University
Critical Incident Response Plan

Index: CIRP-062005

DRAFT

Table of Contents

Critical Incident Response Plan Charter

Critical Incident Response Plan

Purpose

The purpose of this Critical Incident Response Plan (CIRP) is to provide the University with a plan that addresses the dynamics of a critical incident. A critical incident is one that threatens confidentiality, integrity or availability of University information assets with high impact, high threat involving high risk and great vulnerability. The CIRP defines the roles and responsibilities for critical incident response team members, defines incident severity levels, outlines a process flow for incident management, and includes methodologies for conducting response activities.

The CIRP may be used simultaneously during certain disasters along with the existing University Continuous Operations Plan Overview (MUCOPO) to address information security and production computer/network continuity.

A critical incident in IT Services will be addressed as a University Disaster when the Chief Information Officer (CIO) communicates that a University Disaster has been declared as stipulated in the X University Continuous Operations Plan Overview. In the case of a University Disaster, all activities in this plan (The CIRP) will continue to be directed through the CIO.

The following table summarizes these relationships:

Activity	**Managed By**	**Document**
Incident Response	IT Services CNOC	
Critical Incident Response	IT Services CIC	Critical Incident Response Plan
University Disaster	University Disaster Coordinator	University Continuous Operations Plan Overview

Scope

The CIRP applies to University Information Technology Services and all system and services for which it is responsible.

This CIRP covers all computer systems and networks connected to X University's network, to include the campuses of ______. The CIRP is mandated to take all actions required to assure the protection of X University's reputation, information assets and the student's, faculties', and staff's information assets that reside under X University's control.

Under some circumstances the CIRP should be used for servers and systems used by other departments within the University.

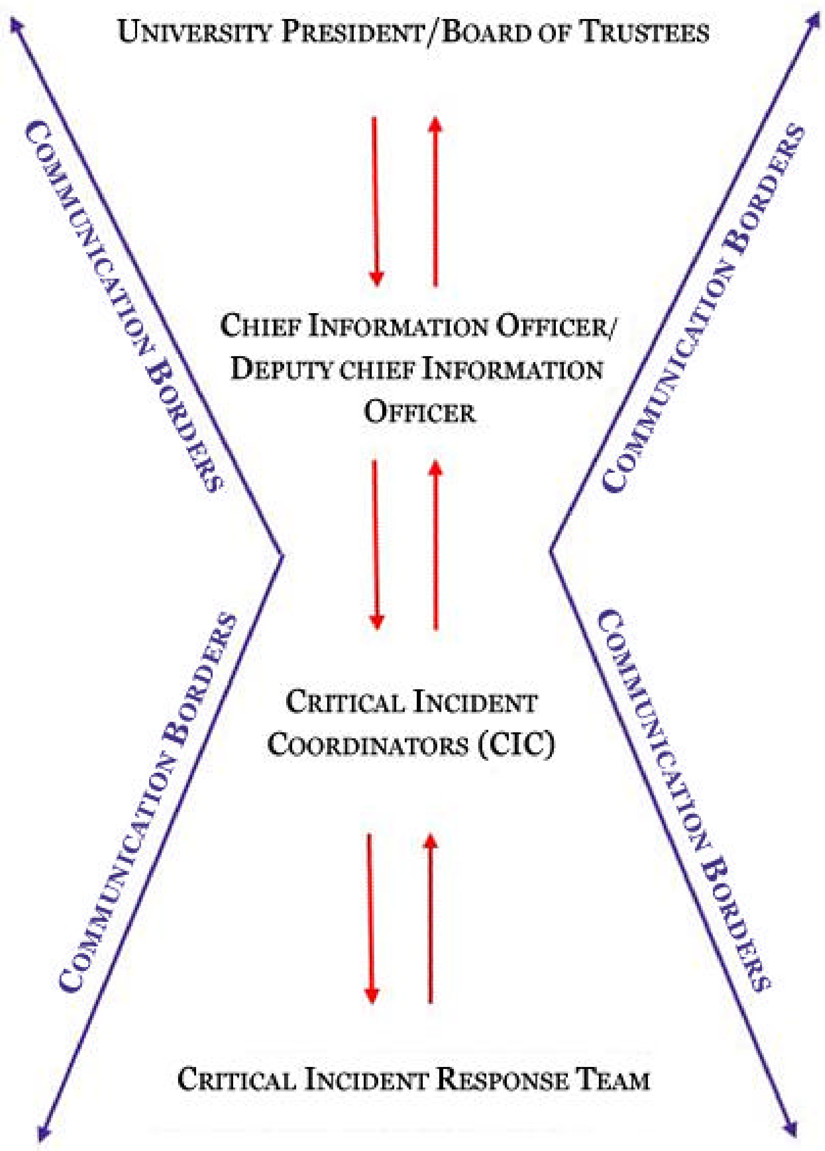
Definitions and Acronyms

- CIRP – Critical Incident Response Plan
- CIRT – Critical Incident Response Team
- CIC – Critical Incident Coordinator(s)
- PDRP– Production Disaster Recovery Plan
- PEC – President's Executive Council
- UCOP – University Continuous Operations Plan
- Critical Incident – See the table of contents for a whole section defining Critical Incident

Policy for IT Services

Critical incidents will occur that require full participation of IT technical personnel as well as divisional leadership to properly manage the outcome. To accomplish this IT Services will establish critical incident response procedures that will ensure that appropriate leadership and technical resources are involved to (i) assess the seriousness of an incident, (ii) assess the extent of damage, (iii) identify the vulnerability created and (iv) estimate what additional resources are required to mitigate the incident. It will also ensure that proper follow-up reporting occurs and that procedures are adjusted so that responses to future incidents are improved.

Critical Incident Response Information Flow



The above diagram illustrates how information regarding the nature and management of a critical incident should be communicated. The CIRT may become aware of a suspected critical incident in a number of ways. Some examples include:

- An intrusion detection (IDS) sensor reports suspicious network traffic
- The log files on the firewall show a large volume of “denied” packets from several Internet sites, with patterns suggesting a determined attempt to gain access
- A user reports, through the Support Desk or other means, that their system appears to have been infected by a computer virus or other malicious agent
- Media reports suggest that a fast-spreading computer virus/worm has been discovered, causing widespread shutdowns of corporate electronic mail systems

- University Communications and/or Risk Management receive a telephone call from a reporter seeking comment on another site's claims that X University's systems were used to break into the caller's systems

Regardless of how the critical incident alert reaches X University, a CIC must be identified and notified in the most expeditious manner to ensure appropriate action (see steps in the Alert phase below). During normal business hours the alert may come from the Support Desk; whereas after hours the alert may be generated by the Computing Network Operations Center (CNOC).

CIRP Services

This plan's main function is to assist with the response and management of a critical incident. This CIRP will provide information on two types of services that contain incidents and protect X University's reputation. The two primary CIRP services are ***proactive*** services and ***reactive*** services and they are described within this section. It is important to understand that this document is a "living" document and routine maintenance is necessary to ensure that the information within it is accurate and current. The Security Office is responsible to see that the Critical Incident Response Plan and related policies and procedures are maintained, distributed to team members, and communicated to upper management. The CNOC is responsible to keep contact information current.

Proactive Services

Proactive Services are CIRT tasks designed to prevent or mitigate the severity of an incident before it occurs. These services are provided when the team is not actively managing an incident, and include: Plan Maintenance, Policy Changes, Plan Education, Announcements, and Compliance Testing.

