Approved: 7/13/05 Revised: 5/03/07

University of Massachusetts
Cybercrime and Data Security Incident Handling Plan and Process

What is a Data Security Incident?

A data security incident is any event whereby some aspect of computer security or University data is threatened and/or adversely impacted. Such events may include attempts (either failed or successful) to gain unauthorized access to a system or its data; loss of data confidentiality, disruption of data or system integrity; disruption or denial of availability/service; misuse of data or resources; violation of law; changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent; damage to systems or software, data or system intrusion, web site defacement, etc.

Why is an Incident Handling Process Needed?

The advent of the Internet and integrated computer systems has resulted in easier access to data and systems by not only legitimate users but also hackers and curious external parties. This new "open" environment lends itself to data security incidents including but not limited to virus/worm attacks, web page defacement, and denial of service. Add to this, incidents that have been taking place for years - data corruption due to human error, natural disasters, and poor backup procedures - and you have a problem waiting to happen. When these incidents occur staff are most often thrust into an emergency, fast paced situation requiring quick decision-making. Under pressure, and possibly not fully knowledgeable about all types of incidents, it is easy for organizations and incident handling teams to make costly mistakes both from a restoration and legal prosecution standpoint. It is therefore critical that a well thought out, simple and understood incident handling plan is put in place before staff are required to react to a data security incident. The creation of such a plan will allow for limited loss/liability (e.g., loss of reputation, financial, data, time; ability to defend against unfounded unfair dismissal claims; avoiding privacy violations during investigations; limit possibility of additional harm done during investigation), consistent handling of security incidents, proper data and evidence collection, appropriate notification and documentation (i.e., reduced misinformation or inappropriate information leaking), full recovery, and proper follow-up.

Incident Handling Plan - Preparation

Before the University Data Security Incident Handling Plan (i.e., Incident Plan) can be implemented several preparation and incident preventions steps need to be implemented. Preventing incidents is usually less costly and more effective than having to react to incidents once they have occurred. Preparation/Prevention steps are included in Attachment 1.

Proper Documentation

One key factor that must be kept in mind throughout the entire incident response process is that of proper and controlled documentation of any security incident. It is important to document security incidents so that the University can be proactive in implementing controls to counteract recurring incidents and so that legal counsel and law enforcement have the information needed to perform a successful prosecution of the incident perpetrator if they choose to do so. The improper/inappropriate handling of evidence could be considered tampering with evidence (e.g., hard drives, logs, emails, etc.). Actions that have the potential to alter, damage or destroy original evidence may be closely scrutinized. Documentation is a critical part of incident handling and takes place throughout all steps and phases of incident response activities.

Documented incident information must be properly handled so that it can later be proven that there was no opportunity for modification of the evidence from the time it was collected to the time it is presented in legal proceedings. Security incidents should be documented on the Data Security Incident Identification and Investigation Report (See Attachment 2 for an example of the online web form). This Report includes general survey and investigation information including but not limited to:

- Date and time of the incident;
- Typed of incident (e.g., virus, equipment theft, probes the network mapping, and appropriate use, hoaxes, unauthorized access, Trojan horse, web page defacement, e-mail harassment, denial of service, hacking, etc.);
- Photos of equipment, location, etc., if appropriate**;**
- Description of the incident;
- Location of the incident (e.g., computer system, software application, web URL, data center/facility);
- Serial numbers of hardware, software that have been impacted by the security incident;
- Descriptions of facilities impacted by the security incident;
- Assets affected;
- External systems affected;
- Names of departments and personnel involved in or impacted by the incident (e.g., persons discovering/reporting and researching the incident, the individuals to whom the incident was reported, the perpetrator- if known, legal authorities involved in any related investigation); and
- The response to the incident (e.g., network/system shutdown, account monitoring or locking, web page removal, etc.), and
- Any follow-up actions discussed or taken.

Additionally, Coordinating and Investigating Team members should include any other detailed documentation about the incident as part of this Report. Teams should also complete the Incident Communication Log (Attachment 4) detailing all contacts made regarding the declared incident.

Individuals investigating an incident should also recover backup data that predates the incident, as it may prove valuable as additional evidence of the incident prior to its detection. Documentation should also include all logs and printouts used to determine that an incident has occurred or used to monitor continued security incident activity. All logs, printouts and documentation should be numbered, and dated by appropriate personnel. Original handwritten notes should be copied and the original notes sealed as part of the chain of custody (i.e., legal term that describes the collection, transportation, and storage of evidence to prevent alteration, loss, physical damage, or destruction). Electronic data should be captured as soon as possible and the process of making copies (e.g., hard drive of laptop or desktop, disks, etc.) of evidence should be videotaped (including the surroundings/office in which the computer/object was located), witnessed and signed off by an independent party. If the incident type requires that law enforcement be notified and the Investigating Team must disconnect the impacted computer from the network or shutdown a stand-alone computer/object, the computer/object should be segregated, stored in a secure container then labeled and marked with the date, time and initials of the individual disconnecting and placing the computer in the secure container. All steps taken/activities performed should be documented by anyone accessing the secured object from the point of the incident report (e.g. If it is necessary to remove the object for any type of testing, then there would be another series of "markings" on the container, indicating who did what and when).

