threats and descriptions around those threats can found in the Common Threat Section of this document.

Top IS-3 compliance gaps in the Unit: **{List the top 3 specific IS-3 compliance gaps for your Unit. Keep it high-level, about 1-2 sentences each.}**

* Gap 1
* Gap 2
* Gap 3

Security Action Items to be Implemented: **{List the top 3 initiatives your unit will be working on to mitigate the threats or gaps identified above. Keep it high-level, about 1-2 sentences each}**

* Action Item 1
* Action Item 2
* Action Item 3

Assumed Risks: **{List the top assumed risks in your Unit. The assumed risks can be items that can’t be implemented now due to lack of resources, budget, time, etc.}**

* Assumed Risk 1
* Assumed Risk 2
* Assumed Risk 3

The details of {Unit Name} high risk assets, security risk assessments, and identified risks can be found within IT Security’s Governance, Risk, and Compliance (GRC) Tool, [OneTrust](https://app.onetrust.com/auth/login).

## ISMP METHODOLOGY

The purpose of the ISMP is for the Unit to:

* Gain knowledge of what major threats are impacting the Campus
* Document their current security practices and their compliance with ISS
* Identify what resources are needed to help implement security within the Unit
* Communicate the unit’s security posture to campus leadership

## GUIDING PRINCIPLES

The {Unit Name}’s Information Security Management Program is based on the following guiding principles. These guiding principles help shape the unit’s security strategy to remediate cyber risks and maintain a healthy security posture.

1. **Policy guides decisions** - the Unit views the UCI Information Security Standard (ISS) as a baseline of security requirements needed to keep Institutional Information and IT Resources safe.
2. **Responsible for security** – the Unit is responsible for implementing information security. The Unit understands what their assets are and the threats those assets face. This makes the Unit the best decision maker and responsible party for implementing security.
3. **Risk-based approach** - the Unit understands not all security action items can be applied immediately, therefore a risk-based approach is used to implement security controls in a timely manner. All assumed risks have a date for re-evaluation.
4. **Security is a shared responsibility** – the Unit cannot implement security by itself. Security is a shared responsibility between the Unit, Campus Service Providers, Suppliers, and Workforce Members.
5. **Security is an ongoing effort** – as the Unit and it’s supporting technology evolves, security needs to evolve as well. Therefore, the Unit embeds security into the lifecycle of systems, services, and software.

## ROLES & RESPONSIBILITIES

Per IS-3 policy Unit leadership is accountable for information security within their Unit, supported by Unit Information Security Leads (UISLs) and Service Providers. {Unit Name} has the following role assignments in place:

|  |  |
| --- | --- |
| Role | Name |
| Unit Head | {Full Name}{Title} |
| Administrative UISL | {Full Name}{Title} |
| Technical UISL | {Full Name}{Title} |
| Service Providers |  |

Detailed role descriptions can be found at:

* <https://www.security.uci.edu/program/roles/>

Role descriptions directly align to UC’s system wide [IS-3 Electronic Information Security Policy](https://policy.ucop.edu/doc/7000543/BFB-IS-3).

## MANAGEMENT

Unit Resources Dedicated to Security

**{Please briefly describe what resources your unit currently has available and/or would need to have to implement security.}**

## SCOPE

This ISMP applies to:

* All Unit Institutional Information
* All Unit IT Resources included those supported by campus Service Providers
* All Unit Workforce Members
* All Unit Suppliers that have access to Unit Institutional Information or IT Resources
* **{Please list any additional items that may be specific to your Unit}**

## COMMON THREATS

New security threats are being introduced into the world every day. Below is a list of the top security threats identified by OIT Security that are currently impacting the campus:

Security Threats to Campus:

* Cyber Attack (system compromise, interruption of service, ransomware)
* Unauthorized Data Leak
* Human Error or Social Engineering
* Third Party / Supply Chain Attack
* Technical System Failure or Environmental Disaster

Every unit has a unique function to supporting the mission of the campus. Below is a list of unique security threats impacting {Unit Name}:

Security Threats to Unit: **{Briefly describe security threats specifically impacting your unit}**