MAINTENANCE	▪ Maintain the CIRP according to lessons learned from post-mortem review, and update contact information as members change ▪ Schedule regular testing procedures to ensure information is correct and the information flow is clear to the named CIRT members
SECURITY POLICY CHANGES	▪ Develop and request necessary policy changes related to the specific root cause of an incident ▪ Ensure the recommended solution is aligned with the business risk model
EDUCATION	▪ Provide necessary training to their roles and responsibilities as identified in the plan ▪ Ensure that the named personnel are educated on their expectations ▪ Ensure that the CICs have an understanding of their roles and responsibilities ▪ Provide security awareness training to the CIRT
ANNOUNCEMENTS	▪ Disseminate information about protective measures to take against existing and upcoming security threats to the enterprise
COMPLIANCE TESTING	▪ Perform security vulnerability assessments and coordinate the remediation of identified security risks

1.0 Preparation steps

Main Idea: create an infrastructure that provides rapid answers to questions that you will have <u>after</u> an incident occurs.

1.1 Identify your vital assets.
1.2 Prepare individual hosts
1.3 Prepare the network
1.4 Establish appropriate policies and procedures
1.5 Create a response tool kit
1.6 Establish an incident response team

Reactive Services (Response Steps 2 thru 6)

Reactive Services are broken into five (5) categories; Alert, Triage, Response, Recovery, and Maintenance.

ALERT PHASE: During the Alert phase, the initial incident report is generated and reported to the CIC. Once the report is received, the CIC makes a preliminary escalation determination based upon suspected or confirmed elements of the alert.

2.0 Detection and Analysis Begin Alert Phase

2.1 Incident is suspected to be critical

2.1.1 Reports of incidents without classification are received by Support Services and/or the CNOC from a variety of sources. Picture a large funnel of sources feeding Support Services and/or the CNOC with reports. For example: TSR's, Red Siren, Abuse@listserv.muohio.edu which feeds Security@listserv.muohio.edu. The CNOC monitors these lists. TSR's have the direct phone number to the CNOC. The support desk voice mail changes at 10:00 p.m. to indicate that emergency calls may be pushed through to the CNOC.

2.1.2 Remedy tickets created by Support Services and the CNOC. Can be created in parallel with other activities. Support opens one Remedy ticket per caller, the CNOC opens one per incident.

2.1.3 Incident is suspected to be a **Critical Incident**? No = proceed. Yes = goto 2.2

- See the definition of critical incident in this document (page 13)
- See examples of critical incident in this document (page 14)
- Consider the following. Has confidential data been exposed? Could it involve violation of the law? Could it involve notification of customers? Have critical services been disrupted for an unacceptable length of time?
- See Appendix D summarizing data valuation

2.1.4 Staff assigned by the Support Services or the CNOC to evaluate non-critical incidents. The result may be that the incident is suspected to be critical.

2.1.5 Incident is suspected to be a Critical Incident after further investigation? No = resolution Yes = goto 2.2

TRIAGE PHASE: Whether an incident is actually critical is assessed by the CIC during Triage phase. It may or may not be declared a Critical Incident; if so, a CIRT is assembled and resources are assigned through by CIC. This is true regardless of the method by which an incident arrives, e.g. Support Desk Call, the CNOC, email from external source or student, or Intrusion Detection alert).

2.2 Suspicion of Critical Incident is reported to a Critical Incident Coordinator selected by the CNOC from the approved list in this document (page 21). The best technical person for an incident should not be chosen as the CIC to coordinate the incident; rather that technical person would serve as a technical resource.

2.2.1 Suspicion of Critical Incident should be logged with the time stamp and relevant factors that raised the suspicion. Mandia p. 19

2.2.2 How long after suspecting that an incident is critical does the CNOC have to contact and/or get ownership by a coordinator? Generally 10 minutes. Note that in other cases the CNOC has procedures to get a person on the job in 10 min. The answer should take into consideration how long the CIC has to respond to the call.

2.2.3 Assess the extent of the damage, identify the vulnerability created, and estimate what additional resources are required to mitigate the incident.

2.3 Incident is declared to be critical

2.3.1 See page 13 for the ways that an incident may be declared critical

2.3.2 See section 2.1.3 for ways to distinguish a critical from a non-critical incident

2.3.3 Critical Incident Declaration is issued? No = goto 2.1.x. Yes = proceed.

2.3.4 What is a declaration? An oral notification to the CIO/DCIO constitutes a declaration.

2.3.5 Who received the declaration? The CIO/DCIO. Go to the CIO if he is available, otherwise to the DCIO. You may walk into his office, call him at home or on his cell phone (the NOC has the numbers).

2.3.6 How is a declaration recorded? The CNOC will record the fact that the incident has been declared critical by marking the 'Incident Report' form. The CIC should also make a written log entry with date/time stamp and the factors that made the incident critical.

2.3.7 Notification checklist is completed? The CIC should log the fact that all required notifications are complete.

> **RESPONSE PHASE:** The Response phase includes developing the plan to provide analysis and containment of compromised systems and elimination of the incident's source. The CIC will assign response plan tasks to specific members of the CIRT.

RESPONSE }

- The CIRT will identify the cause of the critical incident
- The CIRT and CIC will fully determine the containment process and determine which actions are immediately required to minimize any additional loss and/or exposure to information assets
- During the response phase the first responder(s) need to be familiar and comfortable with the evidence collection guidelines. Every incident is handled differently, however, strong documentation will assist with protecting the evidence and ensuring the Chain of Custody is intact. (See Appendix F)

2.4 Critical Incident Response Team is assembled **Begin Response Phase**

2.4.1 The coordinator identifies team members and uses whatever resources including the NOC to contact team members and draft them to be part of the team. Membership on the team will vary according to the nature of the incident. At minimum you will have a CIC, a scribe, and a technical person. The CIC could act as the scribe if the time permits. Team members may negotiate with the CIC on whether to serve but ultimately must report if the CIC requests it. Any IT Services employee may be drafted to the team although the preference is to select from the list of CIC's and technical staff in this document (page 21).

2.4.2 The coordinator formulates initial response

2.5 Initial Response

2.5.1 Any emergency measures not already taken including initial containment

2.5.2 Is it really a Critical Incident? No= goto 2.1.x. Yes = proceed

2.6 Formulate Response Strategy. Mandia, p. 21

2.7 Present Response Strategy Options to Management. The Critical Incident Coordinator will attempt to get management input but may proceed without it.

3.0 Containment and Investigation

3.1 Containment and investigation may be pursued simultaneously. Containment means prevent the spread of a problem from A to B, secure means prevent the problem from getting to A again. Containment could occur in the CNOC before a critical incident is declared. Hardening will secure the environment but could do more -- hardening could go beyond preventing the particular critical incident being responded to at that time.

3.2 Secure the system, Mandia p. 26
3.3 Forensic Duplication? No = proceed with investigation. Yes = duplicate

Appendix F is a helpful summary of forensic information. The decision to capture forensic data is made by the CIO / DCIO or their designee within 10 minutes after the CIC has posed the question, otherwise the CIC is authorized to decide and proceed. Protection of confidential information is more important than obtaining evidence.

There is a difference between "forensic" and "diagnostic". Diagnostic procedures are followed to recognize that there is a problem and to discover the cause and solution of the problem. The word 'forensic' is reserved for scientific methods of collecting evidence intended for presentation in a court of law. Forensic methods may or may not be used in diagnostic procedures.

