UMass Chan MEDICAL SCHOOL

Information Security Incident Response Team Policy

POLICY **07.01.04**

Effective Date: 12/31/2014
Last Revised Date: 04/19/2024
Last Reviewed Date: 04/19/2024

The following are responsible for the accuracy of the information contained in this document.

Responsible Policy Administrator
Information Security Officer

Responsible Department
Information Technology

Contact UMassChanInformationSecurity@umassmed.edu

Policy Statement

The purpose of the Information Security Incident Response Team Policy is to establish procedures in accordance with applicable legal and regulatory requirements and University policy to address instances of unauthorized access to University networks, systems or data, to be known as an incident.

Reason for Policy

In addition to all the defenses implemented to protect infrastructure and the information processed within, conventional wisdom recommends a high level of preparedness for a security incident. This protocol describes the response to such events, the conditions whereby this process is invoked, the resources required, and the course of recommended action. Central to this process is the Incident Response Team (IRT), assembled with the purpose of addressing that particular circumstance where there is credible evidence of an incident. See "Process Flow – Appendix A" for a graphical representation of the information flow and decision process.

The primary emphasis of activities described within this protocol is the return to a normalized (secure) state as quickly as possible, while minimizing the adverse impact to the University. The capture and preservation of incident relevant data (e.g., network flows, data on drives, access logs, etc.) is performed primarily for the purpose of problem determination and resolution, and methods currently employed are suitable for that purpose. It is understood and accepted that strict forensic measures are not used in data capture and retention.

Entities Affected By This Policy

This policy applies to all users of computing, data, and information technology resources including faculty, staff, students, guests, external organizations, and individuals accessing network services, such as the Internet, via UMass Chan resources.

Scope

Information Security Incident Response Team

The Information Security Incident Response Team (IRT) is comprised of individuals with decision-making authority from within the University and charged by the Administration with the responsibility of assisting in the process described within this document.

University Information

University Information is any information maintained by or on behalf of the University that is used in the conduct of University business regardless of the manner in which such information is maintained or transmitted. University Information formats include, but are not limited to oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or any other medium.

University Client (Client)

A University Client (Client) is:

- any faculty, student, staff, or alumni affiliated with the University, or
- any department or school of the University, or
- any employee (permanent, temporary and contract personnel)

3rd Party

A 3rd party is:

- any entity having a relationship with the University not described as a Client (e.g., business partner, research subject, vendor), or
    - any external entity initiating contact with the University (e.g., RIAA, target of DDoS attack, student applicant, member of the general public).

Responsibilities

Information Security Incident Response Team (IRT)

A. Incident Response Team - Executive & Information Technology

The IRT Executive team and the IRT Information Technology Team consist of a Primary Team and Secondary Team, if deemed necessary. Each member of the Primary Team will designate an Alternate member to participate if the Primary Member is unavailable. See "Primary and Alternate Contact List - Appendix B" for a listing of individual members. The Primary Team will consist of representatives from the following areas:

A1. Primary Team (Required)

Executive Team	Information Technology Team
IRT LEAD: Information Technology's Information Security Office Department Head / Senior Management / Dean or Provost of Impacted Area (for example, IRB, IACUC, HR, Finance, etc) Chief Information Officer Chief of Police – UMass Chan ForHealth Consulting Leadership Environmental Health & Safety Facilities Office of Communications Office of Management University of Massachusetts General Counsel	***IRT LEAD:*** Information Technology's Information Security Office Information Technology's Customer Service Office Information Technology's Engineering Office Information Technology's Hosted Systems Office

A2. Secondary Team (as needed)

The circumstances surrounding each incident may differ and require personnel with expertise or skills beyond that of the Primary Team. Members of the Primary Team will determine what, if any, additional resources are required and a Secondary Team may be established with:

- Individuals with decision-making authority identified to have a vested interest in the resolution of the incident.

- Individuals identified as subject matter experts or having skills required for resolution of the incident.

Information Security Coordinators representing an affected Client or 3rd Party or known to have an established relationship with an affected Client or 3rd Party may be requested to serve on the Secondary Team.

