UCLA Policy 420: Information Security Incident Response

Issuing Officer:	Executive Vice Chancellor and Provost
Responsible Dept:	Information Technology Services
Effective Date:	TBD, **Draft for Public Review**
Supersedes:	UCLA Policy 420, dated 5/1/2012

I. PURPOSE & SCOPE

In carrying out its mission of teaching, research, patient care, and public service, UCLA's faculty, other academic personnel, staff, and other affiliates create, receive, transmit and collect many different types of Institutional Information. UCLA also maintains significant investments in IT Resources, which include information technology (IT) infrastructure, computing systems, network systems, and industrial control systems. Information Security Incidents that threaten the confidentiality, integrity, or availability of Institutional Information or of IT Resources must be managed quickly and effectively to minimize disruption and damage and comply with legal and administrative obligations.

This Policy:

- Defines the responsibilities of Organization Heads for complying with this Policy in their respective Organizations;
- Identifies specific roles of campus officials that have responsibility for institutional response to Information Security Incidents.

This Policy applies to:

- All UCLA Organizations, including the UCLA Health Sciences.
- All UCLA Workforce Members, including those in the UCLA Health Sciences.
- All use of Institutional Information, independent of the location (physical, cloud, or with a third party), ownership of any device or account that is used to store, access, process, transmit, or control Institutional Information.
- All devices, independent of their location or ownership, when connected to a UC network or cloud service used to store or process Institutional Information.

II. DEFINITIONS

For the purposes of this Policy:

Information Security Event (Event) means an identified occurrence in a process, system, service, or network state indicating a possible breach of information security policy, a possible breach of privacy policy, a failure of controls or a previously unknown situation that may be relevant to security. This also includes alerts and notifications.

Information Security Incident (Incident) means either (1) a compromise of the confidentiality (privacy), integrity or availability of Institutional Information in a material or reportable way, whether caused by unauthorized action or accident; or (2) a single event or a series of unwanted or unexpected Information Security Events that have a significant probability of compromising business operations or threatening information security.

IT Resources broadly describes IT infrastructure, software and/or hardware with computing and networking capability. These include, but are not limited to: portable computing devices and systems, mobile phones, printers, network devices, industrial control systems (SCADA, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic media, Logical Media, biometric and access tokens and other devices that connect to any UC network. This includes both UC-owned and personally owned devices while they store Institutional Information, are connected to UC systems, are connected to UC Networks or used for UC business.

Institutional Information broadly describes all data and information created, received and/or collected by UC.

Organization is a unit headed by an Organization Head.

Organization Head is one of the following:

- Dean
- Vice Provost
- Vice Chancellor
- University Librarian
- Associate Vice Provost, Institute of Informatics
- Assistant Provost, Academic Program Development
- Executive Director, ASUCLA
- Director, Intercollegiate Athletics

Unit Information Security Lead (USIL) is the Workforce Member(s) assigned responsibility for tactical execution of information security activities for an Organization, 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 Organization; and reviewing access rights. These activities are performed in consultation with the Organization Head.

Workforce Member is an employee, faculty, staff, volunteer, contractor, researcher, student worker, student supporting/performing research, medical center staff/personnel, clinician, student intern, student volunteer or person working for UCLA in any capacity or through any other augmentation to UCLA staffing levels.

III. POLICY STATEMENT

Effectively responding to Information Security Incidents is a crucial component of UCLA's overall cybersecurity program to safeguard its IT Resources and Institutional Information, minimize disruption and damage, protect individuals' privacy, and comply with legal and administrative obligations.

A. Reporting Requirements

1. Organizations

When an Information Security Incident is discovered or suspected in an Organization, it must be immediately reported by the Organization to the appropriate Chief Information Security Officer for the campus or Health Services. The procedure for reporting can be found at https://ociso.ucla.edu/report-cyber-security-concern.

2. Workforce Members

A Workforce Member must report an Information Security Incident when they become aware, or suspect, that one has occurred. The procedure for reporting can be found at https://ociso.ucla.edu/report-cyber-security-concern.

B. Roles and Responsibilities

1. Organization Heads

Organization Heads are ultimately responsible for compliance with this Policy in their respective Organizations, even if an Organization Head has designated those responsibilities.

2. Unit Information Security Leads

USILs are responsible for reporting any occurrence, or suspected occurrence, of an Information Security Incident in their Organization to the UCLA Chief Information Security Officer, per Section III.A.

3. Workforce Members

When Workforce Members become aware, or suspect, that an Information Security Incident has occurred, they are responsible for reporting it to their Organization, per Section III.A.

4. UCLA Chief Information Security Officers (CISO)

The Campus and Health Sciences CISOs are the primary sponsors of the UCLA security incident response program and are responsible for directing response activities when an Information Security Incident is reported or suspected, including convening other campus officials and functional units as appropriate.

5. UCLA Cyber-risk Responsible Executive (CRE)

The Administrative Vice Chancellor is designated as CRE for UCLA, including the UCLA Health Sciences, for systemwide cyber governance purposes. The CRE has broad oversight for Information Security Incident response, ensures the UC Cyber Incident Escalation Protocol is followed, and is liaison with UCLA leadership.

C. Consequences of Non-Compliance

Organizations may bear all or some of UCLA's direct costs that result from an Information Security Incident under the Organization's area of responsibility if the Information Security Incident resulted from a significant failure of the Organization to comply with this Policy.

A significant failure to comply with this Policy may affect an Organization's ability to seek cyber insurance reimbursement in the event of an Information Security Incident and could impact UCLA's overall ability similarly.

Merit increases for Organization Heads for their administrative role whose units are found to be non-compliant with systemwide and campus cyber security policies require approval from the Chancellor.

IV. REFERENCES

1. UC Business & Finance Bulletin IS-3, Electronic Information Security;
2. UC Information Security Incident Response Standard;
3. UC Business & Finance Bulletin BUS-80, Insurance Programs for Institutional Information Technology Resources;
4. Letter from President Drake to Chancellors on Cybersecurity (February 26, 2024).

Issuing Officer

Executive Vice Chancellor and Provost

Questions concerning this policy should be referred to the Responsible Department listed at the top of this document.