* Threat 1 – Defined by Unit
* Threat 2 – Defined by Unit
* Threat 3 – Defined by Unit

## CONTROLS

{This section should *briefly summarize* the state of compliance, gaps, action items, and assumed risks from the Unit or application risk assessments completed in OneTrust. If no risk assessment or similar analysis has yet been completed, please document these sections as “unknown”.}

* Risk Management
	+ Objective

The goal of this section is to briefly describe what the Unit has done to comply with the Risk Management requirements of UC IS-3 and UCI ISS, what gaps in compliance exist, what gaps are actively being worked on during the next 12 months, and what risks will be formally accepted by the Unit.

Compliance topics for this section include:

* + - Risk Assessment Process – Describe how the risk assessment process is implemented in the Unit.
		- Risk Exception Process – Describe how gaps that will not be addressed are formally documented in the Unit.
		- Unit Security Governance – Describe how the Administrative and Technical UISLs work with the Unit Head to develop security strategies, priorities, and documentation in the Unit.
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Human Resource Security
	+ Objective

The goal of this section is to ensure that Workforce Members understand their key responsibilities and are trained for their current roles or any roles for which they are considered.

Compliance topics for this section include:

* + - Prior to Employment – Describe how any security duties are documented in posted jobs descriptions.
		- Background Checks – Describe how background checks are implemented in the Unit.
		- Security Training and Awareness - Describe how security awareness training and any additional security training is implemented in the Unit.
		- Change of Employment – Describe how Workforce Member security responsibilities are updated when job duties change.
		- Separation – Describe processes in place to revoke access when job duties change or a Workforce Member separates from the University.
		- Workforce Manager and Workforce Member Responsibilities – Describe how Workforce Members are informed of their security responsibilities in a Unit.
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Asset Management
	+ Objective

Identify UC assets (Institutional Information and IT Resources) and define appropriate protection responsibilities.

Compliance topics for this section include:

* + - Inventory of IT Resources and Institutional Information – Describe the process for how IT Resources and Institutional Information is inventoried.
		- Classification of Institutional Information – Describe Unit processes for ensuring that IT Resources and Institutional Information is appropriately classified with Protection Level and Availability Levels
		- Secure Disposal of IT Resources and Institutional Information – Describe processes for ensuring that IT Resources and Institutional Information is securely disposed of when no longer needed.
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Access Control
	+ Objective

Limit access to Institutional Information and IT Resources to authorized users.

Compliance topics for this section include:

* + - General Access Control Principles – Describe processes for ensuring that only authorized users have access to Unit IT Resources and Institutional Information
		- Functional Account Management – Describe how functional accounts are managed in the Unit.
		- Service Account Management – Describe how service accounts are managed in the Unit.
		- Privileged Account Management – Describe how privileged access accounts are managed in the Unit.
		- Guest, Supplier, and Affiliate Account Management – Describe how guest and other third-party accounts are managed in the Unit.
		- Authentication and Passphrase Management – Describe requirements for authentication in the Unit including the use of multi-factor authentication.
		- Web Session Length – Describe how web session length is enforced in the Unit.
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Encryption
	+ Objective

Ensure that the Unit has processes in place to adequately encrypt Institutional information while it is stored on systems and in databases, and while it is being transferred across the network.

Compliance topics for this section include:

* + - Encryption at Rest – Describe how information is encrypted when stored on systems
		- Encryption in Transit – Describe how information is encrypted when transmitted over the network
		- Database Encryption – Describe the database encryption technologies in use.
		- Encryption Key Management – Describe how encryption keys are secured and stored
		- Certificates and Web Server Certificate Management – Describe how certificates are stored and managed
		- Code Signing Certificate Management – Describe how code signing certificates are managed
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Physical and Environmental Security
	+ Objective

Ensure appropriate physical security to protect UC Institutional Information and IT Resources.

Compliance topics for this section include:

* + - Physical Security Requirements – Describe how Unit systems are secured against loss, theft or tampering
		- Environmental Requirements – Describe how critical Unit systems are protected from power failures and other environmental risks
		- Transportation and Transfers – Describe how Unit systems and information are kept secure when being physically transferred from one location to another
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Operations Management
	+ Objective

Ensure operational security to protect Institutional Information and IT Resources.

