ICT Security Incident Response Plan

The University of Waikato

Title	ICT Security Incident Response Plan
Author	Milton Markose (Systems Administrator – Security)
Contributors	Dougal Mair (Manager ICT Infrastructure)
Date	28-05-2014
Reviewed By	Information Security Forum (ISF)
Document Version	V1.0

Revision History

0.1 (draft)	30/04/2013	Initial ICT Security Incident Response Plan doc	Milton Markose
0.2 (draft)	17/06/2013	Include communication procedures	Milton Markose
0.3 (draft)	28/05/2014	Amendments following review by ISF	Dougal Mair
1.0 (final)	25/06/2014	Final version following ICTC approval	Dougal Mair

Table of Contents

1. Purpose

The purpose of the University of Waikato's Security Incident Response Plan is to monitor security incidents, calculate the level of threat associated with them and then set a response plan to follow when incidents occur. This Security Incident Response Plan provides the University with the steps to follow in the event where ICT security is compromised and sets out the roles and responsibilities of ICT staff in case of a security incident.

In the event of a security incident, the Security Incident Response Plan's goal is to stabilise the computing assets and networks as well as guide timely recovery from security mishaps. This ICT Security Incident Response Plan helps the University to

- facilitate rapid and successful recovery of systems and networks in the event of a security incident
- process security incidents in a systematic way
- make quick and efficient recovery from incidents
- minimize loss or theft of University's data
- effectively communicate to University stakeholders throughout the incident

This plan has been developed by the Information Security Forum (ISF), endorsed by IMAF at the June 2014 meeting and approved by the ICT Committee at its June meeting.

2. Scope

The Security Incident Response Plan applies to the entire University of Waikato's ICT infrastructure. The guidance explained in this document is applicable to staff and students of the University. This plan is the basic framework for ICT security incident preparedness. This plan does not cover individual needs of each faculty. Therefore, we encourage each faculty to customise this incident plan based on their requirements, while remaining in compliance with this plan.

3. Roles and Responsibilities

While each user (staff and students) of the University's ICT infrastructure is responsible for maintaining the security of computing systems and networks, and keeping them safe from IT security incidents, the following describes specific responsibilities for incident response.

3.1. System Administrator – Security (ITS Systems Team role)

- First point of contact in reviewing information system security issues
- Review and maintain the security incident plan in coordination with the Information Security Forum
- Take ownership, investigate and manage information system security issues
- Works with other ICT staff to analyse and resolve security incidents
- Responsible for the ICT security awareness program across the University.

3.2. ICT staff

ICT staff within the University (including System Administrators, Network Administrators, Programmers, Service Desk staff, etc.) are familiar with the University's ICT infrastructure and may be the first to discover a security incident. ICT staff are responsible for immediately reporting security incidents to the System Administrator – Security, or the ITS Systems Team during absences, and then to perform Security Incident Response Plan actions as required.

3.3. Staff and Students

Any security anomalies detected by end-users must be reported by staff and students to the ITS Service Desk, or local ICT Support staff. End-users (staff and students) should:

- Be alert for unusual behaviour of a computing system
- Report both suspected and known security incidents
- Collect and preserve any evidence if it is available
- Cooperate in the investigation as required

4. Types of Security Incidents

The types of security incidents listed here are based on common attack vectors and covers only a subset of the security incidents that can happen within the University's ICT infrastructure. Identifying the common types of security incidents helps staff and students to be prepared, and then detect and report security incidents in a timely manner.

4.1. Threat

A threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. Threats can be either internal or external.

- Internal Threat – A situation where a user misuses the University resources, attempts to gain unauthorised access or run a malicious code in any of the University's computing systems.
- External Threat – An instance where an unauthorised person attempts to gain access to University's ICT systems and services and that can result in disruption of service or theft of data.

In the event of a possible threat, the end user must immediately inform the Service Desk, or Local ICT Support staff.

