Coversheet & Checklist form—for submitting to Academic Senate Executive Committee
Proposal for addition/revision of University Regulation.
(Rev.2011-9)  http://www.regulations.utah.edu/info/IPCresources.html

1. Regulation(s) involved (type, number, subject): new Rule 4-004B Information Security and Privacy Training and Awareness; and new Rule 4-004C Information Security Incident Response Rule; (in conjunction with existing Information Security Policy 4-004).

2. Responsible Policy Officer (name & title): Eric Denna, Chief Information Officer

3. Contact person(s) for questions & comments (name, email, phone#): Chris Kidd, chris.kidd@utah.edu, 801-585-7483

4. Presenter to Senate Exec (if different from contact person. name, phone#): Kevin Taylor, kevin.taylor@utah.edu, 801-585-3314

5. Approvals & consultation status.
   a. Administrative Officers who have approved (VP/President, name & date): Eric Denna, Chief Information Officer 9/26/2012
   b. Committees/Councils/other Officers consulted: Office of General Counsel
       Security and Privacy Advisory Team
       Information Technology Council
       Institutional Policy Committee

6. Check YES or NA (not applicable) of documents submitted--- (In digital form. Preferred file format MS Word doc. Special exception allowed for PDF format if previously arranged.)
   YES  Explanatory memorandum (key points of proposal, rationale).
   YES  VP/Presidential approval signatures  (separate sheet, or affixed to memo cover).
   YES  Text of proposed Regulation addition/revision.
   NA  (If revision of existing Regulation) text changes are clearly marked, using permanent font markings (not MS Word ‘Track’ Changes non-permanent markings).

Date submitted to Senate Office:

The Executive Committee will consider whether the proposal is ready for presentation to the full Senate, and if so will schedule it for a subsequent Senate meeting either as i) a matter of academic significance-- set on the “Intent” & “Debate” Calendars over two monthly meetings with final “approval” voting at the second, or ii) not academically significant—set on the “Information” Calendar for a single monthly meeting, with opportunity for questions and recommendations. See Policy 1-001  
MEMORANDUM

To: Eric Denna, CIO
From: Kevin Taylor
Date: December 12, 2012
Subject: Executive Summary – Proposed new Rules 4-004B and 4-004C, attached to existing Information Security Policy 4-004

This is a proposal to adopt two new University Rules in conjunction with existing University Policy 4-004 Information Security Policy.

The first is Rule 4-004B Information Security and Privacy Training and Awareness. This proposed Rule has been developed to ensure those involved in managing Information Technology are apprised of the security policies and best-practices required to secure those devices from unauthorized access. The Rule requires those in IT positions to take on-line training once per year.

The second is Rule 4-004C Information Security Incident Response. This proposed Rule has been developed to ensure that security issues are reported centrally to ensure the University responds appropriately and consistent with legal requirements. Examples of a security issue would include unauthorized access, loss of a laptop with University data, etc.

If you approve of the proposal, with your signature of approval it should then be forwarded for the approval and signature of President Pershing, and subsequently submitted for processing through the Academic Senate.

It is recommended that the effective date of the amended version be immediately upon completion of processing through the Academic Senate.

Please contact me at 5-3314 if you have any questions. Thank you.

Approved ________________________________ Date __December 12, 2012__

Eric Denna, CIO
Rule 4-004B Information Security and Privacy Training and Awareness. Revision 0. Effective date [upon final approval]

I. PURPOSE AND SCOPE

A. The University of Utah’s information and information resources are best protected by those who access, use, and disclose them. This Rule implements Information Security Policy 4-004, which requires the University to provide information security training and awareness.

B. This Rule’s scope is the same as University Information Security Policy 4-004.

II. DEFINITIONS   The definitions provided in Policy 4-004 apply for purposes of this Rule.

III. RULE

A. University employees are encouraged to take the on-line training annually to ensure they are aware of campus information security regulations. It is the responsibility of each employee to understand these regulations.

B. Mandatory Annual Training for Information Technology Personnel

1. All employees whose job titles are classified as ‘Information Technology’ by Human Resources must complete annual information security and privacy training.

2. The Information Security and Privacy Office will track on-line training completion for compliance. It is the responsibility of the department to address issues of non-compliance, upon notification.

3. Violation of this Rule by an Information Technology employee may result in disciplinary action in accordance with pertinent University policies, including those referenced in Section IV of this Rule.

[Note: Parts IV-VII of this Rule (and all other University Regulations) are Regulations Resource Information--the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

IV. REFERENCES

C. NIST 800 Series, Federal Information Security Standards
D. Policy 4-001, University Institutional Data Management
E. Policy 4-002, Information Resources Policy
F. Policy 4-003, World Wide Web Resources Policy
G. Policy 5-111, Disciplinary Actions and Dismissal of Staff Employees
H. Policy 6-400, Code of Student Rights and Responsibilities
I. Policy 6-316, Code of Faculty Rights and Responsibilities
J. Pub. L. 111-5, Division A, Title XIII, Subtitle D: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

V. CONTACTS

A. Policy Officer: Chief Information Officer, 801-581-3100
B. Policy Owner: Chief Information Security and Privacy Officer, 801-587-9241
C. It_policy@utah.edu

VI. HISTORY

A. Revision History:
   1. Date approved by
   2. Effective date:
Rule 4-004C Information Security Incident Response Rule.
Revision 0. Effective date [upon final approval]

I. PURPOSE AND SCOPE

A. The purpose of this Rule is to implement Policy 4-004 Information Security by helping mitigate the effects caused by information security incidents, protect information resources from unauthorized access, use, disclosure, or damage, and ensure compliance with federal and state laws with respect to information security incidents.

