UISL Role Summary	A term for the Workforce Member(s) assigned responsibility for **tactical implementation of UC IS-3 and UCI ISS and the coordination and oversight of information security activities within a Unit**. Depending on the size and complexity of the Unit, this can be a single person such as a senior director of IT or operations, multiple people such as the lead IT or operational managers of several departments within a Unit, or assigned to someone outside of a Unit such as an IT director in a central IT organization along with an internal operational manager. **In consultation with the Unit Head, the UISL(s) works with the Workforce Members within a Unit, Service Providers, Suppliers, OIT Security, and the CISO to ensure compliance with IS-3** including but not limited to: implementing security controls; reviewing and updating Risk Assessments and Risk Treatment Plans; devising procedures for the proper handling, storing and disposing of electronic media within the Unit; and reviewing access rights.

Topic	Administrative UISL	Technical UISL	Unit Information Security Lead Responsibilities
Governance	Responsible	Consulted	Coordinating with the Unit Head, ensure that UISLs have the appropriate authority and resources available to implement IS-3 and any additional regulatory compliance requirements within the Unit.
	Responsible	Consulted	Act as the Unit's central contact regarding information security.
	Responsible	Consulted	Understand business workflow in the Unit and provide tactical oversight for the execution of information security responsibilities within the Unit.
	Responsible	Responsible	Coordinate with Principle Investigators in the Unit to ensure that research activities are compliant with IS-3 and any security requirements documented in IRB protocols, grants, or contracts.
	Responsible	Consulted	Regularly keep the Unit Head informed of the Unit security posture including the status of risk assessments, gaps, action items, and assumed
	Responsible	Consulted	Provide oversight and execution of information security responsibilities within the Unit and facilitate development and implementation of the Unit Information Security Management Plan.
Risk Management Process	Responsible	Consulted	Take a risk-based approach to coordinating and completing appropriate Unit Risk Assessments or Risk Treatment Plans.
	Responsible	Responsible	Document gaps and develop plans to remediate gaps or implement compensating controls.
	Responsible	Consulted	Document any remaining unmitigated gaps or request exceptions using the risk acceptance process.
Human Resource Security	Responsible	Informed	Coordinate Information Security Training and Awareness efforts within the Unit.
	Responsible	Responsible	Attend and participate in campus-wide security activities such as information security meetings, security announcements and alerts, and requests from the CISO.
	Responsible	Informed	Propagate information security policies and procedures to appropriate Unit leadership and staff.
	Responsible	Informed	Working with Unit HR, help ensure that appropriate employment procedures are being implemented.
Asset Management	Responsible	Consulted	Coordinate the inventory and classification of Unit IT Resources and Institutional Information.
	Responsible	Responsible	Ensure that Unit IT Resources and Institutional Information are deleted and disposed of securely.
Access Control	Responsible	Responsible	Ensure proper account management processes are implemented and documented in the Unit.
	Consulted	Responsible	Implement multifactor authentication in the Unit as required for compliance.
Encryption	Responsible	Responsible	Ensure Unit Institutional Information is appropriately protected by encryption at rest and in transit.
	Informed	Responsible	Ensure Unit encryption keys and certificates are properly managed and protected.
Physical and Environmental Security	Responsible	Consulted	Document requirements and procedures for protecting Unit assets and data from unauthorized access, loss, theft, or damage.
Operations Management	Informed	Responsible	Implement and document secure configuration standards for Unit systems and software.
	Informed	Responsible	Document change management processes for Unit systems.
	Informed	Responsible	Implement compliant system patching procedures for Unit systems and applications.
	Responsible	Consulted	Ensure that Unit systems are backed up and recovery processes tested.
	Informed	Responsible	Implement a Unit vulnerability management process.
	Informed	Responsible	Document a Unit logging plan meeting UC security requirements and ensure implementation in the Unit.
Communications Security	Consulted	Responsible	Ensure Unit networks are architected to sufficiently segment and protect Unit systems and data.
	Informed	Responsible	Ensure firewalls and other security controls are in place to protect Unit systems and data and that traffic is monitored to detect unauthorized access.
	Consulted	Responsible	Ensure that unneeded services on Unit systems are disabled.
	Informed	Responsible	Ensure only secure, encrypted protocols are used for Unit services.
System Acquisition, Development and Maintenance	Responsible	Responsible	Ensure minimum security standards are implemented for all Unit systems connecting to the UCI network.
	Informed	Responsible	Ensure that the UC Secure Software Development Standard is used when writing code or developing applications in the Unit.
	Responsible	Consulted	Work with the Unit Head to plan, budget, design, and implement information security compliance as part of the lifecycle of Unit information systems.
Supplier Relationships	Responsible	Responsible	Ensure Units select and use Suppliers who can adequately protect Unit Institutional Information.
	Responsible	Consulted	Coordinate as needed with UCI Procurement and OIT Security Risk & Compliance to ensure that appropriate Supplier risk assessments are conducted and Appendix DS is negotiated on all applicable Supplier contracts.
	Responsible	Consulted	Monitor Supplier security compliance throughout the term of the agreement.
Information Security Incident Management	Responsible	Responsible	Coordinate the development, documentation, and implementation of a Unit Information Security Incident Response Plan.
	Responsible	Responsible	Ensure that all applicable confirmed or suspected security incidents are reported to the campus CISO and Unit leadership.
Information Security Aspects of Business Continuity	Responsible	Consulted	Ensure that Unit business continuity requirements are documented and comply with UC policy.
	Responsible	Consulted	Ensure that appropriate Unit IT Resources and the continued security of those resources are part of the Unit and campus business continuity and disaster recovery plans.
Compliance with External Requirements	Responsible	Consulted	In addition to UC Policy, ensure that Unit security procedures meet any additional requirements related to information security, intellectual property, records, privacy, personal information and encryption required in laws, government regulations, agreements, contracts, and grants.
	Responsible	Responsible	Ensure that Unit security documentation is sufficient to meet IS-3 and external security requirements.