B. Team Objectives

Led by the University's Information Security Office, the IRT's objective is to:

1. Coordinate and oversee the response to Incidents in accordance with the requirements of state and federal laws and University policy.
2. Minimize the potential negative impact to the University, Client and 3rd Party as a result of such Incidents.
3. Where appropriate, inform the affected Client and 3rd Party of action that is recommended or required on their behalf.
4. Restore services to a normalized and secure state of operation.
5. Provide clear and timely communication to all interested parties.

C. Team Members

1. New team members will be trained to fully understand roles and responsibilities within 90 days of assuming their role.

2. Team members will complete incident response training on an annual basis.

3. Incident response training will be necessary when changes to an information system dictate additional awareness.

4. The incident response team will test and/or exercise incident response capabilities regularly.

D. Responsibilities

To ensure an appropriate and timely execution of this protocol, the IRT Lead (or designated IRT Member) is required to:

1. Confirm the occurrence of an Incident requiring the execution of this protocol. Confirmation activities include but are not limited to:
   - direct conversation with Client, 3rd Party, HelpDesk, NOC personnel, "on call" engineer, IRT members or others having information about the event.
   - review of system logs or audit records.
   - examination or analysis of anomalies or untoward events.
   - collection of any evidence supportive of the event.
2. Supervise and direct the consistent, timely, and appropriate response to an Incident.
3. Provide appropriate communication to parties having a vested interest in the incident.
4. Notify critical vendors as needed (i.e. Microsoft, Iron Mountain, Salesforce, Amazon Web Services).

5. Notify local law enforcement and regional FBI office (Boston, MA), if necessary.
6. Offer support to the Client or 3rd Party as appropriate until the Incident is resolved.
7. Conduct a post-Incident review.
8. Maintain the procedures contained in this document.

E. Accountability

Individual IRT members are accountable to the Team and University Administration for the timely and effective execution of this protocol and associated activities.

F. Reporting a Security Incident

UMass Chan IT Help Desk staff should be notified immediately of any suspected or confirmed Security Incident involving a UMass Chan Information Technology Asset. If after normal operating hours, UMass Chan Campus Police should be notified. If it is unclear as to whether a situation should be considered a Security Incident, UMass Chan Information Security staff may be contacted to evaluate the situation.

G. Activation of Team

Once the IRT Lead has determined an Incident has occurred, the IRT Lead will activate this protocol within 24 hours after Incident determination. Notification of the Primary Team member or Alternate should occur, depending on the type of incident, communication will be via email or via direct communication by telephone or face-to-face contact. In the event that email, or direct communication is unavailable, Zoom will be leveraged to facilitate IRT communication. Respective Primary and Alternate Team members should exchange information frequently to ensure their knowledge of the incident is current.

Consult the "Notification Tree – Appendix C" for details and notification assignments.

Procedures

Key Components of Response Protocol

The Incident Response Protocol consists of five key components: Assessment, Notification / Communication, Containment, Corrective Measures and Closure, including post incident review.

Assessment

The IRT Lead will determine the category and severity of the Incident and undertake discussions and activities to best determine the next best course of action, i.e., decide if protocol execution is required. The "Assessment Checklist - Appendix E" is used in the initial assessment process conducted by the IRT Lead. Once the IRT is assembled, the Assessment Checklist is executed and reviewed to ensure all pertinent facts are established. All discussions, decisions and activities are to be documented.

Notification/Communication

Designated persons will take action to notify the appropriate internal and external parties, as necessary.

Internal Notification (within the University)

All Internal notification and communication must be approved by the Primary IRT.

1. Primary Team members notify Alternate Team members (and vice-versa). The IRT will notify members of Secondary Team (if assembled).

2. IRT Lead will notify University Administration, IT Directors and the Information Security Coordinators of the Incident and provide ongoing status.

3. IRT Lead will issue or direct all "sensitive" internal communications.

4. IT-Technology Support Services will issue all public internal communication.

External Notification (outside the University)

All External Notification and communication must be approved by the Office of General Counsel.

