



Tulane University Computer Incident Response Plan

Part of Technology Services Disaster Recovery Plan

Version - 1.0
October 02, 2006

1. Purpose

The purpose of this Computer Incident Response Plan (CIRP) is to provide the University with a plan that addresses the dynamics of a computer security incident. A computer security 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 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 University Technology Services Hurricane and Disaster Recovery Plan to address information security and production computer/network continuity.

A computer security incident will be addressed as a University Disaster when the Chief Information Officer (CIO) communicates that a University Disaster has been declared. In the case of a University Disaster, all activities in this plan (The CIRP) will continue to be directed through the CIO.

2. Scope

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

Definitions and Acronyms

- CIRT – Computer Incident Response Team
- CIO – Chief Information Officer
- ISO – Information Security Officer
- PCAB – Presidential Cabinet
- TS – Technology Services

Policy for Techonogy Services

Computer security incidents will occur that require full participation of TS technical personnel as well as divisional leadership to properly manage the outcome. To accomplish this TS will establish computer 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.

3. Role and Responsibilities

Within this section, the roles and responsibilities for the CIO, CIRT, ISO, and Supporting Groups are defined. In addition, this section addresses the various Technology Services functional areas within the University and their CIRT responsibilities.

3.1 Chief Information Officer

The CIO 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 is responsible for executing or delegating the following:

- Setting priorities
- Notifying the University President and/or Board of Trustees of an incident declaration
- Disaster Declaration
- Participating with ISO in forensic investigation decisions
- Designating the Deputy CIO or an alternate to cover the responsibilities of the CIO role
- Notifying University Communications as appropriate for internal and external communication
- Owning of the ISO's incident work plan(s)
- Defining and issuing 'gag' orders within Technology Services for particularly sensitive issues; the default guideline for communicating about a computer security 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

3.2 Information Security Officer (ISO)

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

The ISO is responsible for the following:

- Managing incident resources
- Determining if an incident is at Critical Level and declaring it to be so
- Maintaining communications between CIRT and the CIO

Tulane University Computer Security Incident Response Plan

- Reminding staff that communication is on a need to know basis or if the CIO has defined a 'gag order' informing team members of the nature of the 'gag'
- Communicating to the Technology 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 and University General Counsel during forensic investigations
- Managing the incident work plan(s) and task assignments
- Raising dependency issues as they arise
- Designating a deputy ISO 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, if warranted, that the critical incident be upgraded to a disaster

3.3 Computer Incident Response Team (CIRT)

During an incident the ISO 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. This team will be responsible for both response and recovery.

Response Phase. 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 ISO on remedial action on affected systems
- The CIRT may be called up 24 hours a day, 7 days a week, 365 days a year during a critical incident

Recovery Phase. The response aspects of the team are centered around damage assessment, return to normal operations, rebuilding servers 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

Tulane University Computer Security Incident Response Plan

- Determining what data is lost and cannot be recovered or restored
- Reloading data on affected systems
- Restoring normal operations

Follow-up Phase:

- 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

3.4 Public Safety

- 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

3.5 General 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 and/or ISO regarding decision to simply protect its operations or to pursue civil or criminal actions
- Consults with the CIO and/or ISO regarding involvement with law enforcement
- Advises the CIO and/or ISO regarding involvement with regulatory agencies
- Reviews communications drafted by University Communications as required
- Liaison to external counsel

3.6 Human Resources

- Advises CIO 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

3.7 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

4. Incident Defined

An computer security **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.

Incident Levels

Critical Incident is defined as any unexpected or unauthorized change, disclosure or interruption to Tulane University's information resources that could be damaging to our students, staff, faculty, and/or reputation.

As part of the initial incident response process, the ISO 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 Tulane University, and/or their students, faculty, and/or staff. An critical 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 Tulane University, only incidents whose severity level is **high** are managed; however, other severity levels are outlined below for completeness.

High 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.