The incident coordinator is responsible for obtaining a secure repository for the evidence and documentation related to the security incident under investigation. Access to this repository should be severely limited and controlled, so that the University can later prove who had access to the evidence thereby supporting the necessary chain of evidence. If a key gains access to the repository, this key should be stamped “not a duplicate” and access to this key should be severely limited and controlled. Note that any and every person with access to the evidence may have to testify if the security incident results in a court trial.

Whenever evidence changes hands, the recipient should sign for each item. The incident coordinator should ensure that every item turned over to law-enforcement or legal counsel is detailed and signed for as part of the chain of custody process. Maintenance of this chain will be critical if the incident goes to court. Individuals having access to incident documentation and evidence should be kept to a minimum, and the contents of the documentation should be on a need to know basis.

Because different people may view/interpret some types of materials (e.g., “obscene” or inappropriate materials) differently, it is important to present such materials in a direct, non-emotional way. One unbiased way to present such information is by creating a spreadsheet noting the activity type (e.g., download, stored, sent, created) and the material rating (e.g., PG, R, X, etc.). The use of standard, consistent documentation will remove investigator judgment and bias from materials collected that may later be used in legal prosecution. It is critical that evidence be factual and not contain speculation, assumptions, or judgments.

As noted in the Identification Section of this document, legal counsel should be notified at the onset of any incident investigation related to inappropriate use (e.g., access, storing or transmission of pornographic material, online stalking) and all information/materials compiled during the incident survey and investigation should be returned to only the attorney. Legal counsel will know how to appropriately secure such sensitive evidence.

There is no federal legal rule that requires the University to keep evidence for specific length of time. Normally, law enforcement will keep its copies of evidence associated with a prosecution as long as they deem fit. This does not however, affect or determine how long the University has to keep copies of evidence used as evidence in the prosecution of a computer crime. Generally, the statute of limitations for a computer crime is five years, so unless dictated otherwise by legal counsel this retention period should be followed.

Incident Handling Plan

The University Data Security Incident Handling Plan (i.e., Incident Plan) functions in conjunction with the University Business Continuity and Planning Guidelines and includes the following stages:

I. Detection – Identification and Reporting
II. Containment
III. Eradication
IV. Recovery
V. Follow-up

The Incident Plan can be followed independent of the particular hardware, operating systems, protocols, or applications involved in the incident. The Incident Plan insures that: mechanisms are in place to prevent, detect and alert personnel that an incident has taken place; consistent and appropriate steps are taken to contain and/or eradicate the incident; proper documentation is developed to assist with incident recording and possible prosecution of the incident; appropriate and comprehensive recovery steps are followed; and timely and comprehensive incident follow up takes place to minimize the risk of the vulnerability occurring again. The cost of a security incident includes damage to reputation, loss of productivity due to system downtime, loss of data, and time spent on incident investigation, containment and eradication. The implementation of an Incident Plan will minimize costs by allowing the University to respond to the incident quickly, knowledgably, and comprehensively.

The Incident Plan will ensure that everyone understands how a security event or incident will be handled. It should be noted however, that not every step of the full plan will always be called for. The significance/priority of the suspected/declared incident will determine who is notified and which steps are included in the incident handling process. The Incident Plan should be regularly updated as the environment and responsible parties change, and as new vulnerabilities and risks arise.

The following individuals/teams are involved in incident handling and may include overlapping members or may be made up of totally different members that will handle security incidents:

- The **Incident Coordinator** is the individual responsible for incident handling at a specific campus or within the President's Office. The Incident Coordinator coordinates incident investigation, documentation, and follow-up. The incident coordinator does not need to be a security expert, but does need to have general knowledge of the University; its policies, standards, and procedures; and some experience in incident handling including evidence handling. The incident coordinator needs to be accessible during off-hours as incidents often take place outside of normal working hours, weekends or on holidays, and should have a backup to ensure that someone is available should an incident take place.

- **Coordinating/Organizing Team** (i.e., Coordinating Team) - This team, led by a Campus/President's Office Incident Coordinator, is centrally oriented and performs overall coordination of the Incident Plan implementation when an incident has been determined to have taken place. This team also works with the various incident Investigating Teams to decide whether the shutdown of the system involved in the security incident is needed in order to avoid even greater harm, translate the assessments of the Investigating Team into recovery steps that the Incident Coordinating Team authorizes, and to perform post-incident analysis.