1. 3rd Party – IRT Lead (or designated representative) and the Office of General Counsel will establish communication with any 3rd Party, as appropriate for the circumstance.

2. Law Enforcement – University Police notifies local, state, and/or federal law enforcement agencies as appropriate.

3. Regulators – University Office of General Counsel and UMass Chan Office of Management notifies the appropriate regulatory agencies.

4. IRT members will assist in determining if other parties should be notified (e.g., Dell's Stolen Computer Division).

5. News outlets – IT-Technology Support Services and Office of Communications will determine if, how and when news outlets should be notified, and respond to all inquiries from news outlets.

6. Office of Research and the Institutional Review Board (IRB) determine if government notification (e.g., DOD, FDA) is required and take appropriate action.

7. Other affected parties – The IRT will determine if there are other parties of interest, with communications issued accordingly.

Client Notification

1. Client should be informed that the Incident has been reported, recorded and an investigation underway.

2. Client shall be kept abreast of the status of the Incident investigation in a timely manner.

3. Client shall be notified of results, closure of investigation, and recommendations.

Status

1. IRT Lead and IT-Technical Support Services assumes responsibility for preparing and issuing timely communication to IRT members, Administration, and other interested parties.

2. Communications may include meetings, video conferencing, teleconferencing, e-mail, telephone/messaging, voice recordings or other means as deemed appropriate.

3. Frequency and timeliness of communications will be established and revised throughout the life of the incident.

Containment

When an incident occurs, UMass Chan IT will work to isolate and protect the compromised device(s). Discontinue use of the device immediately, but do not power off the device. These steps are to ensure the successful collection of potential evidence.

Corrective Measures

The IRT will determine and cause to be executed the appropriate activities and processes required to quickly restore circumstances to a normalized (secure) state. Recommended activities addressing Unauthorized Access and Unauthorized Acquisition are described in "Corrective Measures - Appendix G".

Corrective measures are designed with the primary objectives of:

- Secure the processing environment.

- Restore the processing environment to its normalized state.

Closure

The IRT will stay actively engaged throughout the life of the Incident to assess the progress/status of all containment and corrective measures and determine at what point the incident can be considered resolved. Recommendations for improvements to processes, policies, procedures, etc. will exist beyond the activities required for incident resolution and should not delay closing the Incident.

Post-Incident Review

A review of incident-related activities is a required element of this protocol. All members of the IRT primary and secondary teams are recommended participants.

Discussion

The IRT Lead will host a Post-Incident Review after each Incident has been resolved; this discussion should be scheduled within 2-3 weeks of the Incident's remediation. The review is an examination of the Incident and all related activities and events. All activities performed relevant to the Incident should be reviewed with an eye towards improving the over-all incident response process.

Recommendations

The IRT's recommendations on changes to policy, process, safeguards, etc. are both an input to and by-product of this review. "Fix the problem, not the blame" is the focus of this activity. All discussion, recommendations and assignments are to be documented for distribution to the IRT and Administration, and follow-up by IRT Lead.

Follow-up

The IRT Lead will follow up with the Client and 3rd Party or other parties, as required and appropriate.

Definitions

Information Security Incident: an incident meeting one or more of the following conditions

- Any potential violation of Federal law, Massachusetts law or UMass Chan Policy involving a UMass Chan Information Technology Asset or sensitive or protected information in any form.
- A breach, attempted breach, or other Unauthorized Access of a UMass Chan Information Technology Asset. **Unauthorized access** is any action or attempt to utilize, alter, or degrade a UMass Chan owned or operated Information Technology Resource in a manner inconsistent with UMass Chan policies.

  The incident may originate from the UMass Chan network or an outside entity and includes from the following:

- External/Removable Media: An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
- Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services
- Web: An attack executed from a website or web-based application.
- Email: An attack executed via an email message or attachment.
- Improper Usage: Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
- Any Internet worms, viruses, or phishing attacks.
- Any conduct using in whole or in part a UMass Chan Information Technology Asset which could be construed as harassing, or in violation of UMass Chan Policies.

- The loss or theft of a UMass Chan computing device (including desktop, laptop computers and mobile devices) or the loss of any personal computing device containing UMass Chan information.