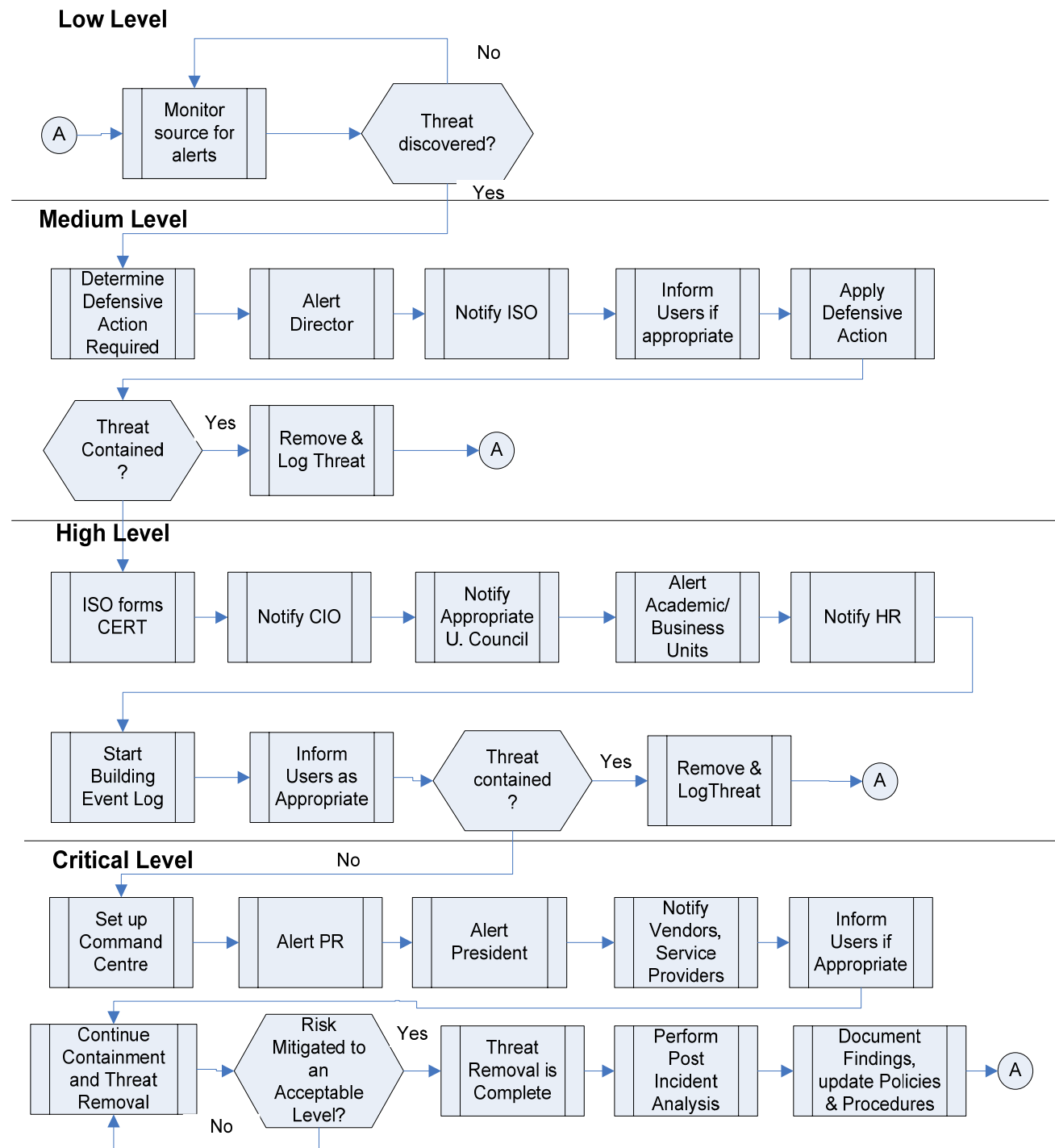
Medium Level: Penetration or denial-of-service attack(s) detected with limited impact on operations. Minimally successful, easy to control or counteract, small number of systems compromised, little or no loss of confidential data, no loss of mission-critical systems or applications. Widespread instances of a new computer virus or worm that cannot be handled

Tulane University Computer Security Incident Response Plan

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.

4 Incident Response flowchart



6. Roles and Responsibilities

The roles and responsibilities of each of the teams involved in incident response vary with the particular escalation level which is active at any particular point in time. These roles & responsibilities are described below. A summary of these is shown in tabular format in Appendix A of the document.

6.1 Low Level Incident

Normal system operations coupled with periodic and real time monitoring of the university's information assets.

System/Network Administrator

1. Monitor all known sources for alerts or notification of a threat.

6.2 Medium Level Incident

Early indications of a possible attack or intrusion have been detected by the monitoring processes.

System/Network Administrator

1. Analyze monitoring data and determine early defensive action.
2. Notify the local IT Director
3. If users are affected, communication message via Director of User Services.

Director / Manager

1. Receive and track reported incident event information from System/Network Administrator.
2. Escalate incident response to the next level if event information points to a genuine threat.
3. Alert relevant business unit, ISO of the threat (as appropriate).
4. If users are affected, communication message via Director of User Services.

