
**Information Security Office**

# Proecdure III-3b
# Information Security Incident Response Procedure
# (version 2, Dec 2009)

# I. The Information Security Incident Response Plan

The purpose of the Information Security Incident Response Plan is to establish procedures in accordance with applicable legal and regulatory requirements and University policy to address instances of unauthorized access to or disclosure of University Information, to be known as a Security Incident.

In addition to all the defenses that have been implemented to protect the infrastructure and the information processed within, the information security office will maintain a high level of preparedness for any security incident. This Plan describes the response to such events, the conditions whereby this process is invoked, the resources required, and the course of recommended action. Central to this process are two response teams, Technical Response and Management Response, which are assembled with the purpose of addressing that particular circumstance where there is credible evidence of an incident. See "Process Flow – Appendix A" for a graphical representation of the information flow and decision process. One additional team, First Responders, augments the Technical Response team as needed.

**The primary goals of activities described within this Plan are, in order of precedence:**

1. **Minimize adverse impact to university IT infrastructure.**
2. **Capture and preserve relevant incident data with the aim of causal analysis supporting corrective actions.**
3. **Return to a normalized (secure) state as quickly as possible.**
4. **Ensure incident handling and response is optimized and effective.**
5. **Perform selected incident post-mortems to critically evaluate flaws in infrastructure, architecture, and IT processes (protect, detect, defend, sustain)**
6. **It is understood and accepted that strict forensic measures are not used in the data capture and retention.**

The scope of this plan applies to incidents involving computer and network resources at Case Western Reserve University, as well as information considered to be under the stewardship of the University. The plan also covers associated University Circle institutions that have an established partnership with the University, as evidenced by network connections between Case and these organizations.

This document may reference other documentation, policies and procedures that support this Plan but are not contained within the document, e.g., information categories, quarantine procedures, Case Help Desk and Network Operations procedures, University Emergency Response procedures. Where this occurs, instructions to obtain these materials will be specified.

Circumstances may dictate the activation of other operational teams and execution of other Plans. The Management Response Team must monitor and coordinate all activities occurring under other operational teams and Plans, and communicate to all interested parties in a timely manner to ensure accurate assessments and avoid efforts that may be duplicated or at cross-purposes.

# II. Definitions

### A. Information Security Events and Incidents

All circumstances that require some level of attention by the Information Security Office are categorized as Events. Case has implemented an approach that uses two levels of exigency, events and incidents.

An **Information Security Event** is a known condition or sequence of reports and indicators that is a suspected incident. Most incidents are initially categorized as an event. Not all events will be resolved into an incident.
Examples of an Information Security Event may include but are not limited to:

- A host or server compromise resulting in root or Administrative access, where public information is hosted.
- Continuous network scanning or probing.
- User violation of the University Acceptable Use Policy (e.g. Copyright infringement notification).
- Infringement of network policy
- eDiscovery Support activities for University Counsel

An **Information Security Incident** is generally defined as any known event (or group of events) that results in a network outage (either by the event or by resultant triage activities required), actual or possible unauthorized release of information deemed sensitive by the University or subject to regulation or legislation, or unauthorized intrusions to the University's networked systems.
Examples of an Information Security Incident may include but are not limited to:

- A network based attack perpetrated by either a Case user or external person, which is detected by Case staff.
- Unauthorized disclosure of sensitive information that the University has stewardship to protect, such as student, staff, faculty, or customer data. This includes theft or physical loss of equipment known to hold sensitive information.
- Destruction or unauthorized modification of data on University systems.
- Sensitive university managed data appears to have been obtained without authority or authorization.
- A network outage or system outage caused by unauthorized physical access to a data centers or cable plant.
- An incidence of social engineering which results in disclosure of sensitive information.
- A report of legal or administrative action that requires gathering of computerized evidence.

- Automated attack/network infection (worm, virus, etc) that is considered a "major" attack, the threshold is if more than 10% of University users are denied access to ITS services.
- A critical application failure deemed or suspected to be the result of malicious human activity.
- A host or server compromise resulting in root or Administrative access where Restricted Information is present, or a critical service is affected.
- A defacement of a Case website.
- Any sequence of events that are correlated into a distinct incident, as determined by the Technical Response Coordinator.
- Any computer related security event that involves the senior management at the University, including the President, Provost, VP level Executives, and Deans of the various Colleges.
- Criminal activity that warrants formal response in support of University Police.

Incident Priorities
Incidents are always high priority.
Events are moderate to low priority.

Note that due to the high risk tolerance of the environment, many classically defined issues are considered events within this plan, and elevated to a security incident status when the impact crosses the defined thresholds.