Characteristics of security incidents where *unauthorized access* might have occurred may include but are not limited to:

- Evidence (e-mail, system log) of disclosure of sensitive data
- Anomalous traffic to or from the suspected target
- System alerts
- Unexpected changes in resource usage
- Increased response time
- System slowdown or failure
- Changes in default or user-defined settings
- Unexplained or unexpected use of system resources
- Unusual activities appearing in system or audit logs
- Changes to or appearance of new system files
- New folders, files, programs or executables
- UserID lock out
- Appliance or equipment failure
- Unexpected enabling or activation of services or ports
- Protective mechanisms disabled (firewall, anti-virus)

Unauthorized Acquisition: The unauthorized physical access to, disclosure or acquisition of assets containing or providing access to University information (e.g., removable drives or media, hardcopy, wiring closets, file or document storage, appliance hardware, etc.)

Characteristics of security incidents where *unauthorized acquisition* might have occurred may include but are not limited to:

- Theft of computer equipment where sensitive data is stored
- Loss of storage media (removable drive, CD-Rom, DVD, flash drive, magnetic tape)
- Printed materials containing University sensitive data mishandled or left unsecured
- Illegal entry (burglary)
- Office equipment in disarray or out of place
- Suspicious or foreign hardware is connected to the network
- Normally secured storage areas found unsecured
- Broken or non-functioning locking mechanisms
- Presence of unauthorized personnel in secured areas
- Disabled security cameras or devices

Severity: Incidents are further delineated by the actual and potential impact on the business of the University. For additional information on severity assignments and associated symptoms, see "Incident Severity, Appendix D". The primary focus of this protocol is the handling of Severity 1 Incidents

Approvals

DocuSigned by:
Brian Coleman
232D95E3184B416...

Responsible Policy Administrator — Date: 5/28/2024

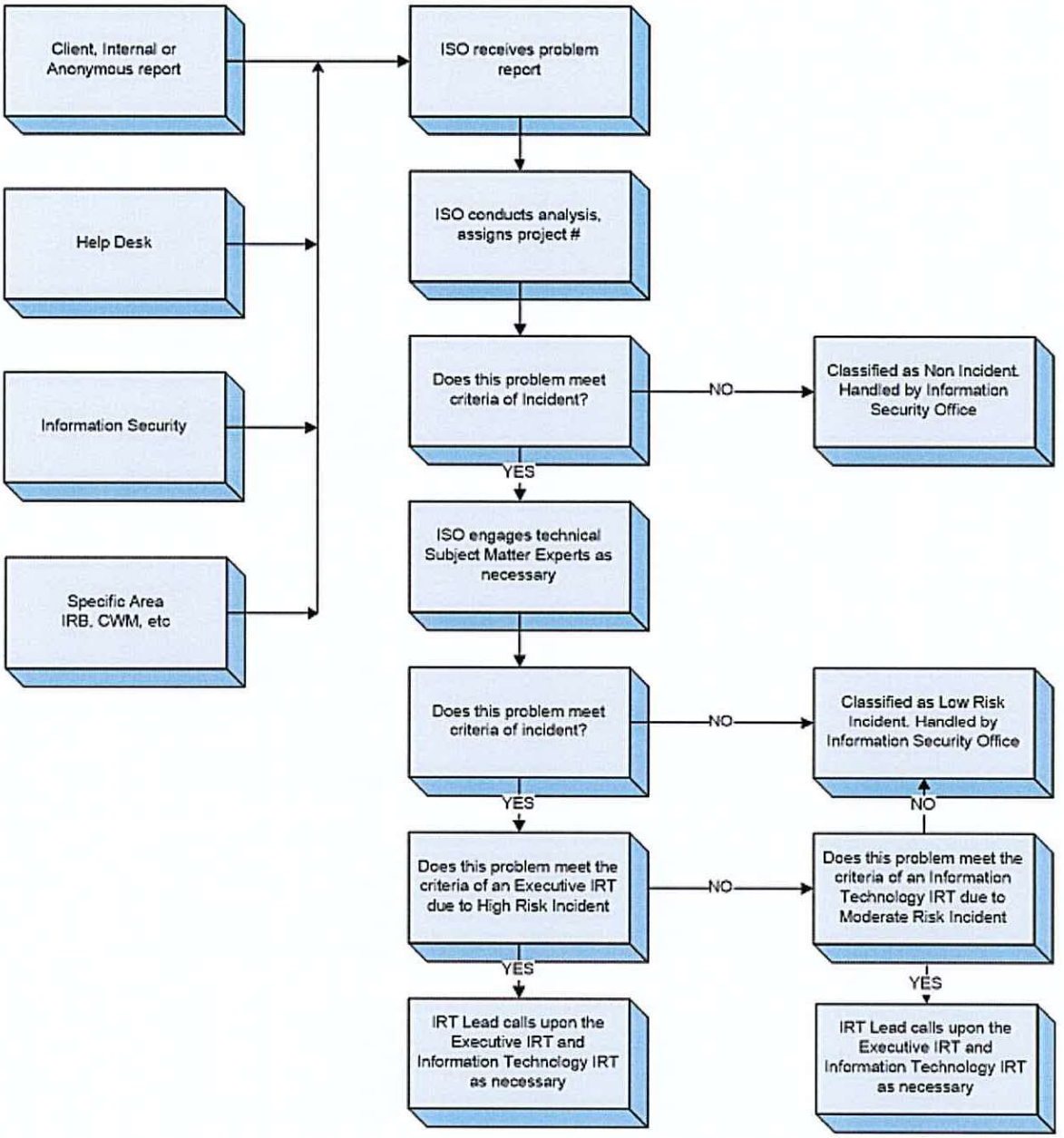
Executive Vice Chancellor for Administration & Finance — Date: 5/23/2024