  Representatives from the following areas should be included on the Coordinating Team:

  - Incident Coordinator,
  - Legal counsel,
  - Public Affairs,
  - Data security including the appropriate Information Security Officer or designee,
  - Audit,
  - Investigating Team lead, and
  - Other personnel (e.g., Campus CIO, local law-enforcement, FBI, etc.) determined at the time to be necessary for the complete investigation and follow-up of the particular incident.

  Depending on the size or number of concurrent incidents (at the same campus or within the University), the Coordinating Team may need to organize a command post similar to when a large disaster takes place. Such a command center should include phone lines, voicemail boxes, fax machines, and any other resources needed to properly investigate and document large or multiple incidents. During multiple incident situations, experienced incident investigators may need to work with the Coordinating Team to triage the situation and assign investigative tasks to less trained personnel for some of the incidents. Triage personnel need to be trained to prioritize incidents and disperse teams to the individual incidents.

- **Investigating Team(s) -** This team is local to the site/campus of the incident and performs specific investigative, containment, eradication, and follow-up steps. This/These team(s) should consist of technology and functional specialist from various units in disciplines including:

- A representative from the site/area where the security incident is suspected (e.g. department head, web administrator, network administrator, etc.),
- Staff knowledgeable about or considered experts in the type of suspected incident,
- Computer forensic specialists. It is critical that if each campus is unable to have its own computer forensics trained expert, a University-wide resource is available to assist in campus related investigations,
- Data security personnel,
- Personnel responsible for the physical security of a site under investigation. This is especially important if the area is secured by alarms or other physical controls.
- University Audit, if appropriate, and
- Other personnel determined at the time to be necessary to complete the incident determination, investigation, containment, and/or eradication.

The Coordinating and Investigating teams are responsible for both proactive and reactive efforts related to computer security at the University.

Incident Handling Plan Steps

See Attachment 3 for a flowchart of the incident handling process. Incident response usually includes assessing incoming reports about incidents (identification, triage, prioritization), determining a plan of action if an incident is declared and following up the handling process once the incident has been eradicated

I. Detection

Detection steps include identification and reporting.

A. Identification

All the preparation and prevention in the world cannot fully insulate the University from a data security incident taking place. The identification process (e.g., determining whether or not an incident has occurred, and, if one has occurred, determining the nature of the incident) normally begins after someone has noticed an anomaly in the system or network. This phase includes informing and soliciting help from people who can help the user understand and solve the problem.

If an incident is suspected, the first step is to identify the incident. This initial investigation is considered the incident survey phase in which the nature and scope of the incident is determined. The identification process may call on the expertise of systems or network administrators, or support staff to help determine if system anomalies are indeed security incidents or just harmless anomalies. It is important to recognize that not every network or system anomaly will be a security incident.
It is also important to make sure the appropriate personnel are involved with determining if an incident has taken place and that this process is carried out in an organized, methodical process. Undirected or incorrect activities could cause the misdiagnosis of the nature of the incident, loss of forensic evidence, and possibly creation of a worse situation than the incident itself may have cost.

Unless the Investigating Team is facing a situation requiring the immediate shutdown of the suspect system to stop further damage, the Investigating Team should begin to identify the evidence before they perform any tests/tasks on the suspect system. The Investigating Team should keep track of any expenses incurred to investigate the suspected/declared incident and the number of hours spent investigating the incident. This will allow the Investigating Team to calculate the cost of any damage the incident that may have cause.

1. **Determine whether or not an incident has occurred –** There will be different indicators based on different systems. Systems administrators should determine and document what indicators are needed to monitor their own systems (See Attachment 5 for Recommended List of Tools for Incident Detection and Eradication). Before time and resources are expended performing deep analysis of indicators, check for simple mistakes, including errors in system configuration or an application program, hardware failures, and user or system administrator (i.e., the individual most often responsible for operational security for a subset of machines at a site or facility) errors. Taking the time to evaluate the configurations for simple mistakes may also help systems administrators to expose other related problems or vulnerabilities. Once simple mistakes have been quantified or ruled out, it is much easier to determine the total scope of the security incident. Indicators system administrators should look at include:

   - Abnormal network traffic – look for inexplicable packets originating from UMass bound for the Internet, especially at boot up
   - Activity in previously idle accounts
   - Gaps in accounting logs
   - Increase in general hacker activity; Internet-wide increase in probing
   - New or unfamiliar filenames
   - New setuid root scripts
   - Odd calls to the Helpdesk regarding an account and/or password
   - System crashes
   - System slowdowns – extreme or unusual
   - Undocumented changes in directories
   - Unexplained filling of file systems
   - Unfamiliar or strange user names
   - Unusual offsite access
   - Unusual visits to staff offices (e.g., unknown support staff)
   - Reviewing logs can prove to be invaluable when trying to detect security incidents.