Incident Categories
For the purposes of this Plan, incidents are grouped by common impact[1]:

A. Denial of Service: a deliberate attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. These may result in interruption of service network outage with enterprise impact (key business systems interruption).
B. Malicious code: a "bot," virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
C. Theft or Loss of physical IT assets.
D. Unauthorized access: a person gains logical or physical access without permission to a network, system, application, data, or other resource.
E. Inappropriate usage: a person violates the university Acceptable Use Policy.
F. Disclosure of Restricted Information (Restricted information) that requires notification:
    - Patient information or Personally Identifiable Information (PII)
    - SSN, DoB, Names or other academic PII

[1] Grance, Kent and Kim. Special Publication 800-61: Computer Security Incident Handling Guide. US National Institute of Standards and Technology, 2003: p3-5. <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

### B. Information Security Incident Response Teams

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

### C. University Information Architecture

The term "University Information" refers any information maintained by or on behalf of the University that is used in the conduct of University business regardless of the manner in which such information is maintained or transmitted. University Information formats include, but are not limited to oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or any other medium. The University has a 3-level information architecture. Each level of information requires equivalent control sets of increasing capability.

| Information Type | Control Set |
|---|---|
| 1. Public | Tier I Controls (baseline security controls) |
| 2. Internal Use Only | Tier II Controls |
| 3. Restricted | Tier III Controls |

### D. Sensitive Data

Sensitive Data is a generic term for any University Information declared to be Internal Use Only, or Restricted by University policy (the use of 'confidential' as a label for information is common, but not within the definition of the architecture). Restricted information includes any personally identifiable information (PII) as determined or governed by law or regulation or University policy requiring protection from disclosure.

Examples include but are not limited to:

- NetworkID and Password
- Name in combination with SSN
- Credit or Debit Card Number and Access Code (e.g., PIN or Password)
- Personal medical records, also called Personal Health Information (PHI)
- Unpublished results of research or financial investment strategies
- Proprietary data (e.g., protected formulas or patents)

### E. University Client (Client)

A University Client (Client) is:

- any faculty, student, staff or alumni affiliated with the University, or
- any department or school of the University, or
- any employee (permanent, temporary and contract personnel)
- any affiliated person (e.g. University Circle affiliated institutions)

### F. 3rd Party

A 3rd party is:

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

# III. Information Security Incident Response Team (IRT)

### A. Incident Response Team Composition

The core IRT consists of the Technical Response Team and the Management Response Team. The First Responders Team is activated as deemed necessary by the Incident Response Coordinator. Each member of the Technical Response Team will designate an alternate member to participate if the primary Member is unavailable. See "Response Team Contact List - Appendix B" for a listing of individual members.

#### A1. Technical Response Team (Required)

This team is a group of IT technicians and managers who will be tasked with the execution of plans that will detect events, triage events, and respond to events for IT systems and workflow within their scope of responsibility. This team will document checklists and procedures. This team serves to triage an event or incident on a technical level with peers within the university and with other universities as necessary. Team membership includes

1. Manager of Networking and Security- Team Lead
2. Information Assurance Analyst- Team Lead
3. Network Security Engineering Staff
4. Information Assurance Analysts
5. Chief Information Security Officer (advisory role)
6. Managers of affected IT areas and systems, as applicable
7. Technicians from affected IT areas
8. Additional resources as needed, such as First Responders, and contracted forensics analysts
9. Information Security Coordinators representing an affected Client or 3rd Party, or known to have an established relationship with an affected Client or 3rd Party, may be requested to serve on the Secondary Team.

#### A2. First Responders Team (as needed)

This is a team of field IT staff, typically IT administrators from various departments involved in a particular incident, including select Help Desk/Customer Care staff and Central ITS organization administrators, who are trained and employed in a "volunteer fire department" model in the event of an enterprise-wide incident.

Team membership includes:

1. Technical staff from non-ITS departments
2. Pre-selected ITS Customer Service and Support staff (addressing areas with no organic IT staff)
3. Individuals identified as subject matter experts or having skills required for resolution of the incident.

### A3. Management Response Team (Required)

This team is a group of senior leaders at the university who are engaged to make decisions in response for information security incidents that require executive approval. This team will always be convened when the incident response triggers regulatory or compliance response and for incidents that warrant public notification.

Team membership includes:

1. Chief Information Security Officer (CISO)
2. Chief Information Officer (CIO)
3. Chief Financial Officer
4. Deputy Chief Information Officer for Operations
5. Deputy Chief Information Officer for Administration (as needed)
6. University Counsel representative
7. University Marketing and Communications representative
8. ITS Communications Director
9. University President's Chief of Staff
10. Additional resources (as needed)
    a. Deans of affected colleges or professional schools
    b. VP of affected department
    c. VP of Campus Services (for larger incident response needs)
    d. Internal Audit representative
    e. AVP, Office of Human Resources
    f. Chief Administrative Officer
    g. Case Police Department representative

## B. Team Objectives

### B1. Technical Response Team

Led by the Incident Response Coordinator, the Technical Response Team's objective is to:

1. Investigate events, assign tracking numbers to events. Determine details, scope of event, perform general analysis.
2. When events meet incident criteria, declare an incident and initiate response plan.
3. Coordinate and oversee the response to Incidents in accordance with the requirements of state and federal laws and University policy;
4. Perform containment activities to minimize the potential negative impact to the University, Client and 3rd Party as a result of such Incidents; Quarantine machines

as needed, determine required clean up activities before a host/system can be returned to service.
5. Manage communications between and within response teams.
6. Communicate factual decision making information to the Management Response Team where triage activities may require outages that will affect University IT operations.
7. Determine if legal action may be needed, to ensure proper collection of evidence, as necessary.
8. Notify affected administrators within the appropriate domain
9. Restore services to a normalized and secure state of operation.
10. Conduct root cause analysis and recommend possible defenses to manage future risk.

### B2. First Responders Team

The First Responders Team is led by the Incident Response Coordinator to
1. Detect, report, and investigate events
2. Gather data from impacted systems outside of the Central ITS group
3. Take appropriate clean-up actions to manage outbreaks and in areas within their scope of responsibility.