Appendices

In support of this policy, the following appendices are included:

Name	Reference
Process Flow	A
Primary and Alternate Contact List	B
Incident Severity	C
Incident Assessment Checklist	D
Corrective Measures	E
Guidelines for IT Customer Service	F

Process Flow - Appendix A



Primary and Alternative Contact List - Appendix B

Incident Response Team - Executive

Department or Function	Primary Contact	Alternate Contact
Information Technology's Information Security Office - IRT Lead	Brian Coleman	Carleen Miller
Chancellor's Office	Brendan Chisholm	Jennifer Berryman
Department Head / Senior Managers of impacted Area (if necessary - for example, IRB, HR, Finance, MBL, Core Labs UMMHC, etc.)	TBD by IRT Lead	TBD by IRT Lead
Administration and Finance	John Lindstedt	Marcy Culverwell
ForHealth Consulting	Michael Schwab	Patti Onorato
Chief Information Officer	Greg Wolf	Brian Coleman
Chief of Police	Chief C. Leon Pierce	Nancy O'Loughlin
Office of Management	Jim Healy	Andrew Newton
Environmental Health & Safety	Kenneth Lebetkin	Scott Loh
Facilities	David Flanagan	David Adrian
Office of Communications	Jennifer Berryman	Lisa Larson
Privacy Office	June Brooks	Pam Harney

Incident Response Team - Information Technology

Department or Function	Primary Contact	Alternate Contact
Information Technology's Information Security Office - IRT Lead	Brian Coleman	Carleen Miller
IT Help Desk	Jack Cleary	Patricia Lanzillotti
IT Research Technology	Paul Langlois	Anaheed Zaki
IT Academic Technology	Patricia Lanzillotti	Abhilasha Yalamanchili
IT Operations & Network	Bradley Schultz	Curt Walker
Other IT areas as needed	TBD by IRT Lead	TBD by IRT Lead