2. Determine the priority and significance of the incident. When determining this priority the Investigating Team should consider the criticality of the impacted resources (e.g., public web server; Campus student system; user desktop, etc.), and the current and potential technical impact of the incident

(e.g. root compromise, data destruction, confidential data compromise/release, etc.). Resources will be assigned according to the following priorities, listed in decreasing order:

Incident Definition	Priority	Time Frame to Respond
Threats to the physical safety of human beings.	1	Immediate
Actual threat/unauthorized access to confidential, restricted or critical data /systems; or network	1	Immediate
Root or system-level attacks on any IT system or any part of the campus or University backbone network infrastructure	1	Immediate
Large-scale attacks of any kind, (e.g. viruses, sniffing attacks, IRC, botnet, "social engineering" attacks, password cracking attacks)	1	Immediate
Active targeting of critical systems, networks or systems housing confidential or restricted data.	2	Within 2 hours of discovery/detection
Actual threat/unauthorized access to unclassified/non-critical data/systems	3	Within 24 hours of discovery/detection
Threats, harassment, online stalking, child pornograpy, identity theft and other criminal offenses involving individual user accounts	3	Within 24 hours of discovery/detection/ complaint
Compromise of individual user accounts on individual or multi-user systems	3	Within 24 hours of discovery/detection/ complaint
Compromise of desktop systems	3	Within 24 hours of discovery/detection/ complaint
Web site defacement	3	Within 24 hours of discovery/detection/ complaint
Localized virus infection	3	Within 24 hours of discovery/detection/ complaint
Violation of DMCA	3	Within 24 hours of discovery/detection/ complaint

Incident Definition	Priority	Time Frame to Respond
Missing/Stolen equipment	3 (If missing/ stolen equipment housed confidential/critical data, the priority should be escalated to level 1 or 2 depending on the type of data)	Within 24 hours of discovery/detection/ complaint
Active targeting non-critical systems or systems housing unclassified data	4	Within 48 hours of discovery/detection/ complaint
Denial of service on individual user accounts (e.g. mailbombing).	4	Within 48 hours of discovery/detection/ complaint
Incident shows possible malicious intent or unintentional violation of security policy	4	Within 48 hours of discovery/detection/ complaint

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent. Examples of Incidents include, but are not limited to: root compromise; user compromise; denial of service/distributed denial of service attacks (successful or not); website defacement' detection of malicious logic, worms, viruses; scanning of data (confidential, critical, unclassified, etc); misuse of resources; spam emailing; fraudulent email; social engineering; harassing/offensive email;

3. Begin logging incident information on the Data Security Incident Identification and Investigation Report (See Attachment 2 for an example of the online web form the Investigation Team Lead should complete). Investigation notes should indicate the steps taken to determine the nature and scope of the incident, including who did what, when, how and why specific steps were taken. The notes/documentation should be chronological and factual. Care should be taken to avoid speculation and assumption. It is also helpful if the incident results in prosecution, for the Investigating Team to obtain corroborating evidence from multiple, independent sources, if possible. This is the first step in maintaining a clear set of evidence that may become critical if the security incident moves into the legal and prosecution phase.

B. Reporting

Timely and secure methods of communication should be used to notify responsible parties that an incident has been declared and that the investigation process has begun. The use of the call tree will be initiated when the Coordinating Team declares a valid incident has taken place. Coordinating and Investigating Team call lists contain information detailing work, cell, and home phone numbers; pager numbers and other methods of contact can be found in the Computer Security Incident Contact List (See Attachment 6). Laminated business card type documents that include the call list, and minimal tree information should be given and carried by Coordinating and Investigating Team members at all times. The call tree should be tested at least once a year to ensure the process functions properly. Once an incident has been declared a short message (e.g., 911) can be sent to Investigating Team members alerting them to call a predetermined voice mailbox where a full message detailing the status of the incident is placed. This will save time and resources instead of someone having to repeat the same message to get everyone up to speed.

All documentation and evidence, except that involved in inappropriate use investigations, should be turned over to the Incident Coordinator or their designee (anyone handling evidence should be properly trained so as not to compromise possible future prosecution).

1. Notify the appropriate Incident Coordinator that a security incident has occurred. The Incident Coordinator will work with area experts to verify the documented information and ensure that an incident has actually occurred. There is a potential for misdiagnosis if inexperienced personnel have made the original determination. Once verified, the incident coordinator is responsible for declaring the incident is valid and the Incident Plan will go into effect. Once the incident is formally declared, the full notification process and any required in-depth investigation should begin.

2. Notify the appropriate management, legal counsel and Campus/University Coordinating Teams based on the incident priority as noted on pages 8 and 9 above.