Compliance topics for this section include:

* + - General Operations Management Requirements – Describe how systems are architected to protect systems with different Protection Levels or between testing, development and production
		- IT Resource Hardening – Describe how systems are built and hardened to documented standards
		- Change Management – Describe how change management is implemented in the Unit
		- Patching – Describe the methodology for patching systems in the Unit
		- Backup and Recovery – Describe how Unit systems are backed up and how recovery is tested
		- Vulnerability Management – Describe how vulnerabilities are monitored and managed within the Unit
		- Logging – Describe the status of the Unit Logging Plan
		- Cloud Services – Describe how cloud services used by the Unit are secured to IS-3/ISS standards
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Communications Security
	+ Objective

Ensure the security of Institutional Information in transit on networks and between parties.

Compliance topics for this section include:

* + - Network Security – Describe the network architectures being used by the Unit to secure Unit systems and information. This may include network segmentation, use of firewalls, etc.
		- Secure Transfer – Describe how Unit information is secured when being externally transferred to other campuses or Suppliers
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* System Acquisition, Development and Maintenance
	+ Objective

Ensure security by design and throughout the lifecycle of IT Resources and Institutional Information.

Compliance topics for this section include:

* + - Minimum Security Standards for All IT Resources Connected to the UCI Network – Describe how minimum standards are being met for all Unit endpoint systems
		- Additional Minimum Security Standards for Servers, Appliances, and Applications Connected to the UCI Network - Describe how minimum standards are being met for all Unit servers
		- Secure Software Configuration – Describe the status of application security plans within the Unit
		- Software Development – Describe how secure software development practices are implemented and documented within the Unit
		- Security Planning – Describe how security requirements are incorporated into Unit IT project planning
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Supplier Relationships
	+ Objective

Ensure that Supplier relationships are covered by appropriate security requirements and controls.

Compliance topics for this section include:

* + - Contracts and Agreements – Describe Unit processes for ensuring that Supplier Security Reviews are completed and appropriate contract terms are in place to secure Unit systems and information
		- Compliance Requirements When Using Suppliers – Describe Unit processes for ensuring Suppliers use and access Unit systems and information securely
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Information Security Incident Management
	+ Objective

Ensure a consistent and effective approach to the management of Information Security Incidents, including communication of Information Security Events and compromise details.

Compliance topics for this section include:

* Documenting a Unit Incident Response Plan – Describe the status of the Unit Incident Response Plan
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Information Security Aspects of Business Continuity
	+ Objective

Maintain information security during adverse situations and ensure that information security is embedded in UC’s business continuity and/or disaster recovery processes.

Compliance topics for this section include:

* Documenting a Disaster Recovery and Business Continuity Plan – Describe the status of your Disaster Recovery and Business Continuity Plan within the Unit
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

* Compliance with External Requirements
	+ Objective

Ensure compliance with legal, statutory, regulatory or contractual obligations related to information security.

Compliance topics for this section include:

* + - Documenting any additional security requirements to meet any external obligations - Describe unit processes for ensuring that all relevant external compliance requirements are being met.
	+ Current state

**(Briefly describe the current implemented practices and procedures in the Unit regarding the topics identified above}**

* + Gaps

**{Briefly describe what gaps still remain in the Unit for the topics described above}**

* + Action items

**{Briefly describe the action items that the Unit will be working over the next 12 months that address the identified gaps}**

* + Assumed risks

**{Briefly describe the identified gaps that will not be addressed in the next 12 months and therefore will need to be documented as assumed risks}**

Reviewed By

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   |   |   |   |   |
|   |   | Unit Head, [UNIT NAME]  |   | Date  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   |   |   |   |   |
|   |   | Unit Information Security Lead - Technical  |   | Date  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   |   |   |   |   |
|   |   | Unit Information Security Lead - Administrative  |   | Date  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version  | Description  | By  | Date  |
|   |   |   |   |
|   |   |   |   |