6.3 High Level Incident

A threat has manifested itself.

System/Network Administrator

1. Identify countermeasures for containment of the incident.
2. Provide on-going threat status to Director.

Director

1. Notify Dean if appropriate

Tulane University Computer Security Incident Response Plan

2. Notify CIRT of the manifestation of the threat.
3. Report incident details and supporting system logs, audit records, etc. to CIRT.
4. Start logging of events for possible disciplinary / legal proceedings.
5. If users are affected, communication message via Director of User Services.
6. Report continuously to relevant business/academic units.

CIRT

1. Assume responsibility for directing the incident handling activities.
2. Convene Incident Support Team .
3. Determine whether further escalation to the CIO.
4. Determine if countermeasures have reduced the risks to an acceptable level.
5. Receive technical information from Incident Support Team.

Incident Support Team

1. Take actions identified by CIRT
2. Provide feedback to CIRT.

6.4 Critical Level Incident

The threat has become wide spread or is of high severity level.

System/Network Administrator

1. Support the Incident Support Team.
2. Continue reporting status of Director
3. Continue to monitor all event sources for alerts and notification of threats
4. Monitor effectiveness of the countermeasures in reducing the threats

Director

1. Continue monitoring the incident
2. Report continuously to the Dean or executive management

CIRT

1. Set up command center
2. Alert vendors/suppliers/external service providers (as appropriate)
3. Determine if the countermeasures have reduced the risks to an acceptable level.

Incident Support Team

1. Take actions identified by CIRT
2. Provide feedback to ISO & IT Director

CIO

1. Continue to monitor the event and report to the President or Presidential Cabinet if appropriate.

6.5 Post Incident

The threat has been removed. Full recovery is made. Normal operations have commenced.

CIRT

1. For category 2 and 3 incidents, prepare incident report to be reviewed by CIO, ISO and others as appropriate. The report should include:
 - Incident log including findings of Technical work that can be used as evidence.
 - Estimate of damage / impact
 - Details of action taken during the incident
 - Follow on efforts needed to eliminate or mitigate the vulnerability
 - List of policies or procedures that require updating
 - Details of efforts taken to minimize liabilities or negative exposure
 - Recommendations for legal/disciplinary action against intruders.
2. Document lessons learn and take corrective action to prevent recurrence.

HR and Legal

1. As directed by executive management, initiate disciplinary action or legal proceedings against internal / external threat source.

6.6 Incident Review Report Template

Preparation

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

Identification/Detection

1. How soon after the incident started did the organization detect it?
2. Could different or better logging have enabled the organization to detect the incident sooner?
3. Does the organization even know exactly when the incident started?
4. How smooth was the process of invoking the incident response plan?
5. Were appropriate individuals outside of the incident response team notified?
6. How well did the organization follow the plan?
7. Were the appropriate people available when the response team was called?
8. Should there have been communication to inside and outside parties at this time; and if so, was it done?

Tulane University Computer Security Incident Response Plan

9. Did all communication flow from the appropriate source?

Containment

1. How well was the incident contained?
2. Did the available staff have sufficient skills to do an effective job of containment?
3. If there were decisions on whether to disrupt service to internal or external customers, were they made by the appropriate people?
4. Are there changes that could be made to the environment that would have made containment easier or faster?
5. Did technical staff document all of their activities?

Removal and Recovery

1. Was the recovery complete — was any data permanently lost?
2. If the recovery involved multiple servers, users, networks, etc., how were decisions made on the relative priorities, and did the decision process follow the incident response plan?
3. Were the technical processes used during these phases smooth?
4. Was staff available with the necessary background and skills?

Appendix A – Computer Security Event Category Chart

This chart describes the 4 types of Security Event Category / business impact and identifies the actions that must take place for handling the incident. For details of the roles and responsibilities for performing these actions, please refer to Incident Response Team Roles & Responsibilities table in Appendix B.