3.4 Investigation, Mandia p. 25
3.5 Perform Network Monitoring, Mandia p. 27
3.6 Isolation and containment

4.0 Eradication

4.1 Eradication may be necessary to eliminate components of the incident such as deleting malicious code or disabling breached user accounts.
4.2 For some incidents, eradication is either not necessary or performed during recovery.

RECOVERY PHASE: During the Recovery Phase, the CIRT investigates the causes for the incident and the damage incurred. Affected systems and services are restored to their original state. The CIRT conducts post mortem activities to identify and document the root cause and business impact of the incident, and remediation activities to prevent its reoccurrence.

RECOVERY }

- The defined actions determined during the response phase to recover affected systems are implemented. production systems that do not require configuration changes are then returned to their original state
- In addition, systems that require configuration or application changes to prevent the incident's reoccurrence are updated, tested, and redeployed into production

5.0 Recovery **Begin Recovery Phase**

5.1 Consider what was compromised
5.2 Choose a recovery strategy. The following is a suggestive list: ghost, patch, code upgrade, application fix, firewall rule, quarantine, packet shaper filters, access control list, intermediate recovery on alternate equipment.
5.2.1 Intermediate recovery on alternate equipment may involve pre-arranged agreements with alternate sites such as: The Ohio State University or The University of Cincinnati. The CNOC has information on these agreements and the CIC will need to involve the CNOC if they are to be used. The CIC should be aware that intermediate recovery to alternate equipment could lengthen the overall recovery time.
5.2.2 A document titled "Production Disaster Recovery" kept in the CNOC contains an up-to-date and comprehensive description of applicable resources and procedures. A University Disaster does not need to be declared to use many of these resources; a Critical Incident Coordinator (CIC) may use resources provisioned in Production Disaster Recovery when permission is granted by the CIO.

5.3 Recover to normal operations
5.4 Harden systems to prevent similar incidents
5.5 Declare to the CIO/DCIO that the incident is resolved and transfer control of the relevant services back to the CNOC. The incident is not finally closed until the completion of the next phase, phase 6.

MAINTENANCE PHASE: Ongoing validation of the Critical Incident Response Plan and the CIRT process will be achieved through regular exercises and after action reviews in the Maintenance phase.

MAINTENANCE }

- Post-mortem exercise is conducted to identify root cause and areas of improvement. See report in Appendix A.
  - ➢ This exercise should be conducted within 2 weeks of the incident.
- Any changes to the CIRP or policies/procedures should be addressed
- After the post-mortem phase is completed the critical incident can be closed by the CIC.

6.0 Follow-up **Begin Maintenance Phase**

6.1 Support criminal or civil prosecutions
6.2 File a Critical Incident Review Report (Appendix A) with the CIO's office and schedule a review meeting. CIO or a designee is to preside.

- Determine Root Cause*
- Determine Root Effect*
- Determine Total Cost of Incident*
- Publish and close incident with suggested updates to the Critical Incident Response Plan (CIRP)

*The exercise of determining the root cause, root effect and the total cost of an incident may not occur for each incident. The CIO/DCIO will direct the Critical Incident Response Team when **NOT** to perform these tasks.

6.3 Suggest process improvements to the chair of the Critical Incident Response Working Committee. The Committee will discuss and proposed additions to procedures for Steering Committee approval.

Incident Response Guidelines for CIO/ DCIO/ Leadership Team

2.3.5 Receive Declaration of Critical Incident From CIC. Ask questions like the following:
- Are you declaring a critical incident
- Does the NOC know about this and that you are the CIC
- Are there legal issues?
- Has data been lost or corrupted
- Do you need anything from me?
- Contact me when you have formulated a strategy or in _____ minutes.

2.3.5 Begin a personal log of activities for inclusion into the Incident Report

2..3.5 Each time the CIO / DCIO receives reports from the CIC, consider whether to contact other parts of the organization
- University Counsel who in turn is responsible to contact law enforcement and the FBI
- President and the Presidents Executive Counsel
- University Communications who in turn is responsible to make press releases based on information provided

3.3.1 Decide whether to collect forensic data

5.5 Receive Declaration of Resolution from the CIC

6.0 Receive written report from the CIC within time frame specified by the CIO

6.0 Meet with the CIC and other CIR team members to discuss the incident (generally within one week of the incident)

Priorities in Incident Handling

It is important to prioritize the CIRT actions to be taken during an incident before an actual incident occurs. Sometimes an incident may be so complex that it is impossible to respond to everything at once; priorities are essential. Human life and national security will take first precedence and it is generally more important to save data than to save system hardware and software.

PRIORITY	TASK
1	Protect human life and people's safety.
2	Protect sensitive information from disclosure, abuse or misuse.
3	Protect regulated information to ensure no criminal, civil and/or administrative action occurred.
4	Protect critical information, systems, and networks from compromise, damage, alteration or corruption.
5	Minimize business disruption.
6	Certify that the integrity and availability of the areas affected have been restored to a Production Ready and Active Environment.

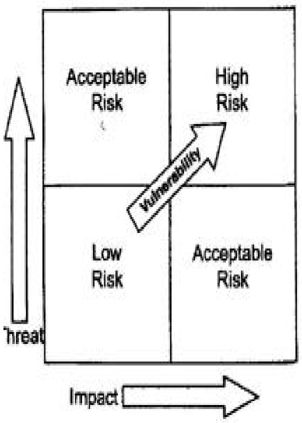
Determining That An Incident Is Critical: Incident Severity Levels

Critical Incident Defined

An **incident** is any adverse event that threatens the confidentiality, integrity, or availability of university information assets, information systems, and the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident.

Adverse events may include, denial-of-service attacks, loss of accountability, or damage to any part of the system. Examples include the insertion of malicious code (e.g. viruses, Trojan horses, or backdoors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks. See Vangelos.

Incidents as defined above vary in their impact on the University and in the degree of threat they pose; consequently not all incidents require the same response. Incidents with high impact and high threat involve high risk and great vulnerability to the University; such high risk incidents are called ‘**critical incidents’** and require that a Critical Incident Response Team (CIRT) be assembled to apply **appropriate response**. Non-critical incidents are incidents with either low or acceptable risk. A non-critical incident could become critical if its visibility could impact the reputation of the university.



Non-critical incidents also have appropriate response; however procedures for non-critical incidents are not outlined in this policy.

An incident is declared to be **critical** and a CIRT assembled in one of the following ways:

- A member of the Incident Response Steering Team declares it to be critical.
- Critical Incident Coordinator declares it to be critical.
- An appropriate University official declares to be critical.
- NOC staff declare it to be critical because the incident is on a list of critical incidents approved by the Incident Response Steering Team. See list below

Examples of a Critical Incident

The following examples of ‘critical incidents’ are given here to provide guidance to the CIC in determining if an incident is critical:

- A major virus attack involving the University
- Destruction or unauthorized modification of data on university systems
- Unauthorized disclosure of student, staff or faculty data
- A network intrusion
- A Denial of Service (DOS) attack
- Widespread electronic mail system failure or slow down
- Critical application failures (i.e., ERP)
- President’s e-mail forgery. Someone sent an e-mail to all students declaring that exams were cancelled and forged the President’s signature.
- Good Friday E-mail forgery. Someone sent an e-mail containing a Trojan Horse (Back Orifice?) forging the support desk signature and requesting recipients to execute it.
- Real time registration failure. The first time real time registration was used on the main campus, scarcity of courses resulted in overpowering the web servers and the database. Registration times for each group had already been advertised so could not easily be changed.
- E-mail migration. During migration of the e-mail system e-mail became unresponsive for 24-hours. Vendor interface with LDAP was a partial cause.
- Blaster worm.
- Machine Room power down. Full service took over 4 hours to restore.
- Slammer.
- Building Fire. A fire in the ___ building severed Network connections and threatened university information. The network was disconnected for over 24 hours.
- Graphics Feed of Objectionable material to the dorms. 1998.
- Road Runner clients in Southwest of the state could not get to the university. Road Runner had changed their router. It took 18 hours to resolve.
- 2000 people were notified via e-mail that they are no longer in class and their account will be disabled in 30 days. There was no actual risk, but high visibility. Because students were notified that they are no longer in class, it was necessary to notify the Provost. Therefore declare this a critical incident.
- Radio station has no network service by which to obtain weather and traffic information from local broadcaster. Subsequently they informed listeners that their internet service was down. This happened on three separate occasions. Equipment was purchased to solve this one.

