IT Security

Incident Response Procedure

Version 1.2

Contents

1. Purpose

This purpose of the procedure is to define the roles, responsibilities and the process for the investigation and response to IT security incidents. The goal of this procedure is to ensure that all IT security incidents are handled in a consistent and efficient manner, in line with the following objectives:

- To provide a consistent and efficient mechanism for reporting IT Security incidents.
- To ensure that IT Security incidents are investigated and contained in an efficient and consistent manner.
- To provide stakeholders with recommendations in order to prevent incidents from reoccurring.
- To communicate the risks of IT Security incidents to senior University management.
- To ensure that the data protection officer is informed of any GDPR related data breaches.

2. Definitions

IT Security is the team is responsible for coordinating and supporting the response to an IT Security event or incident. Depending on the priority of the incident, IT Security may request assistance from service owners, members of the IT Leadership Group or external IT Security Professionals when responding to security incidents or events.

IT Security Event is any observable occurrence to an IT system or electronic information, which does not represent an immediate or serious threat to the University electronic information or computer assets. For example, an unsuccessful social engineering attack, endpoint protection software blocking malware, network firewall preventing brute force password attacks, malicious emails marked as spam, etc.

IT Security Incident is any unauthorized activity that harms or represents a serious threat to the confidentiality, integrity or availability of the University's electronic information, information systems or computer assets. For example, a compromised email account, successful spear phishing attack, critical web vulnerability such as SQL Injection or Cross Site Scripting, etc.

Service Owner is the individual or group accountable for a specific IT system or service within the University regardless of where the technology component resides.

Information or Data means any electronic information including personal data, communications and logs held in any University IT supported service or device whether it is provided directly by a University department or is managed by a third party on behalf of the University.

3. Scope

This IT Security incident response procedure applies to all IT systems, either locally or centrally administered, including University approved cloud services, all devices that access the University's computer network or any electronic device that stores University information.

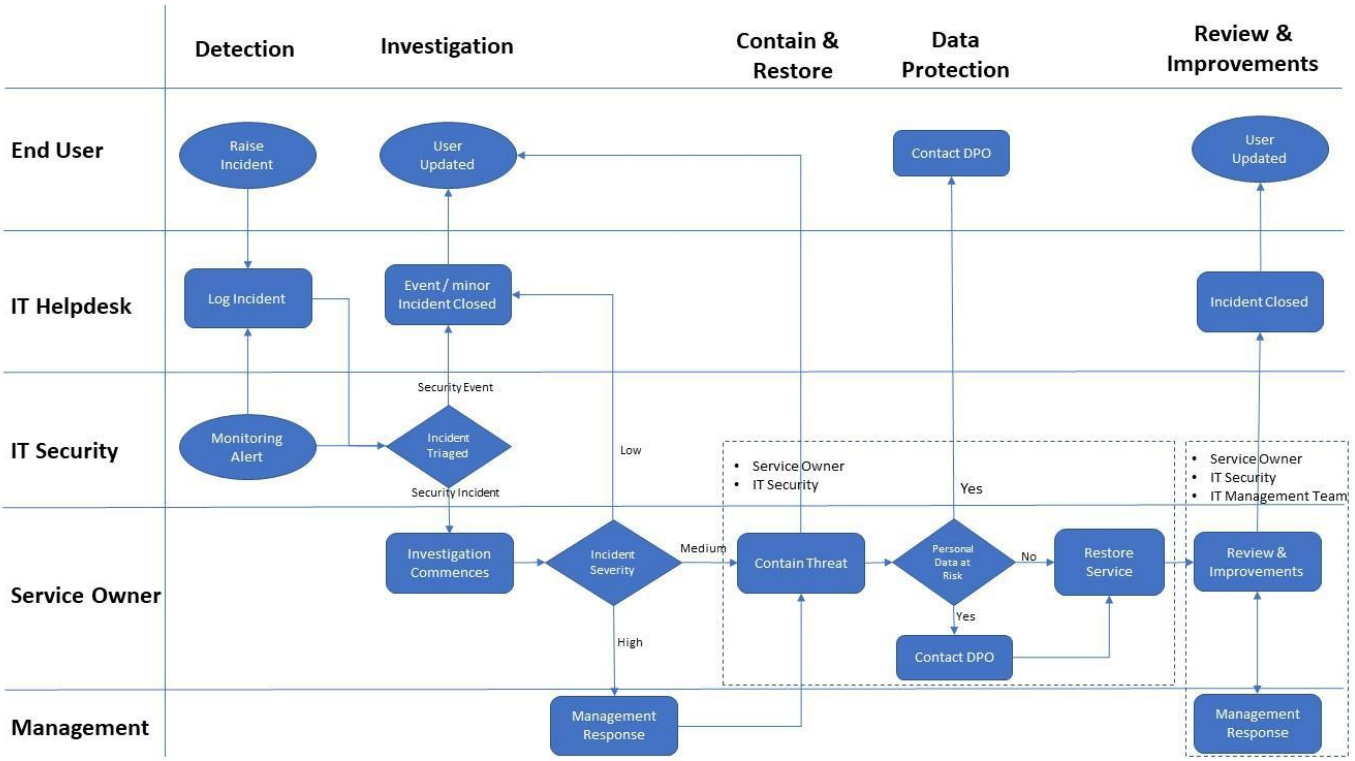
While mainly intended to address breaches to University IT policies, this procedure applies to any IT security incident involving the University's digital information or the University's computer assets, including network, servers, IT record management systems, etc.