   Legal counsel should be notified at the onset of any incident investigation related to inappropriate use (e.g., access, storing or transmission of pornographic material, online stalking). Investigating Teams do not know ahead of time what they may discover. By contacting legal counsel at the onset of an inappropriate use incident investigation, the investigation falls under “Attorney Work Product” privileges. To fall under “Attorney Work Product” privileges, the Investigative Team must work on behalf of the attorney (i.e., requests for the investigation come from the attorney) and all information must be returned to the attorney alone. “Attorney Work Product” privileges protect materials prepared by the attorney or their agents in preparation for possible litigation from discovery (i.e., a legal request to see evidence). Investigating Teams researching inappropriate use should be small and maintain strict confidentiality so as to avoid any damage to any individual's reputation or work environment while under investigation.

Send a notice to all Coordinating Team members (e.g., securityincident@um*x*.edu where x denotes the campus). These email lists not only route the incident notice to the affected campus but to other campus Coordinating Teams so that each campus can determine whether they may be encountering the same issue.

3. Obtain approval of an in-depth investigation, if needed, from the Coordinating Team and upper management. Investigations carry risk (e.g., possible privacy infringement, misinterpretation of law, errors of omission, loss of investigative control to external authorities; damage to personal reputation) so approval should be obtained before further investigation continues.

4. Convene a full Investigating Team if a deeper investigation is approved, or if the group performing the incident survey phase needs assistance or additional expertise. Note that not every security incident will require an in-depth analysis or investigation. Some situations may be as simple as declaring that a virus has infected some University systems and then moving forward with containment and eradication. If in-depth analysis or additional evidence is needed, the Coordinating Team will call for further investigation.

As the investigation into the security incident continues, the Incident Coordinator is responsible for:

- The compilation of all documentation and evidence. Ensuring that documentation and evidence are appropriately sealed and controlled so as to maintain it in original, unaltered, and complete form.

- Acquiring resources needed by the Investigating Team (e.g., backup software or hardware, high capacity drives, cables, diskette/CDs, portable printers, meeting room space, fax machines, etc.).

- Keeping senior management and the system "owner" advised of the status of the incident, as appropriate.

- Ensuring that the University Incident Storm Center is maintained and kept up to date.

- The notification of the incident to external parties other than those under the responsibility of Public Affairs. This includes notification to external parties that are impacted by any incidents initiated from University systems, networks or users. Campuses must comply with the RFC complaint list structure by maintaining a mail list called abuse@umxx.edu (where umxx refers to a specific campus) to receive and respond to notices by external organizations of incidents originating from the University.

- Ensuring that the Investigating Team members have timely access to systems they are investigating, and that they know how to use the system. The system/network administrators should establish procedures to ensure that these passwords stay current and to ensure that the identity of individuals requesting access to envelopes is verified so that only appropriately authorized personnel have access to this information. Additionally, the password should be changed whenever it has been accessed and the system access is no longer required (i.e., when the incident investigation is complete).

5. Notify law enforcement, if appropriate. Law enforcement should be notified immediately when the following incident types are detected: child pornography, online stalking, threatening/sexually harassing emails, counterfeiting, hate crimes, voyeurism, identity theft, fraud/theft and computer trespass. The investigation and documentation of such crimes may require special handling by law enforcement and incorrect handling could compromise future legal options**.** There is no single proper way to report a suspected computer crime. The University needs to discuss the proper method to report computer crimes to local and federal (i.e., FBI) law enforcement and document this process before any incidents takes place.

   When an incident is reported to law enforcement, the following information should be available:

   - Names, location, and purpose of operating systems involved.
   - Names and location of programs accessed.
   - Highest classification of information stored in the systems.
   - Impact (compromise of information or dollar loss).
   - How intrusion access was obtained; how attack was carried out.
   - Status of attack.
   - Steps taken to mitigate or remediate.
   - Other organizations affected.
   - Potential suspects, such as outsiders or current or former employees/contractors.
   - Available evidence to assist in the investigation (i.e., logs, physical evidence).

II. Containment

The goal of containment is to limit the impact and magnitude of a valid security incident, and to gather important information. If data related to the incident is not gather quickly, accurately and completely it may be lost forever, and therefore the University may not have sufficient information to prosecute an incident. In general, the system in which a security incident has been detected and validated should be disconnected from the network from the console. This will ensure that the impact of the incident is limited.

Once the Incident Coordinator, in conjunction with the Coordinating and Investigating Teams, has declared that a valid incident has taken place, a small Investigating Team should be deployed to begin investigating and documenting the incident. The team should be small, so as not to become unwieldy or lead to an unnecessary confusion, bad communication or lack of coordination. The composition of the team (i.e., Internet or network support groups, application specialists, etc.) will depend on the type of incident that has taken place. The Investigating Team should:

- Secure the facilities or area in which the incident took place, if possible. Physical security may require the assistance of University Police.

- Review information provided from the identification phase. This information will give the Investigating Team a starting point so they can determine what tasks need to be completed in what data needs to be further review.

- Conduct further examination as needed. Conducting an examination on the original evidence media should be avoided. Rather, examinations should be conducted on a forensic copy of the original evidence, or via forensic evidence files.

  Examination of the media should be completed logically and systematically by starting where the data of evidentiary value is most likely to be found. These locations will vary depending on the nature and scope of the case. Examples of items to be noted might include:

  - If the media is a hard drive the number and type of partitions should be noted. If the media is an optical disc then the number of sessions should be noted.

  - File systems on the media should be noted.

  - A full directory listing should be made to include folder structure, filenames, date/time stamps, logical file sizes, etc.

  - Installed operating systems should be noted.

  - User created files should be examined using native applications, file viewers, or hex viewers. This includes such files as text documents, spreadsheets, databases, financial data, electronic mail, digital photographs, sound and other multimedia files, etc.

- Operating system files and application created files should be examined, if present. This would include, but is not limited to: Boot files, registry files, swap files, temporary files, cache files, history files, log files, etc.
- Installed applications should be noted.
- File hash comparisons may be used to exclude or include files for examination.
- Unused and unallocated space on each volume should be examined for previously deleted data, deleted folders, slack space data, intentionally placed data. Previously deleted filenames of apparent evidentiary value should be noted. Files may be automatically carved out of the unallocated portion of the unused space based upon known file headers.
- Keyword searches may be conducted to identify files or areas of the drive that might contain data of evidentiary value and to narrow the examination scope.
- The system area of the volume (i.e. FAT, MFT, etc.) should be examined and any irregularities or peculiarities noted.
- Examination of areas of the media that are not normally accessible such as extra tracks or sectors on a floppy disk, or a host-protected area on a hard drive may be required.
- To facilitate examination of data, user settings, device and software functionality, etc. the computer may be booted using either a copy of the boot drive or by using a protected device on the original device to determined functionality of the hardware and/or software.
- The forensic software used during the examination should be noted by its version and should be used in accordance with the vendors licensing agreement. The software should also be properly tested and validated for its forensic use by the examiner or the examiner’s agency.

At the conclusion of the examination process sufficient notation of any discovered evidence of an apparent incriminating or material/significant nature should be made. Sufficient documentation should be made of all standard procedures and processes initiated as well as detailed notation of any variations made to the standard procedures. Any output of the recovered data should be properly marked.

- Complete the incident containment section 6 of the Data Security Incident Identification and Investigation Report (See Attachment 2 for an example of the online web form the Investigation Team Lead should complete) which indicates whether the affected system has been removed from the network, proper backup's have been made, and by whom and when.

- Not allow the system to be altered in any way until backups have been completed.

- Avoid using obvious methods (e.g., ping, finger, telnet to, nslookup) used to look for intruders, if a network-based intrusion is determined. If the perpetrator becomes aware that the Investigating Team is trying to locate them, they may delete University files and temporarily or permanently break off communication in an effort to stop investigative measures.

- Maintain standard procedures (e.g., if an active intrusion detection system is implemented so that it drops connections or blocks attacking IP addresses, do not disable the intrusion detection system to try to gather more information. This might warn the hacker).

- Be cautious regarding the possible compromise of system binaries. Avoid logging into a suspect system as root or administrator, and then start typing commands such as ftp to download tools from another site. If possible, record the cryptographic fingerprint of critical binary files (using md5 hash cryptographic algorithm verify data integrity on known images) for the University’s core operating systems. . The analysis of the system should be performed with known good binaries brought into the system. Some organizations build disks with core binaries.

- Backup the system as soon as an incident is suspected. Computer criminals are becoming more adept at destroying evidence of illegal activity to avoid detection or prosecution. Making full backups immediately captures evidence that otherwise might be destroyed before the Investigating Team has time to review them. Law enforcement prefers the use of write blocking to imaging or file archiving. Write blocking prevents any attempt to write to a drive while allowing complete access to download, view and investigate the drive under examination. If write blocking is not possible, the Investigating Team should use disk imaging/archiving of the impacted system with known good binaries to obtain a full backup. Two backups or at least one backup and a duplicate copy should be made - one to keep sealed as evidence and one to use as a source of additional backups. The backup will provide a basis for comparison later if verification that additional unauthorized activity has occurred is needed.

  It is critical that system backups be made to new, unused media so that juries cannot be convinced that the evidence is faulty because it is written over old information. Sealed backups should be turned over to the incident coordinator or their designee so that they can be secured and the chain of custody can be ensured. If backups are not properly secured and protected, the prosecution of the case can be damaged.