Incident Severity Levels

As part of the initial incident response process, the CIC will need to make an assessment of the incident's impact and assign an appropriate severity level. This severity level will be based upon the potential impact to the operations or reputation of X University, and/or their students, faculty, and/or staff. An incident's severity level dictates the initial response and management activities associated with the event. As incident management activities continue, further assessment may effect a reassignment to a lower severity level. In this phase of the Incident Response Plan for X University, only incidents whose severity level is 'critical' are managed; however, other severity levels are outlined below for completeness.

Critical Level Successful penetration or denial-of-service attack(s) detected with significant impact on operations: very successful, difficult to control or counteract, large number of systems compromised, significant loss of confidential data, loss of mission-critical systems or applications, admin/root compromise, user account compromise, illegal file server share access. Significant risk of negative financial or public relations impact.

Medium Level Penetration or denial-of-service attack(s) detected with limited impact on operations. Minimally successful, easy to control or counteract, small number of systems compromised, little or no loss of confidential data, no loss of mission-critical systems or applications. Widespread instances of a new computer virus or worm that cannot be handled by deployed anti-virus software that may require corporate-wide activations of CIRT and/or site-administrators. Illegal mirrors and unapproved content (eg. games, porn, multi-media servers on corporate networks). Small risk of negative financial or public relations impact.

Low Level Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance. Intelligence received concerning threats to which systems may be vulnerable. Penetration or DoS attacks attempted with no impact on operations. Isolated instances of a new computer virus or work that cannot be handled by deployed anti-virus software.

Critical Incident – Any unexpected or unauthorized change, disclosure or interruption to X University's information resources that could be damaging to our students, staff, faculty, and/or reputation.

CIRT Roles and Responsibilities

Roles and Responsibilities

Within this section, the roles and responsibilities for the CIO/DCIO, Critical Incident Response/Recovery Sub-Team (CIRT), CIC, and Supporting Groups are defined. In addition, this section addresses the various IT Services functional areas within the University and their CIRT responsibilities.

The University has a pool of CICs. Should the initial CIC be unavailable or unavailable during the entire incident, then the CNOC or Support Desk should call the next CIC within 10 minutes.

- Ideally, the CICs should be matched to the type of critical incident occurring at the University.
- CICs should understand they may be asked to run an incident outside of their functional area.
- If the CIC is initially unavailable, an alternate will assume the CIC role in his/her stead.

Chief Information Officer / Deputy Chief Information Officer

This position will report directly to the University's President and Board of Trustee. This role will either involve or inform as the needs of the incident dictate. Communication of information during an incident will follow this flow to eliminate confusion and misinformation between groups.

The CIO/DCIO is responsible for executing or delegating the following:

- Setting priorities
- Notifying the University President and/or Board of Trustees of an incident declaration
- Communicating status of critical incident to the PEC
- Participating with CIC in forensic investigation decisions
- Designating the DCIO or an alternate to cover the responsibilities of the CIO role
- Notifying University Communications as appropriate for internal and external communication
- Owning of the CIC's incident work plan(s)
- Defining and issuing 'gag' orders within IT Services for particularly sensitive issues; the default guideline for communicating about a critical incident is on a need to know basis
- Notifying Human Resources as appropriate
- Notifying Legal as appropriate
- Notifying Campus Security as appropriate
- Chairing the Post Mortem – Closeout Phase

Critical Incident Coordinator (CIC)

This position will update the CIO/DCIO on a regular basis during a critical incident. The CIC will obtain technical expertise based on the incident declared.

The CIC is responsible for the following:

- Managing incident resources
- Determining if an incident is a Critical Incident and declaring it to be so.
- Maintaining communications between CIRT and the CIO/DCIO
- Reminding staff that communication is on a need to know basis or if the CIO has defined a 'gag order' informing team members and the CNOC of the nature of the 'gag'.
- Communicating to the CNOC and the IT Services Leadership Team that a critical incident has been declared and a CIRT has been formed
- Activating the CIRT and notifying the team of meeting locations and call-in telephone numbers
- Beginning a case file for the incident. Use to ensure information is properly collected and documented
- Developing containment procedures
- Establishing a Post Mortem Team to determine the root cause and root effect of the incident

- Working closely with the CIO/DCIO and University Counsel during forensic investigations
- Managing the incident work plan(s) and task assignments
- Raising dependency issues as they arise
- Designating an alternate CIC to cover the responsibilities that span more than 12 hours
- Coordinating hand-off meetings between shifts, and developing work plans that address tasks completed and outstanding
- Certifying that all systems are returned to operational quality with the cause rectified
- The secure destruction/retention of all materials at the end of an incident
- Identifying external personnel/resources as needed
- Recommending to the CIO/DCIO, if warranted, that the critical incident be upgraded to a disaster

Resource Coordinator (CNOC)

The Resource Coordinator must maintain a current list of all contact information for the CIRT. The CNOC will play this role for critical incidents.

The Resource Coordinator is responsible for the following:

- Establishing the “war room” during a computer incident
- Providing appropriate networks, computers, phones, and faxes
- Designating a scribe to document CIRT activities and follow the work plan established by the CIC.
- Establishing food provisions and lodging

CIRT Response Team

During an incident the CIC will assemble a team. Members will vary depending on the skill sets required to assist during an incident. Teams will vary in size depending on the need. This team will remain active until the incident is closed. The members will include staff from the IT Services Division as described later in this document. This team will be responsible for both response and recovery.

Response. The response duties of the team are to conduct triage of the incident, assist in containment of the incident, collect evidence for the post mortem report and if requested, conduct or assist in a forensic investigation.

- Assisting in the collection of evidence during an incident investigation
- Making recommendations to the CIC on remedial action on affected systems
- The Response Team may be called up 24 hours a day, 7 days a week, 365 days a year during a critical incident

Recovery. The response aspects of the team are centered around damage assessment, return to normal operations, rebuilding serves and systems, etc.

