Insurance Programs for Institutional Information Technology Resources

Responsible Officer:	Chief Risk Officer
Responsible Office:	RK - Risk / EH&S
Issuance Date:	12/17/2018
Effective Date:	12/17/2018
Last Review Date:	11/29/2018
Scope:	This policy applies to all of the following: • All UC campuses and medical centers, the UC Office of the President, UC Agriculture and Natural Resources, and all other UC locations (Locations). • All Workforce Members, Suppliers, Service Providers and other authorized users of Institutional Information and IT Resources. Note: This policy does **not** generally apply to students who are not Workforce Members. • All use of Institutional Information, independent of the location (physical or cloud), 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. • Research projects performed at any Location and UC-sponsored work performed by any Location.

Contact:	Gary Leonard
Title:	Executive Director
Email:	gary.leonard@ucop.edu
Phone:	(510) 987-9824

TABLE OF CONTENTS

I. POLICY SUMMARY

The Office of Risk Services manages the funding and administration of insurance programs for the University of California. Various programs are available to assist in the event of a loss involving Information Technology Resources (IT Resources) and Institutional Information. These programs involve purchased insurance policies through the University's captive insurance company, Fiat Lux Risk and Insurance Company, with various retentions (deductibles). The terms and coverage change frequently due to external market conditions, therefore it is not feasible to provide a complete summary.

THIS IS NOT INTENDED TO BE A COMPREHENSIVE LIST OR A COMPLETE DESCRIPTION OF COVERAGE.

II. DEFINITIONS

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

IT Resources: A term that broadly describes IT infrastructure, software and/or hardware with computing and networking capability. These include, but are not limited to: personal and mobile computing systems and devices, 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 and physical 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.

Location: A discrete organization or entity governed by the Regents of the University of California. Locations include, but are not limited to: campuses, laboratories, medical centers and health systems, as well as satellite offices, affiliates or other offices in the United States controlled by the Regents of the University of California.

Unit: A point of accountability and responsibility that results from creating/collecting or managing/possessing Institutional Information or installing/managing IT Resources. A Unit is typically a defined organization or set of departments.

Unit Head: A generic term for dean, vice chancellor or person in a similarly senior role who has the authority to allocate budget and is responsible for Unit performance and administration. At a particular Location or in a specific situation, the following senior roles may also be Unit Heads: department chairs, assistant/associate vice chancellor (AVC), principal investigators, directors or senior managers.

Workforce Member: 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 UC in any capacity or through any other augmentation to UC staffing levels.

III. POLICY TEXT

Property Insurance Program – Provides coverage for direct physical loss or damage to IT Resources or Institutional Information (unless other excluded under the policy terms).

IT Resources

The cost to repair or replace hardware, subject to the applicable conditions, exclusions, limits and deductible.

Institutional Information and Software

The cost to repair, replace or restore Institutional Information, programs, and software, including the costs to research, re-create and develop recovery solutions.

Information Security and Privacy Liability Program – Provides 1st and 3rd party coverage for damages and claims arising out of a privacy or security incident.

Privacy Liability Coverage

Covers damages and claim expenses UC is legally liable to pay arising out of the failure to prevent unauthorized access, disclosure or collection of information, or for not properly notifying in the event of unauthorized disclosure of personally identifying information or other protected categories.

Security Liability Coverage

Covers damages and claim expenses UC is legally liable to pay arising out of a the failure of system security, including written policies and procedures, to prevent or mitigate a computer attack.

Breach Notice Response Services Coverage

Covers Crisis Management and Breach Response Costs incurred as a result of a Security Breach.

This may include expenses associated with any of the following:

- Breach notice legal and forensic expenses;
- Breach notice fulfillment services;
- Credit monitoring services;
- Identity restoration services; and/or
- Call center services.

Privacy Regulatory Claims

Covers damages and claims expenses UC is legally obligated to pay resulting from a regulatory claim arising out of a privacy breach or security breach.

PCI DSS Assessment Coverage

Covers amounts UC is legally obligated to pay as a result of a Payment Card Industry Digital Security Specification (PCI DSS) Assessment resulting from a Security Breach.

Cyber Extortion

Covers investigation of the event and reimbursement of any cyber-extortion expenses and cyber-extortion payments paid by UC directly resulting from a Cyber-Extortion Threat. ***To be covered, any payment of extortion/ransom fees requires prior approval from OGC, OPRS and Insurers.***

Multimedia Liability

Covers damages and claims expenses UC is legally obligated to pay arising out of allegations of libel, slander, copyright infringement, plagiarism, etc. in relation to publishing, transmitting or displaying media content.

Digital Asset Restoration

Covers restoration costs incurred because of the alteration, destruction, damage, or loss of digital assets.

Conditions of Coverage

Coverage is dependent upon the adherence to the requirements stated in BFB IS-3 Electronic Information Security, related standards, and any local procedures not in conflict with BFB IS-3.