Incident Level	Description	Example Incidents	Action
Low	These are not classified as attacks and have no effect on the system operations	<ul style="list-style-type: none"> - Isolated reconnaissance activities by potential attackers - Password policy violation by an employee - Detection and removal of viruses by a server before it enters the university's network. 	Alert Director
Medium	Attempted intrusions. No impact on business activities. Small impact on operations	<ul style="list-style-type: none"> - Repeated reconnaissance activity from the same source. - Attack blocked by the university's security infrastructure. - Regular occurrences of Category 0 incidents. - Successive attempts to gain unauthorized access to a system. 	Take Defensive Action Inform Users (if appropriate) Alert ISO Escalate to level 2 if appropriate.
High	Successful breaches of university's IT security policies	<ul style="list-style-type: none"> - Unauthorised access to sensitive systems (HR, Payroll, Finance, etc.) - Financial frauds using the university's computer. - Improper use of high level accounts such as root, administrator, etc. - Defacement of Tulane web site. - Denial of service attacks against Web server, mail server. - Unauthorised modification of hardware, software, configuration information. - Theft of computer systems containing sensitive information. 	Notify CIRT, CIO Inform Users (if appropriate) Start event log Form an Incident Support Team.

Incident Level	Description	Example Incidents	Action
Critical	Major attack against the university's IT infrastructure. Impact on the university's ability to meet its mission objectives Major impact on operational activities.	<ul style="list-style-type: none"> - Wide spread attacks such as Slammer worm attack in February 2003 against Microsoft SQL Server 2000 (which brought down Bank of New York's 13,000 ATMs for 8 hours). - Unauthorised changes to key components such as the main network switch. 	Notify and continually update President Inform Users (If appropriate)
Business Driven	These incidents can cause financial / reputation damage to the university	<ul style="list-style-type: none"> - Unusual transactions such as those exceeding pre-defined limits - Fraudulent transactions detected by business units - Unusual system activities reported by staff 	Alert Director Notify Legal & HRM Notify relevant Business/Academic Units

Appendix B – Incident Response Team Roles & Responsibilities

Indicent Level	Team	Responsibilities
Low	System/Network Admins	<ul style="list-style-type: none"> - Real time and periodic monitoring of all information assets for alerts and notification of threats.
Medium	System/Network Admin	<ul style="list-style-type: none"> - Determine initial defensive action - Notify Director - If immediate corrective action identified and required for users, communicate details to Help Desk
Medium	Director	<ul style="list-style-type: none"> - Receive and track incident data - Analyze incident data and escalate to Level 2 if appropriate - Notify ISO of the threat if appropriate - Include incident in the normal period reports of CIO if appropriate.
Medium	Director	<ul style="list-style-type: none"> - Notify CIRT to respond to the manifestation of the threat - Receive technical information from System/Network Admins - Forward incident details and supporting system logs, audit records, etc. to CIRT - Start logging of events for possible disciplinary / legal proceedings - If employees are affected, communicate message via Help Desk - Include incident in the normal period report to CIO and ISO.
Medium	System/Network Admins	<ul style="list-style-type: none"> - Identify countermeasures for containment of the incident - Provide feedback to IT Director - Support CIRT
Medium	CIRT	<ul style="list-style-type: none"> - Convene Incident Support Team - Assume responsibility for directing the incident handling activities - Determine whether further escalation to the next level is appropriate - Determine if the countermeasures have reduced the risks to an acceptable level
High	Incident Support Team	<ul style="list-style-type: none"> - Take actions identified by System/Network Admin countermeasures - Inform Director, CIRT, of the details of the action taken
Critical	CIO	<ul style="list-style-type: none"> - Continue monitoring the incident and communicate with the President

Critical	CIRT	<ul style="list-style-type: none"> - Set up command centre - Notify vendors / external service providers as appropriate - Determine if the countermeasures have reduced the risks to an acceptable level
Critical	Director	<ul style="list-style-type: none"> - Continue monitoring the incident - Report continuously to executive management - Communicate with Dean if appropriate - Include incident in the normal period reports to CIO and ISO
Critical	System/Network Admins	<ul style="list-style-type: none"> - Support CIRT - Continue countermeasure actions - Continue reporting status to IT Director - Continue to monitor all event sources for alerts and notification of threats - Monitor effectiveness of the countermeasure in reducing the threats
Post Incident	CIRT	<ul style="list-style-type: none"> - For category 2 and 3 incidents, prepare incident report to be reviewed by ISO, CIO and Dean as appropriate. The report should include: <ul style="list-style-type: none"> - Incident log including findings of Technical work that can be used as evidence. - Estimate of damage / impact - Details of action taken during the incident - Follow on efforts needed to eliminate or mitigate the vulnerability - List of policies or procedures that require updating - Details of efforts taken to minimize liabilities or negative exposure - Recommendations for legal/disciplinary action against intruders. - Document lessons learnt and take corrective action to prevent recurrence.

CIRT Core Team

1. Adams Krob
2. Tim Devees
3. Leo Tran

Director of User Services
Director of Network Services
ISO