- Determining whether affected systems can be restored from backup tapes, or must be reinstalled
- Scrubbing all data before making it ready for reinstall
- Determining what data is lost and cannot be recovered or restored
- Reloading data on affected systems
- Restoring normal operations

CIRT Post Mortem Team

The Post Mortem Team is assembled by the CIC, chaired by the CIO or the DCIO. This team is part of the Reactive Services “Maintenance”. Their responsibilities are:

- Sending final incident reports to parties with a need-to-know
- Discussing procedural changes and updates
- Discussing configuration issues
- Deciding whether to conduct an investigation to determine what the root cause and root effects of the incident
- Discussing any task that were not completed

- Deciding whether it is necessary to determining the Total Cost of Incident (TCI)
- Recommending updates to policies, procedures, standards and the Critical Incident Response Plan as necessary

Support Desk

- Initiates communications for critical incidents to the CIC during business hours.
- Provides liaison with the user community
- Provides liaison with the CNOC
- Provides informational announcement for serious incidents per the direction of the CIC or CIO/DCIO
- Assesses an incident's impact to the desktop computer environment
- Provides assistance with viruses, Trojan horses, and worms
- Collects, stores, and assists in desktop system audit data analysis as necessary
- Coordinates change management in the desktop environment
- Coordinates change testing for the desktop computer environment
- Coordinates, implements, maintains and certifies all Microsoft operating systems changes on desktop and server systems
- Certifies changes to the desktop environment
- Implements desktop changes

Computing & Network Operations Centers (CNOC)

- Provides the critical phones numbers for X University President and Board of Trustees manila folder. The folder is labeled "Contact Phones. Mgt: Pres Exec Council: Board of Trustee"
- Holds the call-out list for University resources. This list resides at the following URL:

www.unitsmuohio.edu/mcs/techserv/noc/nocstaffonly/dreamweavernxfiles/phonelist.htm

- Initiates communications to the CIC as problems are detected or reported
- Responsible for coordination with emergency change management as directed by the CIC
- Monitoring of Intrusion Detection and/or Intrusion Prevention Systems
- Monitoring the Network using OpenView
- Assess alerts from the IDS/IPS
- Alerts the Support Desk to any incident for escalation
- Liaison with Red Siren

Security Office

- Creates security policies and procedures
- Create and maintain university security awareness
- Manage perimeter controls
- Oversight of Managed Security Services
- Oversee separation of duties for financial systems technical management
- System Hardware and software vulnerability analysis
- Create multiple platform technical and admin incident management procedures
- Perform system risk assessments
- Manage network user access. Disable and enable end-user accounts if required

Critical Incident Response Steering Committee *(proposed)*

- Appoint the Critical Incident Response Working Committee
- Receive requests for clarification and assistance from the Critical Incident Response Working Committee and advise them in their work
- Approve changes to the CIRP

Critical Incident Response Working Committee *(proposed)*

- Meet at least quarterly to update the CIRP
- Conduct training at least annually
- Receive recommendations from Post Mortem teams for improvements to CIRP
- Ongoing testing and evaluation of the CIRP operation

Campus Safety and Security

- Assist in interviews when requested
- Assist human resources during policy violations
- Coordinate with external law enforcement as required
- Liaison to Federal Bureau of Investigations (FBI) as requested by University Counsel

Disaster Recovery Team *(not part of Critical Incident Response)*

- Manages the development and maintenance of the Disaster Recovery Plan
- Receive declaration of disaster that would upgrade a critical incident to a disaster
- Liaison with X University's recovery sites
- Interfaces with the CIO/DCIO and/or the CIC to ensure proper integration and coordination between the CIRP and other crisis management plans, as required by event circumstances (Disaster Recovery Plan, Hurricane Preparedness Plan)

University Counsel

- Provides guidance to the CIO regarding legal and regulatory aspects of the incident and its public disclosure
- Advises Human Resources regarding investigations involving employees
- Advises the CIO/DCIO and/or CIC regarding decision to simply protect its operations or to pursue civil or criminal actions
- Consults with the CIO/DCIO and/or CIC regarding involvement with law enforcement
- Advises the CIO/DCIO and/or CIC regarding involvement with regulatory agencies
- Reviews communications drafted by University Communications as required
- Liaison to external counsel

Human Resources

- Advises CIO/DCIO and/or CIC on personnel matters
- Initiates employee related investigations along with University Counsel
- Participates in investigation interviews and furnishes legally permissible personal information as necessary
- Alerts the CIRT of any unusual employee behavior patterns during a critical incident or investigation
- Manages internal rumors and fields internal questions from the employee base that are not associated with an incident
- Coordinates internal employee communications along with University Counsel, as necessary

University Communications

- Provides external communications in consultation with University Counsel
- Responds to all external media inquiries
- Liaison to external public relation firms
- Ensure internal communications are consistent with external communications

Operations and Telecommunications

- Establishes new lines and communications bridges as directed by the CIC
- Provides necessary communication lines for the CIRT War Room
- Assesses an incident's routing and transmission impact
- Provides log data to the CIRT as required
- Provides assistance to the CIRT related to modems
- Provides assistance investigating PBX accounts and permissions
- Liaison with the following: Anixter, Sprint North Supply, Accu-tech – Supply Chain, Magnum Cable, Westco, Famous Telephone, NEC Integrated Business Solutions (Labor contract with them), Cincinnati Bell

Technical Support

- Coordinates change management and testing for Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Coordinates, implements, maintains and certifies the Operating System Environment for all Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux operation systems.
- Assesses an incident's impact to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Certifies and implements changes to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Coordinates and implements patches to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment
- Develops, maintains and implements hardening procedures for the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment
- Responsible for the entire electronic mail system utilized by X University.
  - ➢ Coordinates changes to the electronic Mail environment
  - ➢ Implements changes to messaging systems
  - ➢ Assesses impact of email or messaging based malware (malicious code)
- Performs backup procedures on the server environment
- Liaison with IBM, Solaris, DNS-1, and SendMail
- Responsible for SAN administration

Communication and Networking

- Collects, stores, and assists in system audit data analysis as necessary for the routers and firewalls
- Coordinates, implements, maintains and certifies all routing changes and OS changes to network devices.
- Provides Firewall Services
  - ? Implements changes to the firewall rule sets to assist in incident containment as necessary
  - ? Provides rule sets to the CIRT as required
  - ? Provides log data to the CIRT as required
- Assesses an incident's impact to Wide Area Network and/or Local Area Network.
- Assists in identifying the impact to the perimeter and Internet facing environments.
- Assists in identifying the impact to X University's wireless network
- Plans, maintains and audits the network infrastructure

CSS

- Assist in evaluation of business continuity and disaster recovery solutions
- Plans, maintains and audits the network infrastructure

Information System and Services / Student Systems and Business Systems

- Responsible for the Banner system and applications
- Conduct software support for the Banner system and applications
- Implements changes to the Banner system and applications

Database Administration

- Rebuild and implement installation for the databases
- Builds and configures the databases
- Provides backup and recovery services for the databases
- Overall security for the databases

Network Applications Group

- Responsible for Blackboard Course Info, MyX, WAS, Account Generation

Team Makeup by Position Title – list specific names

Chief Information Officer
Deputy Chief Information Officer
Incident Response Coordinators
Forensic Resources

Critical Incident Team Members

You may draft any IT Services staff that you need
The above staff are trained and area therefore first choice

Appendix A – Critical Incident Review Report

CNOC Incident Number (CNOC Remedy Ticket Number) __________
Date of Incident __________
Name of CIR Cordinator ___________

For all critical incidents the critical incident coordinator (CIC) must fill out this form within one week of the resolution and file the report with the office of the Vice President of Information Technology. Any relevant documents should be attached.

