University of California
Business and Finance Bulletin

Executive Vice President –
Chief Financial Officer
August 9, 2010

BUS-80	**Insurance Programs for Information Technology Systems** ***http://www.ucop.edu/ucophome/policies/bfb/bus80.html***	Refer specific program questions to the Program Manager, Office of Risk Services.

Business and Finance Bulletins Home Page: http://www.ucop.edu/ucophome/policies/bfb/

This Bulletin provides an overview of the insurance programs managed by the Office of Risk Services that extend coverage for Information Technology Systems and related exposures.

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

For specific questions regarding coverage, contact resources are listed at
http://www.ucop.edu/riskmgt/staff.html

I. RESOURCES

A. The Regents of the University of California Master Property Policy (All-Risk)

B. Business and Finance Bulletin IS-3, Electronic Information Security

C. UC Systemwide HIPAA (Health Insurance Portability and Accountability Act) Breach Response policy

D. UC Systemwide HIPAA Security policy

E. UC Privacy and Data Security Incident Response Plan

II. INTRODUCTION

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 Hardware and Data. These programs involve purchased insurance policies 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.

III. COVERAGE AND COVERED PARTIES/PROPERTY

A. Resources and Property Insurance Program - Physical loss or damage to hardware or data

Hardware

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

Software

The cost to repair, replace or restore data, programs, and software is covered, including the costs to research, re-create and engineer.

Who may be covered

The Regents of the University of California (University), all corporations, partnerships, joint ventures, organizations, and other entities, as have existed or as now or may hereafter exist, or for which it is required to or has agreed to maintain insurance, including any affiliated, associated, allied, and subsidiary entities.

What may be covered

The property covered under this program may include property: owned by the University; in which the University has an insurable interest; in the care, custody or control of the University; for which the University has received instructions or agreed to insure under written contract prior to a loss; or for which the University is legally liable.

B. Cyber Security and Privacy Liability - Damages and claims expenses that the University is obligated to pay because of an actual or alleged privacy breach, confidentiality breach, security breach or online media activity.

Privacy and Confidentiality Breach Liability Coverage

All damages and claims expenses that the University becomes obliged to pay as a result of any claim made against the University (including a lawsuit or regulatory action) for an alleged:

- privacy breach; or
- confidentiality breach.

Security Breach Liability Coverage

All damages and claims expenses that the University becomes obliged to pay as a result of any claim made against the University (including a lawsuit or regulatory action) for an alleged security breach resulting in any covered loss.

Breach Notice Response Services Coverage

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.

Breach notice legal and forensic expenses may include:

- fees incurred for the services of a third party computer forensics professional to conduct an investigation to identify whether notification-triggering data containing personally identifiable information was accessed by an unauthorized person as a result of a covered privacy breach; and,
- attorney fees for outside counsel to determine whether any breach notice laws apply and the obligations of such applicable laws, and assist you[1] to comply with such laws, including but not limited to drafting notice letters to impacted individuals.

Online Media Liability Coverage

Any claim made against you[1] for an alleged online media activity resulting in a media hazard may be covered.

Conditions of Coverage

Coverage is dependent upon the existence and adherence to security protocols outlined in BFB IS-3 or any local procedures not in conflict with BFB IS-3 that have been implemented for critical systems. At a minimum, the following conditions must be in place for coverage to apply:

a. maintain anti-virus and malware prevention solutions, including for student/ dormitory settings on any computer that is part of your[1] computer system and update the protection at regular intervals but no less than at least once every 30 days;
b. maintain firewalls on any computer that is part of your[1] computer system and connected to the internet;
c. take reasonable security precautions when processing, storing, or transmitting credit card payment data or personally identifiable information;
d. maintain, update and enforce written policies for information security, privacy, business continuity/disaster recovery and third party vendors;

[1] (the) University('s)

e. employ qualified information technology and network security representatives at each campus who will implement and maintain campus information technology, physical and network security policy;

f. ensure scan testing is performed on at least a quarterly basis and performed against all internet facing servers of each campus. Such testing should be provided by NetDiligence or some other provider to be agreed by the University and insuring party;

g. perform testing for SQL Based Web Applications for the ability to deflect SQL injection exploit issues through secure coding review and/or application-level scanning with AppScan or WebInspect products;

h. ensure encryption is in place for 'data at rest' for at least student personally identifiable information (within production databases, file servers and backup tapes);

i. ensure laptops are encrypted: any employee laptop with sensitive non-public data has whole disc encryption in place;

j. mandate encryption and/or enforced prohibition of storage of sensitive PII (personally identifiable information) or PHI (protected health information) on mobile USB devices;

k. maintain and implement ongoing patch management process to ensure timely patching of existing network systems and servers, as well as hardening of any new servers that are deployed;

l. deploy an intrusion detection platform along with the implementation and maintenance of a process to receive real time alerts of suspected intrusions and ensure a process exists to manually review the applicability of the warnings and act upon any warnings in a timely manner;

m. ensure a change management process is place that periodically reviews access rights and credentials for anyone who is able to logon to campus servers and will terminate rights when needed;

n. ensure segregation and isolation of PII/PHI servers holding or transmitting personally identifiable information via additional firewalling from the rest of the campus production and student networks;

o. maintain user account provisioning with strong role-based assignments, password composition and change rules, effective termination procedures and periodic stale account reviews;

p. maintain an incident reporting and response program that enables prompt escalation and management response for events reported by students, faculty and staff;

q. ensure that a computer asset map is maintained that details network operations and assets owned, and underscores which servers house sensitive private data or personally identifiable information for students & alumni.

An independent third party assessor (e.g., NetDiligence) will review the circumstances surrounding the event and provide:

- Certification (at inception) of whether the security processes of the campus/department have been adequately implemented, and/or
- Confirmation (in the event of a loss) that the security processes were still in place and were adequately maintained at the time when the loss occurred.