Incident Severity - Appendix C

Severity	Symptoms
High	High probability of propagation. Probable or actual release or compromise of sensitive data (financial records, personal data, passwords, etc.) Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities. Notification of entities outside of the University is required. Examples: - Stolen laptop/portable device with PHI, non-encrypted - Compromised networks/systems - Disgruntled employees w/ high levels of access or amounts of confidential data - Defaced website
Moderate	Adverse effects are localized or contained, or minimal risk of propagation. No apparent release or compromise of sensitive data. Remedial but not immediate action is required. Notification of entities within the University is required. Examples: - Disruptive malware "Bot" - Stolen Laptop that's encrypted and does not contain PHI - Published Vulnerability (Heartbleed)
Low	Completely localized, with few individuals affected, and presenting little or no risk to other entities. No loss or compromise of sensitive data. Remedial action is required. Individual notification is required. Examples: - Phishing Emails - Limited Exposure Compromised Accounts

Incident Assessment Checklist - Appendix D

The activities described in this checklist are designed to assist in the initial assessment process performed and/or conducted by the IRT Lead.

Completion of this checklist is essential for any incident that calls for the execution of the Information Security Incident Response Protocol. Once the IRT is assembled, the Assessment Checklist is reviewed for completion to ensure all pertinent facts are established.

A. Description of Incident - Data relevant to the Incident should be collected for use in the process of Incident determination.
A1. Record the current date and time.
A2. Provide a brief description of the Incident.
A3. Who discovered the Incident? Provide name and contact information.
A4. Indicate when the incident occurred and when it was discovered.
A5. How was the Incident discovered?
A6. Describe the evidence that substantiates or corroborates the Incident (e.g., eye-witness, time-stamped logs, screenshots, video footage, hardcopy, etc.).
A7. Identify all known parties with knowledge of the Incident as of current date and time.
A8. Have all parties with knowledge of the Incident been informed to treat information about the Incident as "sensitive or confidential"?
B. Types of Information, Systems and Media - Provide information on the nature of the data that is relevant to the Incident.
B1. Provide details on the nature of the data (e.g., student information, research data, credit card information, SSNs, etc.).

B2. Does the information (if compromised) constitute a violation of regulatory requirements (e.g., FERPA, HIPAA, PIP Act) or University policy? Describe what is known.
B3. Was the compromised information maintained by a University Client or a 3rd Party? Provide details.
B4. How was the information held? Identify the types of information systems and/or the media on which the information was stored (e.g., hardcopy, laptop, CD, etc.).
B5. If the information was held electronically, was the data encrypted or otherwise disguised or protected (e.g., redacted, partial strings, password required, etc.)? If so, describe measures taken.
B6. If a Client held the information: - Establish the Client point of contact. - Assign responsibility to IRT member to contact the Client.
B7. If a 3rd Party held the information: - Identify the individual within the University who best represents the 3rd Party. If there is no suitable University contact, an IRT member will be assigned responsibility for directly contacting the 3rd Party. - Assign responsibility to IRT member to contact that individual. - IRT member will work with the University contact or 3rd Party to obtain a copy of any contract or confidentiality agreement and ascertain what knowledge of the Incident the 3rd Party might have and what action if any has been taken.
B8. Who currently holds evidence of the Incident? Provide name and contact information.
B9. What steps are required or being taken to preserve evidence of the Incident? Describe.
C. Risk/Exposure - Attempt to determine to what extent risk and/or exposure is presented by this Incident.
C1. Can we reasonably determine the risk or exposure?
C2. To what degree are we certain that the data has or has not been released?

C3. Do we have contact with someone who has "firsthand" knowledge of the circumstance (e.g., the owner of a stolen laptop)? Provide name and contact information.
C4. What firsthand knowledge have we determined? Describe what is known.
C5. Can we identify and do we have contact with the party that received the data or caused the compromise? Describe what is known.
C6. Identify the impacted parties, if possible. Are they University Clients or 3rd Parties? Provide estimated number, if known.
C7. What is the risk or exposure to the University? Describe.
C8. What is the risk or exposure to the Client? Describe.
C9. What is the risk or exposure to the 3rd Party? Describe.
C10. Can we determine to what extent news outlets may know of this Incident? Describe.
D. Next Steps - Determine what information or action is required to better assess or address this Incident.
D1. Do we have enough information to establish the category and severity of the Incident? - If "yes", declare the Incident category and severity. - If "no", describe what else might be required.
D2. If additional data collection data is required, assign responsibility to IRT member for collection and reporting to IRT.
D3. Is there any deadline or reporting requirement (self-imposed or regulatory) we need to address? Provide details.
D4. Based on current knowledge, do we require resources of the Secondary Team? If so, determine the makeup and assign responsibility for contact to IRT members.
D5. What communications need to be established? Provide details.
D6. Are there any immediate issues that have not been addressed? Describe.
D7. Recap all work and responsibility assignments.
D8. When do we meet again to follow-up? Provide details.