Out of Scope

Incidents relating to system availability or performance which are not due to or result in an IT security incident are outside the scope of this procedure.

Data breaches which are not related to an IT Security incident should be reported to the University Data Protection Office as outlined in "UCD's Guidelines on Reporting Personal Data Incidents".

4. IT Security Incident Response Workflow



5. Incident Response Procedure

UCD's incident response procedure is based on the National Institute of Standards and Technology computer security incident response guide (NIST SP 800-61) and consists of the following steps.

Step 1. Detection

Potential incidents are identified using information from various sources, including but not limited to the following:

- User notification to the IT Helpdesk or IT Support Centres.
- Direct contact from affected or impacted University parties.
- Contact from University IT managers, network, system or application administrators.
- Contact from external third parties.
- Monitoring of University networks, systems or applications for anomalies, intrusions or unusual behaviour that could reasonably raise suspicion of potential compromise.

Examples of IT Security incidents covered by this procedure include but are not limited to:

- Breach or improper disclosure of University information.
- Compromise of information integrity e.g. damage or unauthorized modification of data.
- Compromise of information availability e.g. denial of service attack.
- Attacks originating from the University network or devices that impacts the business or services of an external party.
- Misuse or abuse of University services, information or assets, including breaches of University Policies
- Infection of systems by unauthorized or malicious software.
- Unauthorized access attempts that impact University business or services.
- Unauthorized changes to University information assets.

IT Security incidents or events should be reported immediately to IT Services by logging a request in the IT Support Hub www.ucd.ie/ithelp or by calling 01-7162700.

Step 2. Investigation

Once an IT security problem has been detected, IT Security will analyse the situation in order to confirm whether it is a security incident or a minor event.

If the problem is categorized as a minor event, the IT security will review the event with the customer and decide what actions need to be taken before closing the event.

If the problem is categorized as a security incident, the IT security team will contact the Service Owner to start an investigation to help determine the priority of the Incident, what information or systems are at risk and agree what steps are necessary to contain and recover from the incident.

Depending on the priority and scale of the incident, IT Security may contact members of the IT Leadership Group (ITLG) or request assistance from an external IT Security company to review and investigate the incident.

If the incident has a significant impact on the availability or performance of a Tier 0, 1 or 2 service, the ITLG team may decide to invoke the "Major Incident Response Plan" as outlined in IT Services Major Incident Management Planning, Response and Communications" procedure.

Incident Priority

Incident Priority and classification is based on whether an incident poses a threat to The University's IT assets, Information, community or IT systems. The determination may include, but is not limited to, the following factors:

- Does the incident involve unauthorized disclosure of high-risk or confidential information?
- Does the incident involve serious legal issues?
- Does the incident cause serious disruption to critical IT services?
- Does the incident involve active threats?
- How widespread is the incident?

Incident priorities categorized as "Critical" or "High" are referred to the IT Leadership group for review. All other incidents are handled by IT Security and the Service Owner in accordance with established practices. Further assessment may affect a reassignment to a different level of priority by the IT Security team.

IT Security Priority Levels

Critical: Any unexpected or unauthorized change, disclosure or interruption to information assets that could be damaging to the campus community or the University's reputation. Examples: A major attack against the university's IT infrastructure (Tier 0 or 1); a successful breach has occurred, a significant loss of confidential data or mission-critical systems or applications, a widespread malware infection affecting several University assets. Critical priority incidents are recorded as a priority 1 incident in "Service Now"

High Campus-wide and a potential public impact. A successful breach has occurred and/or a threat has manifested itself. A very successful attack that is difficult to control or counteract because no countermeasures, resolution procedures or bypass exist. Personal or confidential data may be involved. High priority incidents are recorded as a priority 3 incident in "Service Now"

Medium: The threat and impact are limited in scope, e.g. a department-wide not campus-wide. Examples may include early indications of a possible attack or intrusion detected with minimal risk to systems or information. Medium priority incidents are recorded as a priority 4 incident in "Service Now"

Low: An event with no effect on system operations. Intelligence received concerning threats to which systems may be vulnerable. Penetration or denial of service attacks attempted with no impact. No critical infrastructure is affected. Solutions or countermeasures are readily available.

Procedures are available and well-defined to resolve the problem. No protected information is involved. Low priority events are recorded as a priority 4 event in "Service Now"

Step 3. Containment

Once a security incident has been positively identified, IT Security will work with the Service Owner to isolate the affected equipment, system or account in order to prevent secondary threats, such as attacks on other internal systems, phishing emails, network disruption, etc.