In the event that an Information Security Incident resulted from a significant failure of the Unit to comply with IS-3 and the related Standards, the Location will be assessed a deductible under the Information Security and Privacy Liability Insurance program as follows:

$20,000 - For incidents involving Institutional Information classified at Protection Level 1

$40,000 - For incidents involving Institutional Information classified at Protection Level 2

$75,000 – For incidents involving Institutional Information classified at Protection

Level 3

$100,000 – For incidents involving Institutional Information classified at Protection Level 4

IV. COMPLIANCE/RESPONSIBILITIES

DUTIES IN THE EVENT OF AN INCIDENT, CLAIM OR SUIT

In the event of a privacy or Information Security Incident, Locations must follow their established incident response process.

The University has system wide contracts in place for forensic firms and response/notification services. ***For information regarding these resources, please contact infosec@ucop.edu.***

Location risk management and/or the UCOP Office of Risk Services must be notified as soon as possible of any Information Security Incident that may result in a claim for response services, possible regulatory action or claims/litigation by third parties.

RESPONSIBILITES

Chief Risk Officer, Office of the President or designee, (e.g., Program Manager)

1. Manage and administer the insurance programs.
2. Review programs on a continuing basis and determine the most effective and efficient manner in which to manage the program risks.
3. Assure any rules, regulations, laws, statues, or other obligatory requirement governing the insurance programs are followed.
4. Secure and manage the services of the claims administrator and review performance.
5. Assist Location in the application of the programs and its coverage to specific situations.
6. Act as the University's representative to the insurance industry.
7. Ensure resolution of all matters in accordance with directives under Settlement Authority Request or other Regents policy.
8. Work in conjunction with the UC Office of the General Counsel to identify and select outside defense counsel to be associated with any insurance program.

Chancellor or designee (e.g., Location risk management)

1. Ensure all Workforce Members and Unit Heads are informed of coverage available under the insurance programs.
2. Ensure all claims (including summons and complaints) are reported in a timely manner and all appropriate parties are notified.
3. Promote cooperation and coordination with and between Workforce Members, Units, Location risk management, the claims administrator and counsel. Maintain communication to advise of any developments that may impact the outcome of pending investigation, claim, or litigation.
4. Provide all required and requested information needed to effectively administer and manage the programs and enable final resolution of claims. Coordinate efforts to determine causes, prevent recurrence, and mitigate loss.

5. Establish local procedures for identification and reduction of risk exposures by updating the Location Information Security Management Plan (IMSP) and related Risk Assessments or Risk Treatment Plans.
6. Coordinate local funding of self-insurance program cost allocation. Develop and implement allocation programs specific to the location to promote risk reduction.
7. Issue or secure certificates of insurance evidencing coverage under the programs.
8. Obtain necessary information to comply with insurance carrier reporting requirements.

Unit Heads

1. Ensure all appropriate Workforce Members have access to the Location Incident Response Plan and are trained on how to report an Information Security Incident.
2. Provide Risk Management office with timely information and assistance as needed to meet legal and University requirements for claims management. Keep all parties advised of developments.
3. Maintain communications with Workforce Members, Risk Manager and the Location Incident Response Team Coordinator in regard to reporting claims and cooperate with all efforts to bring claims to final resolution.
4. Provide necessary information to Location Risk Management, Compliance Management and Privacy Management offices to comply with insurance carrier and/or regulatory reporting requirements.

Lead Location Authority

1. Promote Location compliance with IS-3, Electronic Information Security and supporting standards.
2. Ensure that the Location incident response process complies with the UC Incident Response Standard and is followed.

V. PROCEDURES

New incidents or claims should be reported to location Risk Management

VI. RELATED INFORMATION

- Fiat Lux Master Property Insurance Policy
- Fiat Lux Information Security and Privacy Liability Insurance Policy
- University of California Information Security Policies and Standards

VII. FREQUENTLY ASKED QUESTIONS

What constitutes a "significant failure to comply" with IS-3?

This is a "reasonable person" standard and the same standard set by the State of California and the Office of Civil Rights. The standard defines "significant failure" as "conscious, intentional failure or reckless indifference to the obligation to comply."

Example 1: If a Unit did not encrypt any of its 50 laptops, that would constitute a failure to comply. Conversely, if a Unit encrypted all of its laptops and two new ones were stolen prior to the setup process, that would not constitute a significant failure to comply.

Example 2: If a Unit had two years of history showing the Unit regularly applied software updates (patches), but five systems were missed in the last cycle, that would not constitute a failure to comply. Conversely, if there were no history of patching and recent patching was also incomplete (i.e., most systems were still unpatched), that would constitute a significant failure because there would be a clear pattern of non-compliance.

VIII. REVISION HISTORY

December 17, 2018:

The revisions are made to reflect an update in insurance programs and align with Business and Finance Buletin, IS-3 Electronic Information Security and supporting standards.

The Policy was also reformatted into the standard University of California policy template and has been remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

August 9, 2010: Initial issuance.