In the event that the relevant campus/department/agent fails these assessments, insurance cover will either not incept or will be declined or materially reduced.

IV. CLAIMS: Duties in the Event of an Occurrence, Claim or Suit

In the event of a privacy breach that may trigger a claim, campuses must follow their established local breach or incident response process or the UC Privacy and Data Security Incident Response Plan.

Campus risk management and/or the UCOP Office of Risk Services must be notified as soon as possible. If the privacy breach triggers an obligation for the University to comply with breach notice laws, the UCOP Office of Risk Services, including NetDiligence, has resources available to assist with breach notice response services and incident response and loss control information.

Campus Risk Management and/or UCOP Risk Services will notify the University's insurance broker or the respective insurance company's Claims Representative as soon as possible. Documentation of the incident, including log files, is essential. Be sure to follow the procedures in the established local breach or incident response process or the UC Privacy and Data Security Incident Response Plan.

V. RESPONSIBILITIES

A. 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 campus and medical center locations in the application of the programs and its coverage to specific situations.
6. Maintain and administer any applicable trust fund or other funding mechanism.
7. Act as the University's representative to the insurance industry.
8. Ensure resolution of all matters in accordance with directives under Settlement Authority Request or other Regents policy.

9. Review and approve loss control and loss prevention initiatives for funding through the "Be Smart About Safety" program and other loss control and loss prevention programs.

10. 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.

B. Chancellor (or designee - Medical Center/Campus Risk Management)

1. Ensure all employees/departments/agents 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 employees, University departments, administrative management, the claims administrator and outside counsel. Maintain communication to advise of any developments that may impact the outcome of pending investigation, claim, or litigation.

4. Assist and work in conjunction with other University departments to develop and maintain effective loss prevention and loss control initiatives through the "Be Smart About Safety" program and other loss control and loss prevention programs.

5. 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.

6. Establish local procedures for identification and reduction of risk exposures.

7. Coordinate local funding of self-insurance program cost allocation. Develop and implement allocation programs specific to the location to promote risk reduction.

8. Issue or secure certificates of insurance evidencing coverage under the programs.

9. Obtain necessary information to comply with insurance carrier reporting requirements.

C. Local Department

1. Ensure all appropriate medical center/campus departments or other governing entities that need to be notified are promptly notified in accordance with University procedures, state law, or other obligatory requirements.

2. Provide Medical Center/Campus Risk Management offices 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 employees and other University departments in regard to reporting claims and cooperate with all efforts to bring claims to final resolution.

4. Assist and coordinate with other University departments in the development and implementation of measures to mitigate loss, make accommodations, and enable resolution of claim.

5. Provide necessary information to Medical Center/Campus Risk Management offices to comply with insurance carrier reporting requirements.

D. UC HIPAA Privacy and/or Security Official

1. Oversee all ongoing activities related to the development, implementation, maintenance of and adherence to UC policies and procedures covering the privacy of and access to patient health information in compliance with HIPAA;

2. Post, modify and update all systemwide HIPAA policies and the text of the systemwide Notice of Privacy Practices, in consultation with the Office of the General Counsel and Single Health Care Component (SHCC) and Single Health Plan Component (SHPC) HIPAA Officers. Modifications and updates will be implemented if they are required by changes in federal or state law or as needed to respond to UC policy changes;

3. Coordinate with SHCC Compliance Officers, the Office of the General Counsel, Risk Services, Internal Audit, HIPAA Officers and others as necessary to provide a response to individual complaints, identify and mitigate potential violations, respond to breaches, provide further information about matters covered by the Notice of Privacy Practices and apply and document appropriate sanctions for failures by the workforce to comply with HIPAA, State privacy laws and regulations, and UC HIPAA policies;

4. In coordination with the SHCC and SHPC HIPAA Officers, develop processes for using complaints, incidents, and breaches as evaluative and improvement tools;

5. Organize and manage a systemwide HIPAA privacy and security governance structure; and

6. Report to executive management at the local and system level, as appropriate, and to the Board of Regents, when appropriate or necessary.

E. Campus HIPAA Privacy and/or Security Official

1. Manage the development, implementation, and revisions of the covered component's policies and procedures necessary for carrying out the requirements of the federal HIPAA requirement and UC HIPAA policies;

2. Ensure that all required HIPAA training is accomplished and documented in written or electronic form, and retain the records for at least six years;

3. Provide information on required HIPAA training compliance to the systemwide privacy official upon request;

4. Serve as the covered component's liaison to UC's HIPAA Privacy and Security Official(s);

5. Serve as the covered component's contact person responsible for resolving HIPAA complaints, managing HIPAA investigations, responding to incidents and breaches, and providing information regarding the covered component's HIPAA program to senior executives, UCOP, and external regulatory agencies such as the Office of Civil Rights;

6. Serve as the covered component's individual(s) responsible for assuring that HIPAA-required mitigation, complaint, and sanction policies and procedures are implemented and documented;

7. Assure that HIPAA-required documentation (see Section F, below) is accomplished and records are maintained by the covered component, and provide requested reports to UCOP and campus management;

8. Responsible for periodic reporting to and prompt notification of significant HIPAA incidents or issues to campus management, and to the UC HIPAA Privacy and Security Official(s);

9. Responsible to ensure appropriate HIPAA breach response activities and associated external notifications occur, as required.

F. Lead Campus Authority for the Campus Implementation Plan for Security Breach Notification

1. Promote campus compliance with requirements in IS-3, Electronic Information Security, for incident response

2. Ensure that the campus incident response process is followed

3. Ensure that systemwide and, if applicable, campus notification procedures are followed

4. Coordinate with Campus Counsel and Risk Management