### B3. Management Response Team

Led by the University's Chief Information Security Officer, the Management Response Team's objective is to:
1. Coordinate and oversee the management-level response to Incidents in accordance with the requirements of state and federal laws and University policy;
2. Notify the University President and Provost within 24-hours of any incident deemed to harbor potential negative impact to University operations or reputation. Typically this is for incidents that require notification of constituents for data breaches.
3. Ensure appropriate senior leadership is informed of activities impacting their operational areas. Make decisions about IT systems outages as needed.
4. Manage external communications related to a security incident. Respond to inquiries from affected 3rd parties. Receive feedback from constituents.
5. Provide resources, when needed, to permit the Technical Team to restore services to a normalized and secure state of operation.

## C. Responsibilities of Incident Response Coordinator

To ensure an appropriate and timely execution of this Plan, the Incident Response Coordinator (typically from Network Engineering and Security Group or the Information Security Office) shall:
1. Confirm the occurrence of an event which has been escalated to an incident requiring the execution of this Plan. Confirmation activities include but are not limited to:
   - direct conversation with Client, 3rd Party, HelpDesk, NOC personnel, "on call" engineer, First Responder members or others having information about the event
   - review of system logs or audit records

- examination or analysis of anomalies or untoward events
- collection of any evidence supportive of the event

2. Supervise and direct the consistent, timely, and appropriate response to an incident.
3. Provide appropriate communication to parties having a vested interest in the incident.
4. Offer support to the Client or 3rd Party as appropriate until the incident is resolved.
5. Conduct an incident post-mortem.
6. Maintain the procedures contained in this document.

Responsibility for overall Incident Response is the domain of the CISO. The CISO shall:

1. Ensure management response is initiated within established timelines.
2. Coordinate and communicate with senior management (VPs, Deans, etc.)
3. Ensure the University President and Provost are both appropriately informed of events and actions.
4. Provide Incident post-mortem reports to senior management.
5. Recommend risk management strategies and practices to minimize risk based on incident lessons learned.

### D. Reporting a Security Incident

Anyone with knowledge or a reasonable suspicion of an incident is instructed to make an immediate report to any of the following:

- The Case Help Desk (216-368-HELP (4357)
- The e-mail addresses of **security@case.edu** or **abuse@case.edu**

Note: These e-mail addresses may be used but are less effective than the direct notification of the Help Desk via voice communication or voicemail.

HelpDesk personnel use scripts (e.g., lists of predetermined questions) to assist in problem determination and resolution. These scripts assist support personnel to identify those events that may be classified as an Information Security Incident. Additional information may be found in “Guidelines for HelpDesk– Appendix H”.

**Anyone receiving notification of an Incident must contact the Help Desk immediately. Help Desk personnel will contact the on call Incident Response Coordinator**

### F. Event and Incident Tracking

Events are and incidents are given tracking numbers according to this format.

2008-06-020

| Type | Year | Month | Increment |
|---|---|---|---|
| Event | YYYY | Abbreviation | NNN |
| *Event example* | 2008 | JUN | 020 |
| Incident | YYYY | MM | NNN |
| *Incident Example* | 2008 | 06 | 020 |

The first field indicates the calendar year when the incident was initiated. Any crossover of calendar year is based on the initiating date. The second field is either the three-letter abbreviation for the month (e.g. JUN) or a two-digit month number field (01-12) for events and incidents, respectively. The last field is a 3-digit integer, which increments for each event or incident, and resets each calendar year.

For an example case, an event that is tracked as 2008-JUN-020 was later determined to be an incident. The tracking number was then changed to 2008-06-020.

All correspondence and reporting reference the tracking number. For email communications, the subject line is to contain the tracking number.

# IV. Key Components of Response Plan

The Incident Response Plan consists of five key components: Detection, Notification/Communication, Response, Corrective Measures, and Closure.

### A. Detection

Various groups perform monitoring activities across campus. Systems logs and monitors are key triggering mechanisms to determine events of interest. Examples of event detections include:

- System outage report
- Firewall log review
- Vulnerability analysis report
- Audit findings
- Help Desk calls

The Incident Response Coordinator will determine the event category and severity of the Event, elevating it to Incident status, and undertake discussions and activities to best determine the next best course of action, i.e., decide if Plan execution is required. The “Assessment Checklist - Appendix E” is used in the initial assessment process conducted by the Incident Response Coordinator. Once the Technical Response Team is assembled via phone bridge, the Assessment Checklist is executed and reviewed to ensure all pertinent facts are established. All discussions, decisions and activities are to be documented.

### B. Notification/Communication

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

#### B1. Internal Team Notification (within the University)

All urgent notifications are using emergency communications protocols.

1. The Incident Response Coordinator contact the Case Police Dispatch at 216-368-3333.

2. Police Dispatch is asked to send the CaseWARN alert to the **ITS Technical Response** callout list. Additional callout lists for the management and first-responders teams are available, and uses similarly.
3. Team members receive SMS and automated calls to their cell phones to dial the conference bridge (See Appendix B).
4. Initial conversations will confirm results, define actions.
5. Follow-up calls are scheduled at the conclusion of the call. This may include subsequent face to face meetings.

For non-urgent notifications, a mass email to security@case.edu using GPG encryption is deemed sufficient. All Technical response team members will be proficient in GPG encrypted communications via email.

### B2. Management Team Notification

Management Response is seldom urgent, and thus this team is often scheduled for a teleconference during normal working hours or a regular meeting timeframe. In some instances, telephone calls to senior executives are made to ensure notification has been made.