4.2. Malicious Code

Malicious code like viruses, worms, Trojan horses and other malware can spread rapidly and containing the spread of these kinds of security incidents can be a difficult task to achieve. If anyone notices known\suspected malicious code running in any of the computing systems, it is their responsibility to remove the network connection on the affected system, where possible, to avoid further malicious code spread and then log a security incident with Service Desk, or local ICT Support staff.

Most of the malicious code will be detected by the University's Antivirus Software - Symantec Endpoint Protection (SEP), and will either be deleted or quarantined automatically. It is the responsibility of the end user to ensure that virus definitions are up to date with the latest virus definitions (eg the SEP shield has green light in the Windows task bar). If any of the systems fail to update their virus definitions, a security incident call needs to be raised with the Service Desk, or local ICT Support staff.

4.3. Hacker\Cracker Attacks

Hackers\Crackers attempt to obtain unauthorised access to systems. There will be multiple indications when a cracker\hacker compromises a computer network:

- Someone has logged into a user account from another system
- Logon does not work (someone might have changed the password)
- Email sent from computer without the user's knowledge
- Changes to directories and files

If the end user suspects a possible hacker\cracker attempt, they should immediately inform the Service Desk, or local ICT Support staff.

4.4. Technical Vulnerabilities

The technical vulnerabilities can leave a 'hole' in the computing network and thus allow threats, malicious code and crackers to compromise systems. Most of the vulnerabilities will be identified and rectified by ICT staff in a scheduled manner via proper patching and installation of updates from the system and software vendors. If a user discovers a hardware\software technical vulnerability, they should log a security incident with the Service Desk, or local ICT Support staff, at the earliest opportunity to avoid exploitation of the existing vulnerability.

4.5. Breach of Restricted Data

Any unauthorised access to restricted data maintained by the University that compromises its confidentiality, integrity and availability, is considered as a sensitive data breach and needs to be immediately reported to the Service Desk, or local ICT Support staff.

5. The University of Waikato's response to security incidents

The University defines the process involved in handling IT security incidents in relation to the six-step methodology based on the SANS incident response life cycle. These steps are Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned. This six stage methodology helps ICT staff to deal with and respond to security incidents efficiently. The incident handling life cycle is as shown.

Incident Handling Life Cycle

5.1. Preparation

Being prepared for when an incident occurs.

The University is protecting its computing network using Firewall, IPS and Antivirus, and ICT staff subscribe to security alerts, news, notices and bulletins to ensure that all appropriate defences are in place and up to date in order to protect the computing systems from a security incident. However, the University has to be prepared to appropriately deal with a security incident when they occur.

This Incident Response Plan is key to the University's preparedness.

For response preparedness, 24 hour on-call support for the University's core ICT infrastructure is provided by a member of the Infrastructure team on a weekly roster. The on-call support person is equipped with a smartphone, with all key contact details, and a pager to receive automated alerts for critical systems. The on-call support staff need to be fully conversant with this response plan.

5.2. Identification

Do we have an incident? If so, what scale, impact, severity, etc? Who needs to know?

The University uses several different approaches to identify security incidents, such as system abnormal behaviour symptoms, event logs, monitoring systems, network traffic report, IPS alerts and reports, Antivirus logs, analysing existing risks associated with the University's ICT infrastructure, etc.

End users should also report security incidents through to the Service Desk, or local ICT Support staff, and should protect evidence for further analysis if required - if the evidence collection is not within the user's ability, ICT staff should collect the evidence and incident details for them.

The System Administrator – Security has the responsibility to report incident information to the ICT Infrastructure Manager in a timely fashion. In addition, the System Administrator – Security will analyse the incident details and evidence, in coordination with different technical staff if required, and submit a detailed report to the ICT Infrastructure Manager with further suggestions and recommendations.

The ICT Infrastructure Manager, or delegate, is responsible for communicating the incident as appropriate.

5.3. Containment

Ensure we stop further infection, data leakage, etc.

Once the security incident has been identified, the next step is to limit the impact of the incident and reduce its severity as soon as possible. For example, if a computer is infected with a virus, the next action should be to disconnect the infected system from the network, or disconnect the network segment, to limit the spread of the virus attack.

