Unit Information Security Lead (UISL) “Job Description”

Definition:

A term for the Workforce Member(s) appointed by the Unit Head and assigned responsibility for ensuring tactical execution of information security activities including, but not limited to: implementing security controls; reviewing and updating risk assessments; devising procedures for the proper handling, storing and disposing of electronic media within the Unit; and reviewing access rights. These activities are performed in consultation with the Unit Head.

NOTE: The number of UISLs in a Unit is established by the Unit Head. A single person could oversee the responsibilities for an entire Unit or different UISLs could be assigned to different functional areas. This will largely be determined by the size and structure of the Unit and the Unit Head’s reporting preferences. Smaller Units may also be able to share one UISL.

Responsibilities include:

The UISL doesn’t need to be a technical person (though they can be). The role is responsible for ensuring the following, not necessarily for performing the implementation; there may be a coordination aspect for some of the tasks. For IT Client Services-supported Units, the UISL is expected to work in partnership with the ITCS zone contact for areas requiring technical support.

- Acting as the primary contact for security for the Unit, in consultation with the Unit Head;
- Being the liaison between the Unit and UC Berkeley Information Security Office (ISO);
- Ensuring Institutional Information and IT Resources that the Unit uses and is responsible for are identified and inventoried, including classification;
- Ensuring implementation of security controls for the Unit, including devising procedures for the proper handling, storage, and disposal of electronic media within the Unit, under applicable policies, laws, regulations, and contractual agreements;
    - This includes working with Procurement to ensure that Supplier agreements include required data security contract language.
- Ensuring Unit risk assessments and risk treatment plans, such as MSSEI Self Assessment Plans, are reviewed and updated;
- Ensuring that access rights within the Unit are reviewed and maintained, including managing privileged access;
- Promptly reporting security-related incidents and violations to the Unit Head, ISO, and applicable governing entities;
- Ensuring prompt response to security incident reports and notices from the ISO, and ensuring that appropriate personnel take action in response to each one;
- Membership in and active monitoring of the UCB-Security mailing list;
- Active membership in the ISO Security Workgroup (ISWorkgroup).

Initial tasks for UISLs at UC Berkeley:

- ❏ Review your Unit information security metrics in the Unit Information Security Metrics Dashboard. ***User Guide***
- ❏ Review your Unit's assets, registrations, and Security Contacts in NetReg:
  NetReg User Guide for UISLs
  - ❏ Review your Unit's Security Contacts
  - ❏ Ensure their membership is complete and current
  - ❏ Review their inventory (registered subnets, offsite hostnames, etc.)
  - ❏ Review their Protected Data Application (and Services) registration(s)
  - ❏ Work with your Security Contacts to update information where needed

- ❏ Confirm with your Security Contacts that they have reviewed and confirmed the Protection Levels of their Protected Data Applications and Services in the last year

- ❏ Complete a high-level IS-3 Unit self assessment using the ISORA survey tool
  ISORA Self-Assessment User Guide
  - ❏ Start filling out the assessment
    - Comments are required. Lock each question as you complete it.
  - ❏ Schedule a check-in meeting with the ISO Assessments Team to discuss any questions or issues - email uisl-help@berkeley.edu
  - ❏ When you're done with all questions, acknowledge your assessment -- an "acknowledge" button will appear at the top of the form when all questions are locked
  - ❏ Review the final assessment reports (issued after completion) with your Director or Unit Head

- ❏ Questions or feedback on any of these items: uisl-help@berkeley.edu

Ongoing Tasks

- ❏ Annual review and update of high-level IS-3 Unit Assessment
- ❏ Annual review of NetReg assets and Security Contacts
- ❏ Ensure Unit compliance with MSSND, MSSEI, and UC Minimum Security Standards
- ❏ Ongoing liaison role with Unit Head and ISO
- ❏ Report potential security incidents and ensure security notices from ISO are addressed
- ❏ Maintain active membership in UCB-Security mailing list and ISWorkgroup

Time Estimate

As stated above, UISLs are responsible for ensuring that the activities under their area of responsibility occur, not necessarily for performing the implementation. For IT Client

Services-supported Units, the UISL is expected to work in partnership with the ITCS zone contact for areas requiring technical support. This means that some UISLs will primarily have a coordination role, while UISLs on the technical side will likely be directly involved in implementation. Where a UISL falls on this spectrum will impact the workload associated with the role.

Time Estimates:

- Initial Tasks: 8-16 hours (1-2 days)
    - May take longer for large, complex units; units that are also IT Service Providers; and units with significant compliance obligations (HIPAA, PCI, Federal regulatory requirements, units with significant P4 or A4 assets).
    - May take less time for small units without the factors listed above, and ITCS-supported units.

- Ongoing Tasks: 5-10% FTE*
    - Pilot units indicated that workload will likely be in spurts, not constant throughout the year.
    - Initial tasks will be repeated annually. This should be factored into the anticipated time commitment.
    - * Does not include security-related work already being done by the unit.

If time exceeds these expected ranges, please contact the Information Security Office for review.

UISL Resources:

1. uisl-help@berkeley.edu - email to ISO IS-3 Team for questions or help with UISL tasks
2. UISL Calgroup: uisl@calgroups.berkeley.edu
    - Use for information sharing and communicating with other UISLs on campus
3. Unit Information Security Lead Resources Webpages including:
    - User Guides for UISM Dashboard, NetReg, and ISORA Self Assessment
4. IS-3 Resources Webpage
5. NetReg Documentation Webpages
6. Roles and Responsibilities Policy (draft)