#### B.2.1(Inside the University)

All urgent notifications are using emergency communications protocols.

1. The Incident Response Coordinator contact the Case Police Dispatch at 216-368-3333.
2. Police Dispatch is asked to send the CaseWARN alert to **the ITS Management Response** callout list. Additional callout lists for the management and first-responders teams are available, and uses similarly.
3. Management Team members receive SMS and automated calls to their cell phones to dial the conference bridge (See Appendix B)
4. Initial conversations will confirm results, define actions.
5. Follow-up calls are scheduled at the conclusion of the call. This may include subsequent face to face meetings.

For non-urgent notifications, a teleconference is scheduled during working hours. The CISO will present content in the University's Adobe Connect conferencing system (https://connect.case.edu/response). Management response team members are authenticated for access using their Network ID and password.

#### B.2.2. (Outside the University)

1. 3rd Party – CISO (or designated representative) and the Office of General Counsel will establish communication with any 3rd Party, as appropriate for the circumstance.
2. Law Enforcement – CISO will contact University Police to notify local, state, and/or federal law enforcement agencies as appropriate.
3. Regulators - Office of General Counsel notifies the appropriate regulatory agencies.
4. Management Response members will assist in determining if other parties should be notified (e.g. partner institutions, other universities).
5. News outlets –University Marketing and Communications will determine if, how and when news outlets should be notified, and respond to all inquiries from news outlets.
6. School and Research administration determine if government notification (e.g., DOD, FDA) is required and take appropriate action.
7. Other affected parties – The Management Response Team will determine if there are other parties of interest, with communications issued accordingly.

### B3. Client or Constituent Notification

All External Notification and communication must be approved by the Office of General Counsel and provided by University Marketing and Communications.

1. Client should be informed that the Incident has been reported, recorded and an investigation underway. Whenever possible, email communications will be used as a primary means of notification, followed by hard-copy mail as needed.
2. Client shall be kept abreast of the status of the Incident investigation in a timely manner.
3. Client shall be notified of results, closure of investigation, and recommendations.

### B4. Status

1. Incident Response Coordinator and CISO assume responsibility for preparing and issuing timely communication to IRT members, Administration and other interested parties.
2. Communications may include meetings, video conferencing, teleconferencing, e-mail, telephone/messaging, voice recordings or other means as deemed appropriate.
3. Frequency and timeliness of communications will be established and revised throughout the life of the incident.

## C. Response

The Technical Response Team will determine and cause to be executed the appropriate activities and processes required to quickly contain and minimize the immediate impact to the University, Client and 3rd Party. Recommended activities addressing Unauthorized Access and Unauthorized Acquisition are described in “Incident Containment Activities - Appendix F”.

Containment activities are designed with the primary objectives of:

1. Counteract the immediate threat
2. Prevent propagation or expansion of the incident
3. Minimize actual and potential damage
4. Restrict knowledge of the incident to authorized personnel
5. Preserve information relevant to the incident

### D. Corrective Measures

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

Corrective measures are designed with the primary objectives of:

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

### E. Closure

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

## V. Required Documentation of Incident & IRT Meetings

All Incident activities, from receipt of the initial report through Post-Incident Review, are to be documented. The IRT Lead is responsible for ensuring all events are recorded, assembling these records in preparation and performance of the post-incident review, and ensuring all records are preserved for review. IRT members may be employed in these efforts.

1. General overview of the Incident
   Summary of the Incident providing a general description of events, approximate timelines, parties involved, resolution of the incident, external notifications required, and recommendations for prevention and remediation.

2. Detailed review of the Incident.
   Description of Incident events, indicating specific timelines, personnel involved, hours spent on various activities, impact to Client, 3rd Party and user communities (e.g., system not available, business continuity issues), ensuing discussions, decisions and assignments made, problems encountered, successful and unsuccessful activities, notifications required or recommended, steps taken for containment and remediation, recommendations for prevention and remediation

(short-term and long-term), identification of policy and procedure gaps, results of post-incident review.

3. Retention
   All relevant documentation will be retained by IRT Lead for archival in a central repository. Access to the documentation and repository is typically restricted to IRT membership and University Administration. Incident documentation will be retained for 3 years, or as required by University Counsel.

## VI. Incident Post Mortem

A review of incident-related activities is a required element of this Plan. All members of the Technical and Management teams are recommended participants. The objective of the post-mortem is to improve the incident response process.

1. Discussion
   The Incident Response Coordinator will host a Post-Mortem after each Incident has been resolved; this discussion should be scheduled within 3-4 weeks of the Incident's remediation. The review is an examination of the Incident and all related activities and events. All activities performed relevant to the Incident should be reviewed with an eye towards improving the over-all incident response process.
2. Questions to resolve:
   a. Was there sufficient preparation for the incident?
   b. What preparation wasn't done that should have been done?
   c. Did detection occur promptly or if not, why?
   d. What additional tools and techniques could have helped the detection and eradication process?
   e. Was the incident sufficiently contained?
   f. What practical difficulties were encountered?
   g. Was communication adequate? What could have made it better?
3. Analysis
   a. Analyze the cost of the incident. Gather effort expended in hours (round to the nearest half hour) by FTE.
   b. Convert hours to monetary costs at $100/hr
   c. Summarize how much operational disruption occurred
   d. Were any data irrecoverably lost? What was the data value?
   e. Was any hardware damaged/lost, and at what cost?