Corrective Measures - Appendix E

The IRT will determine and cause the execution of the appropriate activities and processes required to quickly restore circumstances to a normalized (secure) state.

Corrective measures are designed with the primary objectives of:

- Secure the processing environment.
- Restore the processing environment to its normalized state.

A. Corrective Measures – Unauthorized Access Activities that may be required to return conditions from *unauthorized access* to a normalized and secure processing state.
A1. Change passwords/passphrases on all local user and administrator accounts or otherwise disable the accounts as appropriate.
A2. Change passwords/passphrases for all administrator accounts where the account uses the same password/passphrase across multiple appliances or systems (servers, firewalls, routers).
A3. Rebuild systems to a secure state.
A4. Restore systems with data known to be of high integrity.
A5. Apply OS and application patches and updates.
A6. Modify access control lists as deemed appropriate.
A7. Implement IP filtering as deemed appropriate.
A8. Modify/implement firewall rulesets as deemed appropriate.
A9. Ensure anti-virus is enabled and current.
A10. Make all personnel "security aware".

A11. Monitor/scan systems to ensure problems have been resolved.
A12. Notify IR Team of status and any action taken.
B. Corrective Measures – Unauthorized Acquisition Activities that may be required to return conditions from an *unauthorized acquisition* to a normalized and secure processing state.
B1. Retrieve or restore assets where possible.
B2. Store all sensitive materials in a secure manner (e.g., lockable cabinets or storage areas/container).
B3. Install/replace locks and issue keys only to authorized personnel.
B4. Restore security devices and/or apparatus to working condition.
B5. Remove and retain unauthorized equipment from network/area.
B6. Implement physical security devices and improvements (e.g., equipment cables, alarms) as deemed appropriate.
B7. Make all personnel "security aware".
B8. Notify IR Team of status and any action taken.

Guidelines for IT Customer Service - Appendix F

Primary Objective

The primary objective is to determine if the problem being reported is a security incident. In most instances, the problem being reported will not constitute an incident as defined within the protocol (see Definitions – Information Security Incident - Categories).

No set of questions will address every circumstance; previous experience with an individual and intuition may be relied upon to help determine if an incident has occurred. Support personnel are accountable for asking the questions about an incident, making a reasonable attempt at determining if an incident has occurred, recording facts and responses to questions, and forwarding pertinent information to the responsible parties.

Problem Reporting

Familiarity with this protocol's definitions will assist support personnel in making a determination if a security incident has occurred. Individuals reporting problems and/or incidents should be informed as to the reason for the questions (i.e., the University is attempting to determine if sensitive data is at risk or compromised) and all individuals should be encouraged to openly discuss the problem being reported. Any information provided by an individual that helps in the determination is of considerable value; the individual's cooperation is critical, greatly appreciated and should be recognized.

Inquiries

For those individuals who may be reporting a security incident, questions that might be asked include but are not limited to:

- Were passwords accessed and/or released?
- Were Social Security Numbers stored or processed?
- Were medical records of individuals present or accessed?
- Were credit card numbers or financial information disclosed?
- Did physical theft of computer equipment occur?

Discovery and Reporting

If the answers to the inquiries indicate that an incident may have occurred, support personnel should assume that an incident has actually occurred and perform the following activities:

- Obtain and record the contact information for the individual reporting the problem (name, telephone numbers, e-mail address)
- Record relevant information about the incident (e.g., time/date of suspected occurrence, type of information compromised, location of the compromise)
- Inform the individual to expect contact from a member of the Incident Response Team
- Request the individual to treat the incident as a confidential matter
- Contact the "on call" Network engineer for further assistance.