Preparation

1. Were controls applicable to the specific incident working properly? y/n
2. What conditions allowed the incident to occur?
3. Could more education of users or administrators have prevented the incident? y/n
4. Were all of the people necessary to respond to the incident familiar with the incident response plan? y/n
5. Were any actions that required management approval clear to participants throughout the incident? y/n

Detection

6. How soon after the incident started did the organization detect it?
7. Could different or better logging have enabled the organization to detect the incident sooner? y/n
8. Does the organization even know exactly when the incident started? y/n
9. How smooth was the process of invoking the incident response plan? 1 2 3 4 5 (5 = very smooth)
10. Were appropriate individuals outside of the incident response team notified? y/n
11. How well did the organization follow the plan? 1 2 3 4 5 (5 = very well)
12. Were the appropriate people available when the response team was called? y/n
13. Should there have been communication to inside and outside parties at this time; y/n
    and if so, was it done? y/n
14. Did all communication flow from the appropriate source? 1 2 3 4 5 (5 = all did)

Containment

15. How well was the incident contained? 1 2 3 4 5 (5 = very well)
16. Did the available staff have sufficient skills to do an effective job of containment? 1 2 3 4 5 (5 = all did)
17. If there were decisions on whether to disrupt service to internal or external customers, were they made by the appropriate people? y/n
18. Could changes to the environment make containment easier or faster in the future? y/n
19. Did technical staff document all of their activities? 1 2 3 4 5 (5 = all)

Eradication and Recovery

20. Was the recovery complete (no data permanently lost)? y/n
21. If the recovery involved multiple servers, users, networks, etc., how were decisions made on the relative priorities?
22. Did the decision process in the previous question follow the incident response plan? y/n
23. Were the technical processes used during these phases smooth? y/n
24. Was staff available with the necessary background and skills? y/n

Adapted from Kevin Mandea, p.

Appendix B – Who Contacts Whom

Who	Contacts	Whom
CIO/DCIO	Contacts	President / PEC HR University Counsel University Communications Safety and Security
CIC	Contacts	CIO/DCIO CNOC CIR Team Members (CNOC can assist) IT Services Management (listserv)
CNOC	Contacts	CIC Outage Notification list CIR Team Members (If CIC Requests)
Support Desk	Contacts	CNOC CIR Team Members (If CNOC knows) TSR's University
University Communications	Contacts	Press University
Safety and Security	Contacts	Law Enforcement (Oxford Police, FBI)
CIR Team Members	Contacts	

Appendix C – Time Guidelines

Time Guidelines	
Notify CIC if incident is suspected to be critical	10 minutes
Notify CNOC if incident declared critical	Immediate
Notify CIO/DCIO if incident declared critical	Immediate
Length of outage before time makes it critical	
Whether to do forensic investigation	10 minutes to get answer
Length of time between updates to the CIO/DCIO	1 hour or as requested
Conduct Post Mortem evaluation	2 weeks

Appendix D – Tabular Summary of Data Valuation

Appendix E – Components of a Notification Letter

Edit the following components into a letter of notification or web site statement. Headings are boldface, several examples follow most headings. Edit the sample text into your letter and delete the heading. Don't disclose anything that hampers the investigation or gives additional information to those who would do harm.

What happened?
(E.g. A server/laptop/desktop was breached/stolen/lost in <school or location>)
In December 2004, campus officials were notified of the theft of an [department name] laptop computer

When did the breach occur and/or when was it detected?

How was it detected?

What data was potentially compromised?
This computer contained a list of [department] student employees. The list included the names and Social Security Numbers of the students.

How much data was compromised?

For whom was data compromised?

Why you are being notified.
We are notifying you of this security breach because you are one of the students whose personal information was present on the laptop. Although we have no evidence that an unauthorized individual has actually retrieved and is using your personal data, we are bringing this incident to your attention, in accordance with California law, so that you can be extra alert to signs of any possible misuse of your personal identity.

What steps are/were being taken?
(e.g. machine taken off the net, law enforcement (local/FBI), Credit card companies notified (for cases where contact information is needed about cardholders), etc)

Is any data known to be fraudulently used or is notification precautionary?

What steps should individuals take?
(e.g. place a fraud alert with the credit bureaus, contact credit card companies, close accounts, etc.)

Although there is no evidence that an unauthorized person has obtained your personal information and is using it, there are some steps you can take, exercising abundant caution, to protect yourself. First, you may place a fraud alert with credit bureaus and/or periodically run a credit report to ensure accounts have not been activated without your knowledge. If you determine that an account has been fraudulently established using your identity, you should contact law enforcement and the financial agency. The following references provide additional information about identity theft:

- Federal Trade Commission website on identify theft (http://www.consumer.gov/idtheft/)
- Social Security Administration fraud line at 1-800-269-0271
- Major Credit Bureau Numbers

    - Equifax 1-800-525-6285
    - Experian 1-888-397-3742
    - Trans Union 1-800-680-7289
- Identify Theft Victim Checklist (http://www.privacy.ca.gov/sheets/cis3english.htm)

Apology or statement of commitment to security

We regret that your information may have been subject to unauthorized access and have taken remedial measures to ensure that this situation is not repeated. The X University is committed to maintaining the privacy of student information and takes many precautions for the security of personal information. In response to incidents of theft like this one and the increasing number of internet-enabled computer attacks, the University is continually modifying its systems and practices to enhance the security of sensitive information. We sincerely regret any inconvenience this incident presents to you.

Anticipated next steps, if any.
e.g. intention to notify if any additional information becomes available?

Who to contact for additional information
Contact/name, number, hours of availability, web site, hotline, email address, etc.

Should you have further questions about this matter, please contact [name of contact}, [title of contact], at [email address of contact] or [phone number].

Signature
Who makes most sense – president, dean, other contact familiar to the individual, consider multiple signatories for different constituent groups.

Appendix F – Forensic Evidence Methodology

Once an incident has been declared and a decision has been made to preserve electronic evidence for use in either administrative, civil or criminal remedies, specific steps should be taken to ensure integrity of data and preservation of evidence.

The CIRT charter, as defined in Section 1 of the CIRP, is to provide business, service and data preservation and is not chartered with maintaining computer forensic capabilities. Therefore, this methodology is not intended to be in-depth, but rather intended to highlight the importance of evidence handling procedures before outside computer forensics teams are called upon.

The below list is by no means all-inclusive and should not limit the scope of evaluation as to where digital evidence may only be found.

TYPE OF INCIDENT	POSSIBLE LOCATIONS OF RELEVANT EVIDENCE
Network Intrusion	System Logs User Logs Proxy Logs Router & Firewall Logs
Email Threats	Mail Servers Router & Firewall Logs Individual Workstations Backup Tapes
Internal Employee or Contractor Activity	System Logs Mail Server Logs User Logs Proxy Logs Router & Firewall Logs Individual Workstations Electronic Organizers Removable Media

Definitions:

Electronic Evidence:

Electronic Evidence is information and data of suspected investigative value that is stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA evidence is latent. In its natural state, data contained in the physical object that holds electronic evidence such as a server, desktop PC or hand held device such as PDA's like a Palm Pilot, iPAQ or Handspring Visor cannot be seen. Equipment and software are required to make the evidence visible.

Electronic evidence can be found in user created files, encrypted files, and computer created files or in hardware components such as Network Interface Cards (NIC), routers and switches as well as on removable media such as floppy and zip disks, CD and DVD discs, USB thumb drives and tape. Other hardware devices such as all-in-one copiers, scanners, printers and fax machines often maintain user access records and temporary buffer files, which may contain valuable data.

Electronic evidence can be altered, damaged, or destroyed by improper handling or examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. When dealing with electronic evidence, general forensic and procedural principles should be applied. The Federal Guidelines for Searching and Seizing Computers is an excellent resource for an in depth information on this topic.