4. Recommendations
   The Technical Response Team's recommendations on changes to policy, process, safeguards, etc. are both an input to and by-product of this review. "Fix the problem, not the blame" is the focus of this activity. All discussion, recommendations and assignments are to be documented for distribution to the IT Management and Administration, and follow-up by Incident Response Coordinator.

5. Follow-up
   The Incident Response Coordinator will follow-up with the Client and 3rd Party or other parties, as required and appropriate.

# VII. Appendices

A – Process Flow

B – Primary and Alternate Contact List

C – Notification Tree

D – Incident Severity

E – Incident Assessment Checklist

F – Incident Containment Activities

G – Corrective Measures

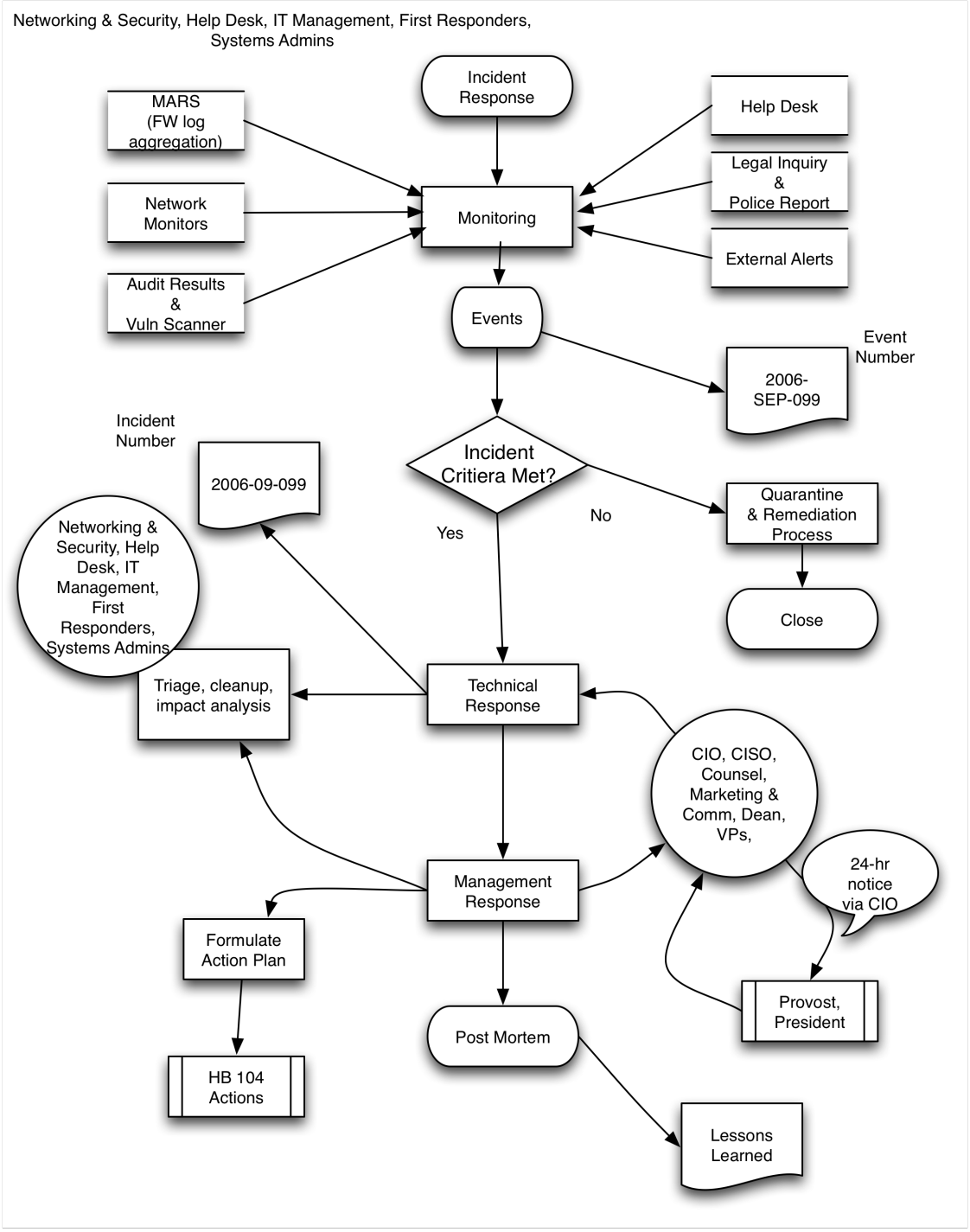
H – Guidelines for Help Desk and NOC Personnel

I – Data breach notification template

J – Briefing note template for public communications of security incidents

# Information Security Incident Response Plan

## Process Flow Appendix A



# Information Security Incident Response Plan

## Incident Response Team Contact List Appendix B

| Technical Response Team | | |
|---|---|---|
| **Department or Function** | **Primary Contact, Role** | **Alternate Contact** |
| Network Engineering and Security Group (NESG) | Chet Ramey, Incident Response Coordinator | |
| Information Security Office | Ruth Cannon, Incident Response Coordinator | David Carlin |
| Network Security | Lou Changeri, Firewall Engineer | Kevin Chan, Network Engineer |
| Chief Information Security Officer | Tom Siu, CISO | Chet Ramey |
| Telecom and Network Services | John Ozanich | Debra Andrews<br>David Weilacher |
| **First Responders Team** | | |
| School of Law | Keith Wane | |
| School of Medicine | Tom Ligman | |
| School of Dental Medicine | Tom Cotter | |
| Office of Student Affairs | Greg Patterson | |
| College of Arts & Sciences | Daniel Farst | |
| ITS Server Engineering | David Miller, Windows engineer | |
| ITS Server Engineering | Riley Wilson, Unix engineer | |
| Instructional Technology and Academic Computing | Mike Thomas, Classroom computing environments | |

# Information Security Incident Response Plan

| Management Response Team | | |
|---|---|---|
| IT Services | Tom Siu, CISO | |
| IT Services | Lev Gonick, CIO | TBD, Deputy CIO for Administration |
| IT Services | Mark Henderson, Deputy CIO for Operations | |
| University Counsel | Peter Poulos | Colleen Treml |
| University Marketing and Communications | Paula Baughn | Glenn Bieler |
| Internal Audit | Kevin Fechter, Deloitte | |
| Law Enforcement | Daniel Schemmel, Case Police | Michael Goliat, Case Police |
| | | |
| | | |
| | | |
| | | |

The Incident Response telephone conference Bridge numbers are:

1-866-921-2203
Bridge ID is *__8417666__*
Moderator code is *__6984__* (Incident Response Coordinator)

Additional Cisco MeetMe bridges:

754-3668 (Management)
754-3662 (Technical)

Email lists also have associated PGP Keys for encrypted communications.

security@case.edu
first-responders@case.edu

## Notification Tree Appendix C

The incident response notification tree is maintained online at the Case Google Apps web documents. This listing is maintained by the Case Help Desk. Contact Crystal Forbes (crystal.forbes@case.edu) for access.

The Information Assurance Analyst serving as the Incident Coordinator will keep a local copy of this notification tree in the event the online version is not accessible.

## Event to Incident Appendix D

| Severity | Symptoms |
|---|---|
| Event | A. Some adverse impact to the operation of the University.<br>B. Adverse effects are localized or contained, or minimal risk of propagation.<br>C. No apparent release or compromise of sensitive data.<br>A. Remedial action is required.<br>D. Notification of entities within the University is required. |
| Incident | A. Network or system outage with significant impact to the user population or operation of the University.<br>B. High probability of propagation.<br>C. Probable or actual release or compromise of sensitive (Restricted) data<br>D. Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities.<br>E. Notification of entities outside of the University is required by statute or policy. |

# Information Security Incident Response Plan

## Incident Assessment Checklist Appendix E

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

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

| |
|---|
| **A. Description of Incident -** Data relevant to the Incident should be collected for use in the process of Incident determination. |
| A1. Record the current date and time. Generate an Incident Tracking Number |
| A2. Provide a brief description of the Incident. What happened? |
| A3. Who discovered the Incident? Provide name and contact information. |
| A4. Indicate when the incident occurred and when it was discovered. |
| A5. How was the Incident discovered? |
| A6. Describe the evidence that substantiates or corroborates the Incident (e.g., eye-witness, time-stamped logs, screenshots, video footage, hardcopy, etc.). |
| A7. Identify all known parties with knowledge of the Incident as of current date and time. |
| A8. Have all parties with knowledge of the Incident been informed to treat information about the Incident as “Official Use Only”? |
| A9. Is the incident still ongoing or is it over? |
| **B. Types of Information, Systems and Media -** Provide information on the nature of the data that is relevant to the Incident. |
| B1. Provide details on the nature of the data (e.g., student information, research data, credit card information, SSNs, etc.).<br>- Interview the system owner and users to determine if system was used to store or process electronic Patient Health Information (ePHI), payroll, application, or academic data containing SSNs, or other Restricted Data. If so, follow Appendix E, Part B: Data Breach Response |

| |
|---|
| B2. Does the information (if compromised) constitute a violation of regulatory requirements (e.g., FERPA, HIPAA, PIP Act) or University policy? Describe what is known. |
| B3. Was the compromised information maintained by a University Client or a 3rd Party? Provide details. |
| B4. How was the information held? Identify the types of information systems and/or the media on which the information was stored (e.g., hardcopy, laptop, CD-Rom, etc.). |
| B5. If the information was held electronically, was the data encrypted or otherwise disguised or protected (e.g., redacted, partial strings, password required, etc.)? If so, describe measures taken. |
| B6. If a Client held the information:<br>- Establish the Client point of contact.<br>- Assign responsibility to IRT member to contact the Client. |
| B7. If a 3rd Party held the information:<br>- Identify the individual within the University who best represents the 3rd Party. If there is no suitable University contact, an IRT member will be assigned responsibility for directly contacting the 3rd Party.<br>- Assign responsibility to IRT member to contact that individual.<br>- IRT member will work with the University contact or 3rd Party to obtain a copy of any contract or confidentiality agreement and ascertain what knowledge of the Incident the 3rd Party might have and what action if any has been taken. |
| B8. Who currently holds evidence of the Incident? Provide name and contact information. |
| B9. What steps are required or being taken to preserve evidence of the Incident? Describe. |
| **C. Risk/Exposure -** Attempt to determine to what extent risk and/or exposure is presented by this Incident. |
| C1. Can we reasonably determine the risk or exposure? |
| C2. To what degree are we certain that the data has or has not been released? |
| C3. Do we have contact with someone who has “firsthand” knowledge of the circumstance (e.g., the owner of a stolen laptop)? Provide name and contact information. |

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

## Data Breach Response Appendix E, Part B

| |
|---|
| **A. If data is determined to be Restricted** |
| A2. Is the nature of the restricted data contained on a compromised or stolen machine ePHI (identified medical data)? |
| A3. Were the data stored on encrypted media? |
| A4. Correlate the identifying data with names and contact info for affected individuals |
| A4.1. Describe and divide the list of affected individuals by type: Students, Alumni, Faculty, Staff.<br>Request database lookups to provide notification addresses for the affected individuals from the following sources:<br>Students: Office of the Registrar, Heidi Wagner<br>Alumni: Alumni Services, Brian Rosen<br>Faculty & Staff: Human Resources, Shawn LeHue |
| A4.2. Transmit sensitive identity information in encrypted form such as a password-protected Acrobat Security Envelope (transmit the password out-of-band, such as via voicemail). |
| A5. Assess and describe Root Cause:<br>- Inadvertent public posting<br>- Theft or Loss of computer<br>- Unauthorized access to Restricted-data server (account sharing, negligent maintenance of Access Control Lists, privilege escalation through application flaw?)<br>- Successful targeted attack/compromise of Restricted-data server (unpatched server OS, weak passwords, vulnerable website components?) |
| A5.1 Communicate requirements for system hardening to System Owner; agree on procedure to prepare system for return-to-service |
| A5.2 Law Enforcement Involvement<br>If the security incident incurs greater than $5000 in damage, or loss of service, law enforcement assistance may be requested to investigate and prosecute perpetrators. This shall be conducted through the Case Police department. |
| **B. Identity Theft Protection Contract** |

| |
|---|
| B1. Provide Breach Notification and List of affected names to Zander Insurance<br>- Contact Diane Sacks: des@zanderins.com<br>- Window of availability for affected users to subscribe: ~2 months<br>- School or Department bear the cost |
| B2. Notification of Affected Individuals within 45 days of incident<br>- Alert the Helpdesk that individuals will be calling in to verify authenticity; instruct to contact CISO<br>- Point of contact: Crystal Forbes, crf50@case.edu |
| B2.1 Notification shall be by email where available |
| B2.2 Notification via conventional mail, on letterhead, where email is not available<br>- School or Department bear the cost |
| B2.3 If more than 1,500 individuals' PII data are exposed, the University must make a public announcement within 90 days<br>- University Office of Marketing and Communications notifies campus community by Case Daily and issues a Press Release |
| B2.4 If more than 500 individuals ePHI data are exposed, the University must<br>- make a public announcement (University Office of Marketing and Communications notifies campus community by Case Daily and issues a Press Release)<br>- Notify US Department of Health & Human Services<br>- Make an annual report to HHS of all ePHI breaches<br><br>(identity theft protection will not be considered for ePHI data unless a material risk of identity fraud is determined by the Management Response Team) |
| B3. Handle customer inquiries via phone & email<br>- Clarify talking points<br>- Verify authenticity/legitimacy of notification<br>- Address complaints<br>- Document process to eventually pass off to a Phone Bank or designated responders. Calls are to be logged with date, time, caller, and a summary of the conversation. |

# Information Security Incident Response Plan

## Incident Containment Activities Appendix F

The IRT will determine and execute the appropriate activities and processes required to quickly contain and minimize the immediate impact to the University, Client and 3rd Party.

Containment activities are designed with the primary objectives of:

- Counteract the immediate threat
- Prevent propagation or expansion of the incident
- Minimize actual and potential damage
- Restrict knowledge of the incident to authorized personnel
- Preserve information relevant to the incident

| |
|---|
| **A. Containment Activities - Unauthorized Access**<br>Activities that may be required to contain the threat presented to systems where *unauthorized access* may have occurred. |
| A1. Disconnect the system or appliance from the network or access to other systems. |
| A2. Isolate the affected IP address from the network. Use quarantine tools. |
| A3. Power off the appliance(s), if unable to otherwise isolate. |
| A4. Disable the affected application(s). |
| A5. Discontinue or disable remote access. |
| A6. Stop services or close ports that are contributing to the incident. |
| A7. Remove drives or media known or suspected to be compromised. |
| A8. Where possible, capture and preserve system, appliance and application logs, network flows, drives and removable media for review. |
| A9. Notify IR Team of status and any action taken. |
| **B. Containment Activities - Unauthorized Acquisition**<br>Activities that may be required to contain the threat presented to assets where *unauthorized acquisition* may have occurred. |

| |
|---|
| B1. Identify missing or compromised assets. |
| B2. Gather, remove, recover and secure sensitive materials to prevent further loss or access. |
| B3. Power down, recycle or remove equipment known to be compromised. |
| B4. Where possible, secure the premises for possible analysis by local management and law enforcement. |
| B5. Gather and secure any evidence of illegal entry for review by local management and law enforcement. |
| B6. Where possible, record identities of all parties who were a possible witness to events. |
| B7. Preserve Lenel (access services card logging) system, video surveillance camera logs and sign-in logs for review by local management and law enforcement.<br>- Lenel logs POC: Michael Goliat<br>- Video camper logs POC: Michael Arnone, Michael Goliat |
| B8. Notify IR Team of disposition of assets and any action taken. |

## Corrective Measures Appendix G

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

Corrective measures are designed with the primary objectives of:
- Secure the processing environment
- Restore the processing environment to its normalized state

| **A. Corrective Measures – Unauthorized Access**<br>Activities that may be required to return conditions from *unauthorized access* to a normalized and secure processing state. |
|---|
| A1. Change passwords/passphrases on all local user and administrator accounts or otherwise disable the accounts as appropriate. |
| A2. Change passwords/passphrases for all administrator accounts where the account uses the same password/passphrase across multiple appliances or systems (servers, firewalls, routers). |
| A3. Rebuild systems to a secure state (e.g. Tier I, II, or III controls as necessary) |
| A4. Restore systems with data known to be of high integrity. |
| A5. Apply OS and application patches and updates. |
| A6. Modify access control lists as deemed appropriate. |
| A7. Implement IP filtering as deemed appropriate. |
| A8. Modify/implement firewall rulesets as deemed appropriate. |
| A9. Ensure anti-virus is enabled and current. |
| A10. Make all personnel “security aware”. |
| A11. Monitor/scan systems to ensure problems have been resolved. |
| A12. Notify IR Team of status and any action taken. |

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

# Guidelines for HelpDesk Personnel — Appendix H

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

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

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

**Inquiries**
For those individuals who may be reporting a security incident, questions that might be asked include but are not limited to:
- Were NetIDs and/or passwords accessed or released?
- Were Social Security Numbers stored or processed (this is Restricted information)?
- Were medical records of individuals present or accessed?
- Were credit card numbers or financial information disclosed?
- Did physical theft of computer equipment occur?
- Was "foreign" or unauthorized equipment connected to the network?

**Discovery and Reporting**
If the answers to the inquiries indicate that an incident may have occurred, support personnel should assume that an incident has actually occurred and perform the following activities:
- Obtain and record the contact information for the individual reporting the problem (name, telephone numbers, e-mail address)
- Record relevant information about the incident (e.g., time/date of suspected occurrence, type of information compromised, location of the compromise)

- Inform the individual to expect contact from a member of the Incident Response Team
- Request the individual to treat the incident as a confidential matter
- Contact the Technical Infrastructure Services (TIS) “on call” engineer for further assistance.

**Escalation**

The TIS “on call” engineer is responsible for making an early determination if an incident has occurred or might be indicated. If the engineer believes an incident has occurred, might be indicated, or unsure, the IRT Lead or Alternate should be contacted immediately, using the department’s notification procedures.

## Sample Notification Letter — Appendix I

Month DD, YYYY

Case Western Reserve University has learned that an unknown computer attacker has breached a department Web server, which contained files with personal data for XXX individuals. We regret to inform you that you have been identified as one of the individuals whose names and Social Security numbers were included on this computer. This breach took place in MM YYYY.

It is not clear whether the attacker intended to access sensitive data on this server. At this time, there is no evidence to suggest that your personal information has been misused.

The department had the personal data for academic and employment purposes. Case Western Reserve has secured this Web server and information on it.

As a precaution, the university is making free identity theft protection available to all individuals whose personal data was on the server. With this protection, an identity theft firm, in conjunction with an insurance company, will help you resolve issues that may result over the next year if your identity is compromised. We strongly encourage you to register for this free service by calling Zander Insurance at 1-800-888-9999, extension 1234.

At Case Western Reserve, we recognize the importance of maintaining the privacy of student, faculty and staff data. Please know that we take this matter seriously. We continue to work to ensure that all of our policies practices promote the confidentiality of such records. We deeply regret any inconvenience or concern this incident causes you.

In addition to this e-mail, we will be mailing a print copy of this letter to your home address in the next few days. If you have questions, please e-mail or call me at thomas.siu@case.edu or 216-368-6959.

Sincerely,

Thomas Siu
Chief Information Security Officer

## Sample Appendix J
## Briefing Note- public disclosure

*FOR INTERNAL USE ONLY*

# BRIEFING NOTE

**Case Western Reserve University Responds**
**to Inadvertent Disclosure of Personal Information**

Case Western Reserve University has learned that group of files containing names, social security numbers and course schedules for approximately XXX undergraduates at the university was accidentally made available on the Internet.

The files were outwardly accessible from public Web pages, but the social security numbers were not clearly identified at that type of data. The information was removed immediately upon discovery, and at this time, it is clear that the major search engines (Google, Yahoo, etc.) had accessed and indexed the data. Because there is no current search engine cache available, there is no evidence to suggest that personal data has been accessed or misused to anyone's detriment.

All students affected are being notified through e-mail DDMMYY and with a print letter to be sent to their permanent home address the week of MM DD. In response to this disclosure, the university is providing free identity theft protection for the next six months/year to all students involved.

The university encourages these students and all members of the university community to follow the cost-free steps to monitor their credit reports described in
http://www.case.edu/its/security/docs/identity_protection.html

---

## VI. KEY MESSAGES

- At Case Western Reserve we recognize the importance of maintaining the privacy of sensitive data. We take this matter very seriously and continue to work diligently to ensure that our policies and technical security measures promote the integrity and confidentiality of such records.
- The posting of these files to a publicly accessible location is not considered to be in accordance with the university's Acceptable Use of Information Technology Policy. These files were intended to be made available behind a password-based authentication mechanism
- In may of this year, the university began using unique student identification numbers rather than social security numbers, so this isolated oversight has been addressed.
- The information was being used for a legitimate university purposes by faculty and staff authorized to access it.