B. This Rule’s scope is the same as University Information Security Policy 4-004.

C. Note: Information Technology departments are expected to have processes in place to prevent, detect, contain, and eradicate threats and ultimately return services to normal - should there be an information security incident. This Rule is not meant to supersede those processes, but to complement and manage the business (or administrative) aspects of responding upon the occurrence of an information security incident.

II. DEFINITIONS

The definitions provided in Policy 4-004 apply for purposes of this Rule. In addition, the following definitions apply.

A. Electronic Information Security Incident — An Electronic Information Security Incident is defined as any real or suspected significant adverse event in relation to the security of computer systems, computer networks, electronic sensitive information or electronic restricted information. Examples of such incidents include:

1. Attempts to gain unauthorized access to a computer system or its data.
2. Theft or other loss of a laptop, desktop, smartphone, or other device that contains “sensitive” or “restricted” Information (as defined in Policy 4-004), whether or not such device is owned by the University of Utah.
3. Unwanted significant disruption or denial of service.
4. The unauthorized use of a computer system for the processing or storage of data.
5. Changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction, or consent.

B. Information Security Incident – An Electronic Information Security Incident or a Non-electronic Information Security Incident.
C. Non-electronic Information Security Incident – Real or suspected theft, loss or other unauthorized access to sensitive or restricted information stored in non-electronic form, such as printed documents and files.

III. RULE

A. A member of the University Community who becomes aware of an Information Security Incident must immediately report it to the appropriate information technology contact person (as appropriate, either their local IT Manager, the Campus Help Desk [801-581-4000] email ___, or the Hospital Help Desk [801-587-6000] email ___).

B. When an information security incident occurs, the information technology contact person to whom the incident is initially reported shall then notify the Information Security and Privacy Office (“ISPO”, as described in Policy 4-004), as soon as possible but no later than one calendar day. The ISPO will then investigate the incident. If necessary to complete the investigation, the ISPO may convene a preliminary fact-finding working group comprised of relevant business and technical personnel. The ISPO shall be given access to all relevant records required to conduct the investigation.

C. If a violation of law or University Regulations is identified through an ISPO investigation, the ISPO will generate a report outlining the conclusions of the investigation and provide it to the appropriate oversight authority.

D. Information Security Incident Response Team

1. Based on the information provided to ISPO and, as directed by and in consultation with the CIO and the Office of General Counsel, the ISPO may convene an Information Security Incident Response Team (ISIRT) to respond to a significant issue. The Chief Information Officer shall chair the ISIRT until a formal hand-off has been made to the Chief Information Security Officer, or other designee. Depending on the circumstances of each situation, the ISIRT may include representatives of some or all of the following offices:

   a) Chief Information Officer
   b) Information Security and Privacy Office
   c) Office of Public Affairs / Marketing and Communications
   d) Office of General Counsel
   e) Internal Audit
   f) University Information Technology (UIT) and/or University of Utah Hospital and Clinics Information Technology Services (UUHC-ITS).
   g) Information Security Operations
h) Departments, colleges or schools directly affected by the Information Security Incident (including both the appropriate business and technical personnel).

i) Other stakeholders, as appropriate.

2. The ISIRT will develop and execute communication and other action plans to ensure appropriate action is taken in a timely manner, including reporting, notification and other communication of the Information Security Incident, as required by law or otherwise deemed appropriate.

3. In carrying out this responsibility, the ISIRT will ensure that important operational decisions are elevated to the appropriate levels to protect the fundamental interests of the University and others impacted by the incident.

E. Violation of this Rule may result in disciplinary action in accordance with pertinent University Regulations, including those referenced in Section IV of this Rule.

F. See University of Utah Information Security Policy 4-004 for the process to request exceptions to this Rule.

[Note: Parts IV-VII of this Rule (and all other University Regulations) are Regulations Resource Information—the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

IV. REFERENCES

A. Rule 4-004A, Protected Health Information Data Breach Notification Rule
D. NIST 800 Series, Federal Information Security Standards
E. Policy 4-001, University Institutional Data Management
F. Policy 4-002, Information Resources Policy
G. Policy 4-003, World Wide Web Resources Policy
H. Policy 4-004, Information Security Policy
I. Policy 5-111, Disciplinary Actions and Dismissal of Staff Employees
J. Policy 6-400, Code of Student Rights and Responsibilities
K. Policy 6-316, Code of Faculty Rights and Responsibilities
L. Pub. L. 111-5, Division A, Title XIII, Subtitle D: Health Information Technology for Economic and Clinical Health Act (HITECH Act)
M. Privacy and Data Security Incident Response Plan

V. CONTACTS:
A. Policy Officer: Chief Information Officer, 801-581-3100
B. Policy Owner: Chief Information Security and Privacy Officer, 801-587-9241
C. it_policy@utah.edu

VI. HISTORY

A. Revision History:
   1. Current version: Revision 1
   2. Date approved by:
   3. Effective date:

B. Earlier revisions:
C. Effective dates: