

IT Security

Incident Response

Table of Contents

.....	1
IT SECURITY	1
INCIDENT RESPONSE	1
1.PURPOSE.....	2
2.BACKGROUND	2
3.ASSUMPTIONS AND DEFINITIONS	3
4.UNIVERSITY SECURITY OFFICER.....	3
5.INCIDENT RESPONSE PROCEDURE.....	3
6.INTERNAL REPORTING.....	3
6.1 UNIVERSITY IT SECURITY OFFICE CONTACTS	4
6.2.LOGGING.....	4
6.3.PRELIMINARY INVESTIGATIONS	4
6.4.IDENTIFIED SECURITY INCIDENTS.....	5
6.5.FURTHER INVESTIGATION AND CONFIDENTIAL SYSTEMS.....	5
7.OPERATIONAL GUIDELINES RELATING TO INCIDENT HANDLING.....	6
7.1.MEDIA	6
7.2.POLICE	6
7.3.COURT ORDERS	6
7.4.AUSCERT	6
8.OTHER ELECTRONIC INVESTIGATIONS	6

1. PURPOSE

This document details the procedures for responding to IT Security incidents. Determining an appropriate response to any one particular incident can be difficult and generalising for all incidents is even more difficult. However without following Incident Response Procedures (IRP) the potential for an individual incident being mishandled by (even well meaning) staff can be greatly increased.

2. BACKGROUND

The computing resources of the University are made available in an 'open' environment to support the academic research, instructional, and administrative objectives of the University. These resources are available to the University Community, which includes staff, students, visitors and guests of the University, as well as non-ANU entities within the physical boundaries of the University, which enable them to accomplish the tasks associated with their individual pursuits within the University.

The ever increasing complexity associated with operating and maintaining the information infrastructure together with the ongoing discovery of new threats and vulnerabilities, poses a major challenge in securing The University's resources. Thus the activities associated with IT Security extend across the University and all information related policies.

There are a number of issues to be considered in managing security within the University environment:

- The immense quantities of information managed and stored.
- The specific and changing needs of the University community.
- The risks associated when security is compromised.
- Risks associated with loss of data.
- Policy, legal and regulatory responsibilities.
- New technologies, exploits and vulnerabilities.
- Protection of privacy.
- Community perceptions, experiences and expectations.
- Increasing threat profile.
- Decentralised environment.
- Increasing requirements for collaboration and relationships with external organisations.
- Remote and mobile access to the full suite of information resources.

Therefore security incidents arising from misuse of the information infrastructure have the capacity to result in:

- Loss of confidentiality
- Identity theft
- Physical loss of information assets
- Denial of service and degradation in network performance
- Threats to persons and property
- Exploitation of system vulnerabilities
- Disruption to University business
- Threat of legal action against the University

It is therefore vital that the incidents identified as security risks to the information infrastructure are handled appropriately to ensure that these risks to the University are minimised.

3. ASSUMPTIONS AND DEFINITIONS

A threat is anything that can lead to a digital asset (electronic information, IT hardware and networks) being compromised through disclosure, modification, destruction, loss or interruption. Threats can be classified as human or non-human. Non-Human threats include natural disasters and failure of networks, hardware or software. Human threats can be categorised as malicious or non-malicious. Non-Malicious threats arise through human error or ignorance, while malicious threats include hackers and disgruntled employees.

The role of IT Security is to protect digital assets from compromise through the use of risk mitigation strategies and actions against known threats.

An IT security incident, in the strictest sense, is therefore any event that leads to, or attempts to compromise a digital asset.

All persons subject to investigation as a result of an IT security incident are assumed innocent.

All information collected as part of an investigation is confidential.

4. UNIVERSITY SECURITY OFFICER

Investigation of any IT security related incident will often involve the inspection of log files and possibly other information stored on the information infrastructure to determine the validity of any reported incident and determining remediation or recommended actions. The Vice-Chancellor and the Pro Vice-Chancellor with the responsibility of information services are the University delegates that can authorise the examination of information stored on the information infrastructure.

It is important for effective and efficient incident management that the university nominate an individual with the authority to take appropriate actions and, as required, direct actions to be taken by local area staff in response to a security incident.

The Chief Security Officer (CSO) is the nominated *Responsible Officer* as described within the University delegation system, who is charged with coordinating a whole-of-University incident response.

To assist in the discharging of these duties the CSO has created an IT Security team that consists of an IT Security Manager and IT Security Support staff. The role of the IT Security team is to assist with the operational aspects associated with monitoring and maintaining University IT Security. Specifically this includes: IT training and awareness programs; monitoring of university IT security logs and systems; and preliminary investigation of incidents.

5. INCIDENT RESPONSE PROCEDURE

6. INTERNAL REPORTING

Under the University IT security policy, all users are responsible for maintaining the security of the information infrastructure. It is therefore incumbent on all users to report any IT security incident or any suspicious activity that leads to a disruption to normal services to the IT Security Office.

As a guide users should report any of the following types incidents or suspected incidents to the IT security team:

- Attempted Intrusion: Scans, port probes
- Denial of Service attacks
- Computer Intrusion: Virus, root compromise, account compromise
- Unauthorised access to information: elevated access, disclosure of confidential material

Although it may be difficult for the average user to determine if a particular problem is a security incident, under no circumstances should individuals commence investigation or notify any external party with the appropriate authorisation. If staff or students are in doubt they should report the matter.

Report any suspected incident to the following email address:

IT.Security@anu.edu.au

6.1. University IT Security Office Contacts

Chief Security Officer

Allan Williams - Head Systems and Desktop Services

Phone: 6125 8404

Mobile: 0400 480 144

David Howse – IT Security Manager

Phone: 6125 3583

Gaby Hoffman – Network Security Officer

Phone: 6125 3264

Stuart Watson – IT Security Officer

Phone: 6125 7268

6.2. Logging

An incident that has been reported to the IT Security team will be recorded and tracked. Similarly if one of the University IT security systems generates particular alerts this is assumed to be an incident and logged within the incident tracking system as well.

Once reported, all incidents are confidential and will trigger off a preliminary investigation. Staff involved in investigating these incidents is bound by the University policy regarding confidential systems and the *Privacy Act 1988*.

6.3. Preliminary Investigations

A member of the IT Security team will undertake a preliminary investigation to determine the nature of the incident. During this initial investigation the IT Security officer must assume that an IT security incident has occurred and is authorised to put measures in place to mitigate against potential/further damage.

In the context of a preliminary investigation the IT security officers have standing authority to:

- 1) access, read, copy and collate relevant log files from any University IT system
- 2) monitor network traffic
- 3) temporarily block network traffic through:
 - a) firewall rules
 - b) access control lists on routers or switches
 - c) disconnection of hosts from the network
- 4) temporarily suspend access or accounts to services

In exercising any of this authority as part of an initial investigation any action taken will be documented and justification recorded. At the conclusion of any preliminary investigation if no evidence was found then the investigation would be concluded, any temporary network blocks or suspensions removed and the logged incident closed.

This preliminary investigation will be completed quickly so that any temporary measures are in place for no more than 24 hours.

If the preliminary investigation can identify the incident as an IT security incident or determines further investigation is required then the investigation will be deemed to be ongoing.

6.4. Identified Security Incidents

Typically these incidents can be readily identified based on the network traffic logs or the system logs. Examples of these types of incidents include virus or malware infections, web site defacements or other external network based attacks.

The investigating IT security officer will contact the system owner or the local IT support staff member to alert them to the problem. Depending on the severity or the level of risk this may be either by telephone and/or official email. During this time the affected host may remain isolated from the network in accordance with the *Network Acceptable Use policy* until the incident is closed and the problem has been resolved.

In consultation and cooperation of with the system owner /LITSS, based on the security classification of data held on the system, the investigation may involve an inspection of the physical system to determine the exact cause of the incident, look for specific source files used in the attack or to determine the extent of the security breach.

Should the need arise to during this investigation to inspect individual accounts, users data or confidential systems, the CSO and the University delegate will be notified and a

interim report prepared. Authority to continue the investigation or to start remedial action must be given by the delegate before proceeding.

Once this part of the investigation is complete it is the responsibility of the local IT support staff member or the system owner to under take remedial action and too inform the IT security office when the work has been completed.

6.5. Further Investigation and Confidential Systems

Incidents involving confidential systems or those incidents that require further investigation need University delegate approval to proceed. The delegate's approval will only be given after the presentation of an interim report outlining what was found and a request to continue the investigation. These reports may be electronic or a verbal briefing but approval to proceed will only be given in writing (email/fax/hardcopy).

In general approval will allow the following actions to occur:

- Copy user files in order to preserve email and data files
- Recover user files from backup media
- Inspect any collected file
- Impound any ANU electronic equipment connected to preserve evidence.

If the ownership of any piece of equipment, relating to the investigation, cannot be determined and it is connected to the ANU network then the equipment may be removed and secured by ANU IT Security staff. Investigation of data held on that equipment may not continue until the ownership has been determined. Where the equipment is determined not to belong to university the equipment owner of the system will need to provide proof of ownership before the equipment is released.

If the investigation reveals a breach of University policy then a report should be completed detailing the evidence found and any recommendations for further action be made to the appropriate management representative. The matter is then covered by the *Information Infrastructure Rules and Services Rules 2008* and will be referred to the appropriate management authority.

If criminal activity is discovered or suspected then the matter must be reported to the delegate immediately and further investigation is to cease.

7. OPERATIONAL GUIDELINES RELATING TO INCIDENT HANDLING

7.1. Media

All media enquires to be directed though the Office of the PVC

- Any statements with respect to any case to go through the Office of the PVC

7.2. Police

- All requests from any law enforcement agency be directed though the Office of the PVC

- Any discovery of potential IT criminal activity, the CSO is to contact the PVC immediately who will coordinate notification to the police

7.3. Court Orders

- All court orders or summons to be directed through the ANU legal office.

7.4. AusCERT

- The CSO and the IT Security Manager are authorised to report security incidents that affect other institutions to AusCERT.
- The CSO and the IT Security Manager are authorised to cooperate with AusCERT and provide network or system log information as part of an AusCERT investigation that does not breach University privacy guidelines.
- All other requests will be referred to the delegate for approval before being released.

8. OTHER ELECTRONIC INVESTIGATIONS

Based on the above definitions the role of the IT Security officers is to investigate IT security incidents and to protect the Universities digital assets from compromise.

Notably, it does not cover the investigation of:

- Abuse of email to send death threats, anonymous allegations or spam etc
- Allegations of plagiarism
- Use of University equipment for commercial gain etc...
- Discovery of or use of illicit software: Illegal copies of software, software that uses prohibited protocols
- Downloading of inappropriate material

Whilst the above examples are not within the strict definition of an IT security incident, they are collectively a breach of one or more of the University policies and involve the use of IT equipment. Because of this the IT Security Office acts as coordination and contact point for these investigations and will accept reports of these activities and refer reports to the appropriate delegate. Should an investigation be required the IT Security Officers will typically undertake these electronic investigations under the direction of the appropriate delegate.