- Acquire logs (e.g., authentication, application, system, and/or network device logs) and other sources of information quickly because many log files turn over fairly quickly. Review logs and cryptographic file signature databases from other systems on the same subnet and from systems that regularly connect to the suspect system.

- Determine the risk to continuing operations. The Investigating Team needs to determine whether the suspect system should be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operation status, so that any activity on the system can be monitored. In most instances, the system should be disconnected from the network to minimize the severity and impact of the incident. The Investigating Team lead should recommend which step to take and, if possible based on the severity of the incident and time available, seek approval from the Coordinating Team before proceeding.

- Change passwords for root or administrator account names, as these are common hacker targets. Passwords should be changed on the suspected systems and all systems that it regularly interacts with. This is especially critical if the system has been a subject of a sniffer attack. If questioned, password changes can be publicized as part of a system upgrade or because of a recommendation by audit. This will minimize rumors and questions during the investigation.

III. Eradication

The goal of eradication is to eliminate or mitigate the factors that resulted in a compromise of system activity. This stage is critical because if the Investigating Team fails to adequately eradicate the problem another similar or more devastating incident could occur.

A. Determine The Cause And Symptoms Of The Incident

Information collected during the initial determination and investigation phase may be sufficient to determine the cause(s) of the incident. Investigating Team members must conduct a comprehensive review of the data gathered and not assume that one factor alone contributed to the compromise. By failing to look at all possible causes, the Team is allowing possible vulnerabilities to continue to exist, thereby putting the University at risk for additional security incidents.

If the Investigating Team has not compiled enough evidence to determine how the incident took place, team members should list all realistic possibilities/scenarios that could have caused the incident based on the available information. If possible, and feasible, the team can use forensics tools to re-create the incident in order to compile additional forensic information (See Attachment 5 For Recommended List of Tools for Incident Detection and Eradication). Only knowledgeable, experienced team members should perform incident recreation to ensure no further system damage occurs.

B. Implement Appropriate Controls

Implement appropriate controls to address the vulnerabilities that allowed the security incident under investigation. Once a system has been compromised, its password file, IP address and operating system may be made public to the hacker community. As result, the system may get repeatedly probed or attacked for weeks after the initial incident. It is therefore critical to implement appropriate controls (e.g., firewalls, router filters, moving the system to a new name or IP address, or moving the business functions on the compromised system to a more secure operating system) as soon as possible. The Investigating Team should not allow a compromised system to reestablish network connections until the cause of the incident is determined and proper controls have been implemented to ensure the incident will not happen again.

If the controls that need to be implemented are outside the control of the Investigating Team, they should work with the Coordinating Team and the system owner to ensure the controls are implemented on a timely basis. The Investigating Team may decide that the cause of the compromise was an insecure operating system or network environment that cannot be addressed by simply rebuilding an existing system or network. The Investigating Team may recommend to the Coordinating Team that management approve redeployment and of a safer operating system before reconnection to the network is allowed. The Coordinating Team, in conjunction with the Investigating Team, should verify that the recommended controls have been implemented before the compromised system is authorized for reconnection.

C. Assess Vulnerability of Other Systems

Make sure other platforms within the University are not vulnerable to the same factors that allowed the security incident under investigation. Investigating Teams should quickly use automated vulnerability assessment tools (See Attachment 5 for Recommended List Of Tools For Incident Detection And Eradication) to search for the vulnerabilities that caused the incident under investigation to make sure other systems are not compromised or waiting to be compromised. Using a combination of tools is most beneficial because each tool may have unique capabilities. Team members should be aware that if a network-based assessment tool is used, they have no guarantee that all potentially vulnerable systems are online at the time of the search. This process should also include determining whether configurations and software versions need to be updated.

Previous work performed to identify critical assets, and instituting a configuration and patch management program become key in determining if other platforms/systems are affected by the cause of a security incident. Without such an inventory, the Investigating Team will waste time trying to track down affected systems or not be able to ensure that all vulnerable systems have been addressed.

D. Decide what to do to remove the cause of the incident.
The steps taken will depend on the type and extent of the incident:

- **Hoax –** use available hoax websites (e.g., http://www.symantec.com/avcenter/, http://urbanlegends.miningco.com/, www.ciac.org/ciac/) to validate whether the mail message is a hoax or valid incident. Notify user community of the hoax.

- **Virus infections** - Remove the virus from all systems and media such as floppy disks with virus eradication software. Many viruses are not detectable or removable. If this situation arises, reformatting the infected system is the only method to ensure that the system is clean and will not further virus infection.

- **Malicious code infections -** Commercial software and public domain software exists to remove common or "in the wild" malicious code (e.g., Trojans, worms, etc).

  The Investigating Team also needs to be aware of the threat of re-infection specially from backup media that have not been disinfected and should also ensure that an effective procedure is in place that updates antivirus software regularly to ensure new viruses will be found.