A copy of a suspected system should be preserved in order to provide business continuity and a copy of the same backup can be used as evidence, if further forensic investigation is required.

It is also a requirement to change the system administrator and/or affected staff passwords immediately on all affected systems. Passwords should be changed on compromised systems and on all systems that regularly interact with the compromised systems.

5.4. Eradication

Removing the cause of the incident.

This step entails the work required to remove the cause of the security incident. For example, the removal of virus software from an infected computer. As part of the eradication process, ICT technical staff should identify the vulnerability(s) exploited and take additional steps to mitigate them. Based on the details collected during the containment process, the attack method would normally have been verified. However, if it is difficult to ascertain that the incident was due to a single attack, ICT staff should take steps to mitigate all of the possible attacks the incident could have been caused by.

A new\improved protection technique may need to be put in place as a result of a security incident, so a thorough vulnerability analysis should be performed on the compromised system. On completion of the eradication process a peer review of the compromised system should be undertaken prior to returning the system to service.

5.5. Recovery

Restoring normal operation.

The main objective of the recovery process is to carefully bring the affected systems back into the production environment by ensuring that the cause of the current incident does not lead to another security incident.

The University of Waikato defines recovery as

- The return of affected systems to an operationally ready state.
- Confirming that the affected systems are functioning normally.
- If necessary, implementing additional monitoring to look for future related activity.

5.6. Lessons Learned

What can we do to prevent similar incidents in future, and what Incident Report Plan actions could be improved?

A post incident report will be developed after a security incident and will include recommendations and suggestions for improved security protection. Based on the incident, the System Administrator-Security will file a report of the incident to the ICT Infrastructure Manager who will distribute the report appropriately. To enhance the existing security user awareness program the System Administrator - Security will highlight any appropriate information for end-users.

Based on the severity of the IT security incident, ICT staff may hold a lesson learning meeting (which would be optional for lower severity incidents).

6. Emergency Communication Procedure

Communication is a vital part of University of Waikato's ICT Security Incident Response Plan and it may need to be external as well as internal. The level of communication for an ICT security incident is based on its severity.

6.1. Communication Procedure – External

If the incident is potentially damaging to the University's reputation then Communications and External Relations (CER) should handle the communication, especially where the media is involved. In the case where the incident has legal implications and police need to be involved and the Head of ITS should liaise with the Senior Leadership Team (SLT). The involvement of other external agencies such as New Zealand National Cyber Security Centre (NCSC) and other third party security forensic companies will be decided by the Head of ITS and ICT Infrastructure Manager based on the incident severity.

6.2. Communication Procedure – Internal

Email is the most effective way of communicating to all staff and students for a large scale ICT security incident. The Information Security Incident Team will liaise with ITS management, and CER staff (for staff email) and SASD staff (for student email), for sending notifications. An email notification may also be distributed directly to specific users or email lists (eg the ISF member list, USG_List, etc).

7. Conclusion

The aim of the six stages of University's incident response plan is to help to secure the University's ICT resources in an efficient and appropriate manner.

The guidelines set by the Security Incident Response Plan for the University facilitates business continuity through a quick and efficient process, thereby minimising the disruption of critical computing services, as well as the loss or theft of crucial and confidential information.

8. Definitions

Terms	Definitions
Incident	*"An incident is an attack or attempted attack against a computer or network that harms, or potentially may harm, the confidentiality, integrity, or availability of network data or systems"*: http://www.ncsc.govt.nz/incidents.html
ICT	Information and Communication Technologies
Cracker / Hacker	A cracker, or hacker, is someone who breaks into, or attempts to break into, someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security.
Threat	Threat is a possible danger that might exploit a vulnerability in order to breach security and thus cause possible harm.
Vulnerability	Any security weakness associated with a computing system.
Malicious Code	A code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.
Virus	A computer virus is a malware computer program that can replicate itself and spread from one computer to another.
Worms	A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
Malware	Malware is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
Trojan horses	A Trojan horse, or Trojan, is a non-self-replicating type of malware which appears to perform a desirable function but instead installs a malicious payload, often including a backdoor allowing unauthorized access to the target computer.