In line with the University's Acceptable Use Policy, any system or account that is deemed to be a risk to the University's information or is actively causing harm, either to internal IT assets or external parties will have its IT service withdrawn.

The IT Security Team may undertake additional forensic or containment actions, including reviewing system logs, configuration, user settings, user activity, network logs, device forensics, etc. in order to help identify the root cause of the incident.

Step 4. Data Protection Incidents

Any incident or event that compromises the integrity, confidentiality or availability of personal or confidential University information must be reported immediately to the University Data Protection Office. It is the responsibility of the Service Owner or individual account holder affected by the security incident to report a data breach to the University Data Protection Office as outlined in "UCD's Guidelines on Reporting Personal Data Incidents". The IT Security team will also report the incident to the Data Protection Office if there is an immediate or potential risk to personal or confidential University information.

Step 5. Restoration

On receiving notice of an incident, the Service Owner for the affected information asset is responsible for resolving the issue. This includes but is not limited to changing passwords, reformatting media, patching, updating or reinstalling software, running scans and taking appropriate remediation action or taking other steps as needed to remove the threat and prevent similar compromises in the future.

Service Owners are expected to follow any specific protocols or recommendations cited in the notice and to document any actions they take to resolve the problem. This includes following established procedures for proper evidence collection, handling and storage; problem identification, remediation and mitigation; incident reporting and documentation, etc.

Once a system is secured, the Service Owners must notify the IT Security team of what actions were taken to eradicate the threat and provide the team with all related information, including root cause, copies of system logs, malware reports, etc. discovered during their investigation.

If the IT Security team are confident that appropriate action has been taken to eliminate the problem, approval will be given for the service to continue, such as allowing the device back on the network, enabling IT accounts, etc.

Step 6. Review & Improvement

The IT Security team and any individual or group affected by the incident or involved in the response process may make recommendations to improve security controls, security practices, business processes or the incident response process. Recommendations will be collected and documented by the IT Security Team and the Service Owners and passed to the IT Leadership group for review.

At the conclusion of serious incidents, the IT Security team and Service Owner may hold a debriefing to review lessons learned and to make recommendations of any changes to this procedure and related procedures if appropriate.

6. Communication

The Service Owner is responsible for ensuring that each step of the incident management procedure is communicated to all impacted customers, business owners and if required, senior University management. If an incident involves IT Services managed systems, the Service Owner will coordinate all customer communications through the IT Services Communications team.

7. Appendix

7.1 Incident Handling Checklist

The following incident handling checklist is a guide to the main step that should be performed when investigating and responding to a cyber security incident. The actual steps performed may vary depending on the type and nature of the incident. For example, if the person investigating the incident (incident handler) knows exactly what has happened based on analysis of indicators (Step 1.1), then there may be no need to perform Steps 1.2 or 1.3 to further research the activity.

Step	Action	Completed
Detection, analysis and report		
1.	Determine whether an incident has occurred	
1.1	*Analyse the precursors and indicators.* *("Precursors" indicate that incident may occur in future. "Indicators" give information that incident might have occurred or is happening now.)*	
1.2	*Looking for correlating information from multiple log sources.* *(Look for association from several log sources such as firewall log, device logs, Application logs, authentication logs, etc.)*	
1.3	*Research the incident* *(Use Search engines and knowledge Base's e.g Virustotal, Sophos logs, analyse email headers, etc)*	
1.4	*Document all details and gather evidence.*	

2.	Prioritized handling of the incident based on the following factors - Functional impact, Information impact and Recoverability effort.	
3.	Report the incident to IT Services via IT Support Hub (https://www.ucd.ie/ithelp) or call 2700. Please provide all details gathered in steps 1.1-1.4	
4.	If personal data is at risk due to the incident, report the incident to UCD's Data Protection Office	
Containment, Eradication, and Recovery		
5.	Acquire, preserver, secure and document evidence.	
6.	Contain the incident.	
7.	Eradicate the incident.	
7.1	*Identify and mitigate all vulnerabilities that were exploited*	
7.2	*Remove Malware, in appropriate material, and other components*	
7.3	*If more affected hosts are discovered (e.g new malware infections), repleast detection and analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them.*	
8.	Recover from the incident.	
8.1	*Return affected systems to an operationally ready state.*	
8.2	*Confirm that the affected systems are functioning normally.*	
8.3	*If necessary, implement additional monitoring to look for future related activity.*	
Post incident Activity		
9.	For Critical incidents create an incident report, otherwise update the IT Support Hub with details of how the incident was resolved.	
10.	For Critical incidents hold a lessons learned meeting.	

8. Revision History

Date of Change	Edited by	Summary of Change
1/11/2019	Paul Kennedy	Approved version 1.0
20/11/2022	Paul Kennedy	Updated Links version 1.1
22/03/2023	Paul Kennedy	Included Incident handling checklist 1.2

This procedure is updated and reviewed on a regular basis.