Chain-of Custody

Chain of Custody pertains to the documentation and securing of evidence items recovered during an incident. Each item is assigned a unique identifying number or name, initialed by the team member recovering the item and documented in a format listing each item, where it was located, the date and time of recovery, and the team member involved. Items are then secured in a controlled environment under limited access. A record is kept documenting each person who comes into contact with the evidence item and the purpose for that persons possession of the item. Accountability for ensuring this process is adhered to lies with the CIC, with responsibility for following this procedure residing with each team member encountering items of an evidentiary nature.

In general, the following concepts should be applied:

- Actions taken to secure and collect electronic evidence should not change the evidence.
- Persons conducting examination of electronic evidence should be trained and preferably certified for this purpose.
- Activity relating to the seizure, examination, storage, or transfer of electronic evidence should be fully documented, preserved, and available for review.

Many incident investigations, especially those expected to result in criminal or civil legal action will include a forensic analysis component. The CIRT members will frequently serve dual roles as investigators and forensic analysts. Each role has distinct areas of responsibility.

NOTE: *Incident responders should use caution when seizing electronic evidence devices. The improper access of data stored in electronic devices may violate provisions of Federal Law such as the Electronic Communications Privacy Act (ECPA). Additional legal process or policy may be necessary.*

Collecting Evidence

Securing and evaluating the scene.

After securing the scene or equipment, the first responder should visually identify both conventional and electronic evidence and determine if perishable evidence exists. The first responder should evaluate the scene and formulate a search plan. Do not at this time alter the condition of any electronic devices unless a threat to the safety of persons is indicated or business operations are such that continued operation or non-operation threatened the continued function of vital business operations. This decision should be made by the CIO/DCIO, CIC or their designee.

IF A DEVICE IS OFF, LEAVE IT OFF. IF IT IS ON, LEAVE IT ON AND SEEK ADDITIONAL ASSISTANCE

Protect perishable data both physically and electronically. Perishable data can be found on pagers, caller ID boxes, electronic organizers, cell phones and other similar devices. The first responder should keep in mind that any device containing perishable data should be immediately secured, documented and if possible photographed.

- Observe and document the condition and location of the computer system including power status of the computer (on, off, or in sleep mode)
- Identify and document related electronic components that will not be collected.
- Photograph, if possible, the entire scene to create a visual record as noted by the first responder.

- Photograph and document the front of the computer or location of a device and take written notes on what appears on the monitor screen. Active programs may require videotaping or more extensive documentation of monitor screen activity.

Handling Evidence

The CIC is accountable for ensuring chain-of-custody on all evidence collected. Individual CIRP team members are responsible for protecting the integrity of any evidence they work with. Whenever possible, analysis should be performed on copies of the evidence not the originals.

Evidence will be handled in accordance with the guidelines set forth within this plan. An effort will be made to conduct analysis of digital evidence only on copies of the suspect media. A forensic duplicate of the original evidence will be made as soon as possible, and will be handled as much as possible in the following manner:

1. A hash (checksum, message digest) of the suspect media will be made.
2. Forensic duplicate of the media will be made. The forensic image(s) may be on tape, disk, magneto-optical cartridge, CD-R, DVD+R or any combination thereof as determined by the investigator.
3. A hash of the forensic duplicate will be made.
4. The hashes of the original and forensic duplicate will be compared to verify accuracy.
5. If necessary, the forensic image may be remounted to recreate its original configuration.
6. Suspect files or data may be transferred to CD/DVD or other media to aid in their review. In such circumstances, it should be noted that the media contains only select files and is not a forensic image of the original media.

NOTE: *Many electronic devices contain sensitive memory that requires continuous power to maintain the data such as a battery or AC power. Unplugging the power source or allowing the battery to discharge can cause a loss of data. After determining the method of collection, collect and store the power supply adaptor or cable if present with the recovered device.*

Analyzing Evidence

Forensic analysis is a technical examination rather than investigative in nature, even though the analysis is part of an incident investigation. When conducting an analysis, the analyst must adhere to the following:

1. **Analysis must be an unbiased examination of the evidence submitted.** The analyst's focus must not be on connecting the evidence to the crime, but rather on analyzing the media in accordance with the investigator's request. Both positive and negative evidence must be documented. Analysts must go beyond the initial indicators of criminal involvement to insure no other possibilities exist. This insures that the investigator has the best possible information from which to work, and that the analyst appears to the court as an impartial examiner.
2. **Forensic analysis <u>does not</u> pronounce or imply guilt.** The purpose of forensics analysis is to determine whether *indicators* exist which can tie the suspect hardware to the incident under investigation. Files and/or data obtained from the media may *indicate* that the suspect computer, hard drive, or whatever may have performed a certain task, but not that a specific person sat at the keyboard and committed some heinous act.
3. **Report only verifiable information.** Even if the analyst knows who owns the suspect equipment, it is a quantum leap to say that person was using it at the time of the crime.
4. **Let the investigator tie media analysis findings to the investigation.** Analysis may indicate or verify that the suspect *computer* connected to a certain IP address (for example). This doesn't necessarily mean it was connected to a specific person's computer.

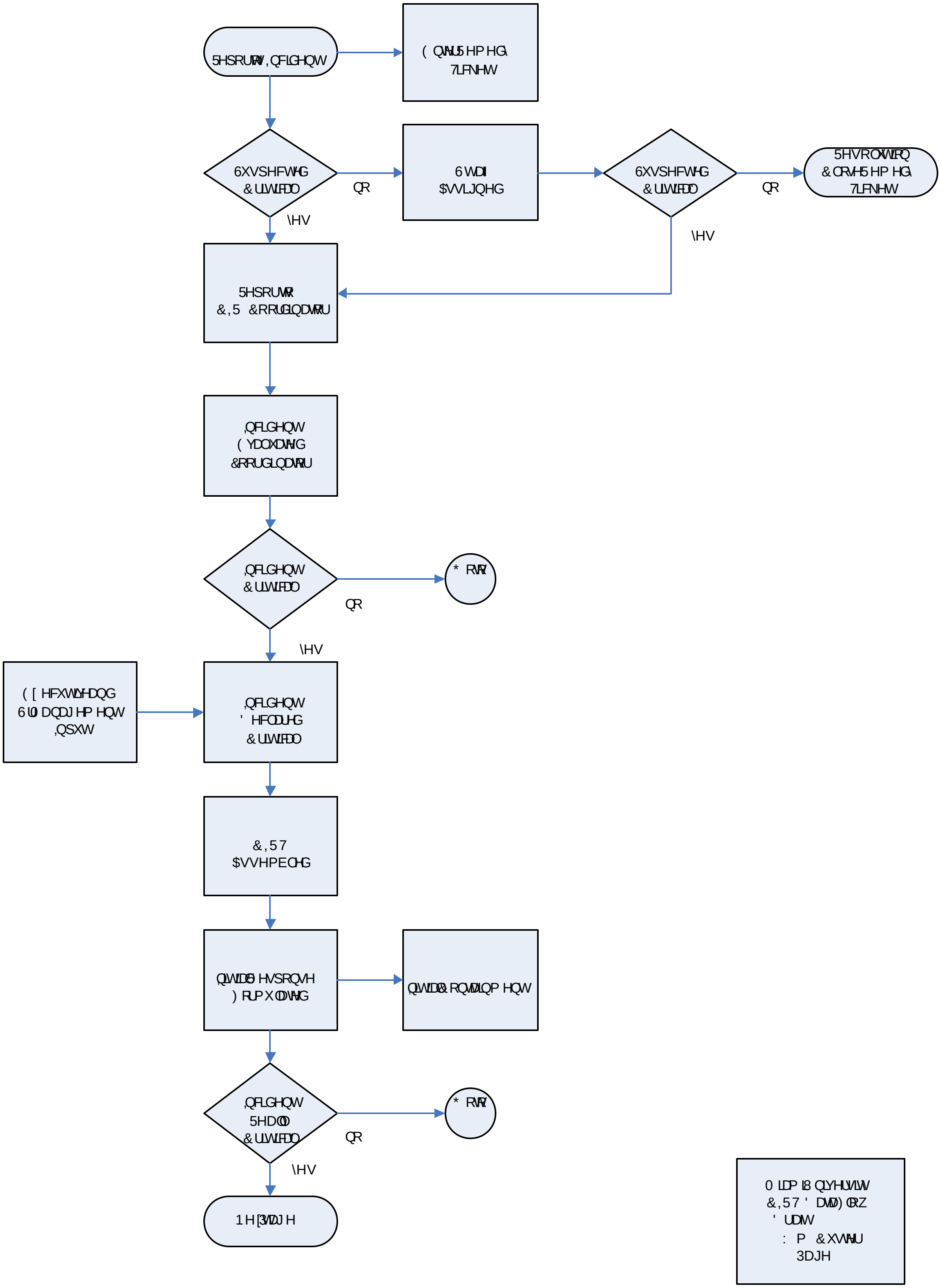
5. **Unless critical to the analysis, do not use names in the report.** Instead, refer to “subject,” “suspect,” or “victim.”
6. **Identify the evidence being analyzed as thoroughly as possible.** The analyst may have to identify the item again in a court of law. This is not the place to be unsure. Analysts should make their own unique mark on the evidence to aid in later identification.
7. **Write the report for the uneducated, not another analyst.** Explain uncommon terms – terms such as hash, clusters, tracks, sectors, etc. should all be explained the first time they are used. Explain processes – what/why is certain information recorded in a file.
8. **Be precise.** Statements such as “numerous,” “many,” “multiple hundreds,” etc. should be avoided. Specifically state the finding, as well as the precise locations of information.