- **Network Intrusion**- Many attacks over networks are achieved in two parts:
  - A vulnerability is exploited and the system is accessed.
  - Once in, the hacker installs a tool or backdoor to provide continued access. The hacker may also try to use the compromised system unauthorized access to other computers.

  If a network intrusion is verified, the Investigating Team needs to:
    - Refrain from direct contact with the suspected hacker. If contact does occur, Investigating Team members should maintain detailed records of all contact noting the dates, times and detailed description of the communication on the Incident Communications Log (See Attachment 4).
    - Search for sniffer and backdoor access programs and remove them immediately.
    - Determine whether the hacker has modified the compromised system (e.g., altered system binaries, etc).

The most practical way to search for system alterations is to, if possible, immediately disconnect the compromised system from the network until the Investigating Team has completed its forensic analysis. If disconnection is not possible than the Investigating Team must consider alternatives (e.g., installing a firewall in front of the compromised system; filtering connections, etc.). The Investigating Team will need information regarding what the baseline norm of the system was before the compromise took place so they can determine if alterations have taken place. They will also need access to uninfected system binaries and application programs installed on the compromised system.

The Investigating Team should notify external sources of attack of the attack on University networks/systems, when possible. All logfiles sent to external entities should have time zone information included in them.

IV. Recovery

During this phase the Investigating Team, with the possible assistance of the system owner, will attempt to return the system to full operational status. Speed is critical, however, it is even more critical to ensure that improper or inadequate recovery does not allow future incidents.

The Investigating Team needs to:

- Make sure the backups are not infected, and are accurate and complete. If clean backups do not exist, the Investigating Team may have to rebuild the system from CD-ROM or other trusted media and apply patches, or use a backup from a similar system that has not been compromised. Because it can be difficult to determine when the attack took place it may be difficult selecting the best backup however every effort should be made to obtain the cleanest, most recent backup.

- Review the Business Resumption Plan for the system. This plan should detail partial and full system test procedures that can be used to verify successful restore.

- Restore the compromised system with the assistance of the system administrator.

- Verify, in conjunction with the system administrator and owner that the system has been fully and properly restored, and that normal operations can resume. Verification can be accomplished through the use of system test procedures outlined in the system’s Business Resumption Plan. If such system test procedures do not exist, verification can be achieved by running the restored system through its normal tasks while closely monitoring it. During testing, the Investigating Team must be aware that patches or controls implemented to prevent future vulnerabilities may cause the restored system to function differently than it did before the incident. This needs to be considered when determining if the restore was successful. Once the system administrator and owner of the restored system verify recovery, they should notify users that the system is back online and available for use.

- Scan machine after restoration to ensure that vulnerable ports are not open, etc. (See Attachment 5 for Recommended List of Tools for Incident Detection and Eradication).

- Continue to monitor the restored system to ensure that that back door, hidden code or other alterations were not missed during eradication thereby allowing other security incidents. The Investigative Team should determine the appropriate monitoring period based on the severity and complexity of the initial incident.

- Recommend the closure of the incident investigation. The Coordinating Team will decide when the investigation is officially closed.

V. Post Incident Follow-Up

Within 2 weeks after the incident has been closed, the incident investigation should be reviewed by the Coordinating and Investigating Team to determine where improvements can be made in the incident handling and response process. Such follow-up will help the Teams learn more from the experience.

Review should result in an Incident Follow-up Report (See Attachment 7 for an example of the online web form the Coordinating and Investigating Teams should complete) that has been discussed and agreed upon by both Teams. The Report will contain the following information:

- Brief description of incident and resolution.
- Preparation steps that assisted in the detection, containment or eradication of the vulnerability.
- Other proactive steps and tools that could have assisted in the blocking or earlier detection of the vulnerability.
- Additional tools that could assist in the containment and eradication of the vulnerability.
- Overview (description, strengths, weaknesses) of communication between Teams, owner, University community, law enforcement, etc. including recommendations for improvement.
- Difficulties/Roadblocks encountered.
- Additional Training needed.
- Need to rotate team members in/out of Coordinating or Investigating Teams.
- Impact of incident on University operations (include amount of downtime, size of affected users, etc).
- Cost, in dollars, of incident.
- Description of any lost data, damaged hardware, etc and its value.
- Summary of recommendations to improve incident handling process.

The Report should be submitted to the CIO Council who will be responsible for authorizing the implementation of any recommendations included in the Report.

Once the CIO Council approves any recommendations made in the Report, the Coordinating and Investigating Teams are responsible for ensuring the recommendations are implemented and reporting back to CIO Council in a timely fashion.

Additionally, Campus Incident Coordinators should submit a quarterly report to the CIO Council summarizing all incident activity (i.e., all priority levels). This will allow the CIO Council to remain informed regarding the level and frequency of data security incidents taking place at the Campus and University level.