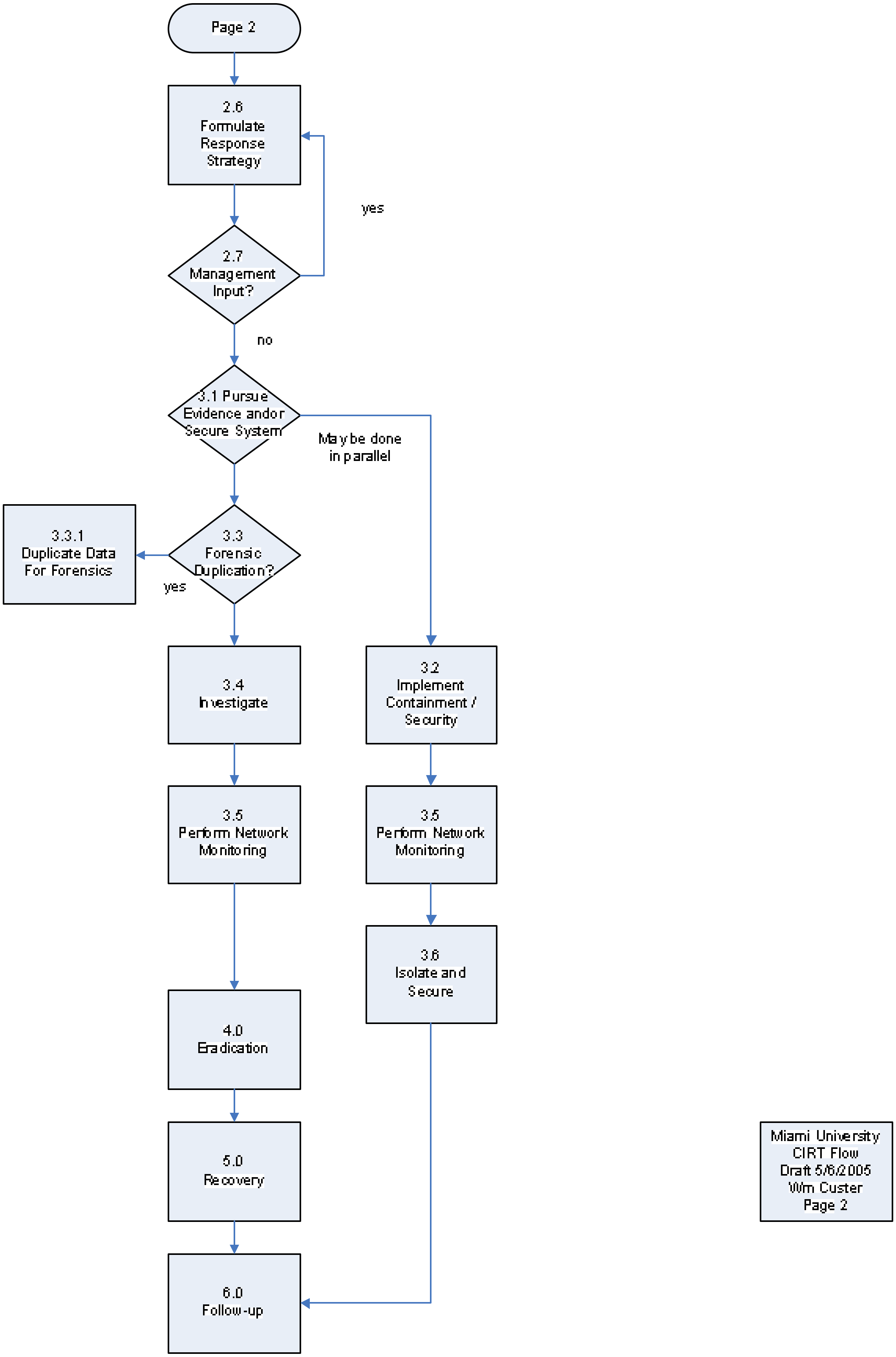
Reporting Findings

The complete evidence collection and subsequent analysis process should be memorialized and documented thoroughly. The format of this documentation report is as follows:

1. **Summary of Analysis.** A short, concise description (no more than about two pages) that summarizes the findings documented in the remainder of the report.
2. **Actions Taken.** A description of the circumstanced that prompted the CIRP activation, actions taken, and personnel involved
3. **Receipt of Evidence.** Documentation of when, where, and from whom the evidence was received (or taken).
4. **Physical Analysis.** A visual evaluation of the evidence that was examined. Complete documentation of the items to include brand name, model number, and serial numbers.
5. **Forensic Duplication.** Document exactly how the image was made (for digital evidence). Include the software and hardware used to make the image, and the hash comparison results.
6. **Analysis.** Document every step taken in the analysis of the media. Explain what tools were used and what was or was not discovered as a result of these processes. Document such information as number and size of sectors, operating systems, significant software, anti-virus and crash-guard software, etc.
7. **Evidence Disposition.** Document how and when the evidence was returned or the manner in which it was disposed.

Appendix G – Incident Flow Chart




Page 2
2.6 Formulate Response Strategy
yes
2.7 Management Input?
no
3.1 Pursue Evidence andor Secure System
May be done in parallel
3.3.1 Duplicate Data For Forensics
3.3 Forensic Duplication?
yes
3.4 Investigate
3.2 Implement Containment / Security
3.5 Perform Network Monitoring
3.5 Perform Network Monitoring
3.6 Isolate and Secure
4.0 Eradication
5.0 Recovery
6.0 Follow-up
Miami University CIRT Flow Draft 5/6/2005 Wm Custer Page 2