

Incident Response Policy

Table of Contents

1. Purpose	4
2. Scope.....	4
3. Definitions	4
4. Policy Statement	5
5. Roles and Responsibilities	6
5.1. Functional Departments	6
6. Severity Ratings	7
7. Process Overview	8
8. Process Detail	9
8.1. Step1 – Prepare	10
8.2. Step 2 – Identify	11
8.3. Step 3 – Contain	11
8.4. Step 4 – Remediate.....	13
8.5. Step 5 – Recover	13
8.5.1. Restore the System to Normal Operation	13
8.5.2. Ticket Closure	14
8.6. Step 6 – Root Cause Analysis	14
8.7. Documentation During an Incident	15
8.8. Post-Incident Documentation	15
9. Escalation Process.....	15
10. Communication	16
10.1. Communication with IT Support Team.....	16
10.2. Communication with OCA Staff – Use email communications	16
10.3. Communication with HR – Face to Face or Group Chats or All Departments	16
10.4. Communication with Students	16
11. Appendices	17
Appendix A – Information Security Categories	17
Appendix B – Evidence Collection	18
B.1. Introduction	18
B.2. Forensics Requirements	18
B.3. Preparation	18
B.4. Principles	19

B.5. Procedures	19
B.6. Identification.....	19
B.7. Seizure	19
B.8. Preservation.....	20
B.9. Extraction.....	21
B.10. Reporting	21
Appendix C – Evidence Collection Sheet	22
12. Document Control	24
12.1 Document Revision History	24

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate high-level guidance and requirements for managing and responding to information security incidents.
- 1.2. The OCA is becoming an increasingly information and data driven business. While this presents opportunities for the OCA to increase efficiencies and enhance our services, it also exposes the OCA to increased risk of security incidents. Such incidents could result in:
 - The theft of personal and confidential data, leading to a loss of customers/student's confidence and potential legal, regulatory or contractual penalties;
 - Customers/students defrauded through the theft of credit/debit card details;
 - Reputational damage to the OCA brand;
 - Financial loss and significant risk to ongoing operations through a major operational systems failure and/or service disruption.
- 1.3. This policy aims at ensuring that information, networks, systems, applications and equipment (hereinafter referred to as "OCA resources") are protected from all threats, whether internal or external, deliberate or accidental.
- 1.4. Details of the process for responding to information security incidents can be found in the [Information Security Incident Response Procedure](#).

2. Scope

- 2.1. This standard applies to all employees of the college (inclusive of external contractors and other third parties), in addition to the systems it owns and/or uses.

3. Definitions

- 3.1. An **IT service incident** is any event which is not part of the standard operation of an IT service, and which causes, or may cause an interruption to, or reduction in the quality of that service.
- 3.2. A **security incident** is an act or event that causes, or has the potential to cause, non-ephemeral harm to the enterprise and/or is in violation of enterprise security policy. It might be, but is not necessarily, a deliberate act intended to harm the enterprise. Not all security incidents are information security incidents (or relate to information technology in any way). As such, not all security incidents fall within the remit of the information security team. A security incident may include events such as burglary, robbery, theft, arson, criminal damage or an intruder on premises.
- 3.3. An **information security incident** is a security incident that specifically impacts upon the organisation's information. Information security incidents typically involve a potential impact to the confidentiality or integrity of information. Events affecting the availability of information are typically handled as IT service incidents by

Service Desk processes in the first instance; as such processes are focused on restoring service availability to users as quickly as possible. Loss of service availability is likely to become a security issue where it stems from a deliberate hostile act, or where change is required to avoid repetition.

3.3.1. Information security incidents include, but are not restricted to:

- Compromise of Non-Public information;
- Malware being discovered on one or more devices;
- Physical damage to OCA equipment that stores, retrieves, transmits or manipulates information;
- Events that significantly disrupt the availability of OCA resources;
- Unauthorised use of another user's profile (masquerading of user identity);
- Divulging a password to another user without authority;
- Improper use of email or the Internet, e.g. harassing email messages, downloading or distribution of pornographic images, and non-business-related activities that rise above minimal usage;
- Unauthorised copying of OCA information;
- Damaging or impairing the functioning of OCA resources in a manner that could impact information security;
- Unauthorised access to OCA resources from internal or external sources;
- Theft of OCA resources.

(In this document, the term *incident* when used without any qualifier is used to refer to an information security incident, except where otherwise noted.)

4. Policy Statement

- 4.1. The policy of OCA in regard to information security incident response is that all information security incidents will be reported immediately, investigated, managed and resolved appropriately in a structured and controlled way.

This shall ensure that:

- Information security incidents are dealt with speedily and efficiently;
- A consistent approach is implemented to deal with information security incidents;
- The damage caused by an information security incident is kept to a minimum;
- The likelihood of recurrence of an information security incident is reduced by the review and implementation of appropriate measures.

5. Roles and Responsibilities

- The IT Manager has direct responsibility for maintaining this policy and providing advice on its implementation.
- The IT Support Team is responsible for incident activities in co-ordination with the IT Manager and business processes.
- The Technology Enhanced Learning team is responsible for managing any student communications (if required).
- Relevant functional line managers teams are directly responsible for implementing this policy within their functional areas, and for adherence by their staff.
- All OCA staff have a responsibility to report information security incidents that they become aware of and to assist with the management of information security incidents where requested.

5.1. Functional Departments

Once the incident has been confirmed and the severity and scope has been determined, it may be necessary to activate support teams particularly with Critical incidents. Some or all the following skill sets may be required:

- **Forensics:** if the incident requires collection of logging data to establish the root cause of the incident, then forensics experts from a third party should be engaged.
- **Human Resources:** If the incident has been perpetrated by an employee/s.
- **Communications:** This is particularly necessary should the incident create a public reaction or may necessitate a public statement.
- **Legal Representative.** This is particularly necessary should the incident create a breach of law and to engage with law enforcement agencies where required.
- **Law Enforcement Agencies:** If the incident involves a crime or evidence of a crime, law enforcement agencies involvement may be required.

6. Severity Ratings

Severity	Impact and Examples
Critical	Impact: 1 or more critical processes have been interrupted completely. - Major disruption / impact to productivity / performance / reputation SLA: 30 mins first response Examples of Information Security incidents: - Unmitigated Malware detected on 5 or more machines. - Event impacts: - Confidential personal data. - Gained privileged access with Administrator/root. - Intruder access is network wide. - Unauthorised command line/shell access. - Backdoor Trojan or root kit found. - Persistent/on-demand access by intruder. - Serious legal issues. - Major downtime and/or loss of services. - Public interest.
High	Impact: 1 or more processes are in danger. - There are significant delays, but alternatives are available. SLA: 1 hour first response Examples of Information Security incidents: - Unmitigated malware detected on 4 or fewer machines. - Event impacts: - Gained privileged system or file access, but not Administrator/root Intruder access is zone-wide; - Re-exploitation required for intruder to re-gain access; - Serious legal issues; - Widespread service disruption; - Public interest; - Discovery of unauthorised device or wireless access point.
Medium	Impact: Processes are delayed but alternatives are available. SLA: 3 hours first response Examples of Information Security incidents:

	- Significant increase in observations of event precursors including malware mitigated by antivirus software. - Event impacts: • Unauthorised non-privileged user/privilege assignment. • Intruder access is VLAN/segment wide. • Unauthorised access to application commands. • Misconfiguration required for intruder to re-gain access. • Important legal issues. • Minor service disruption.
Low	Impact: • Incidents with limited to no impact on the process flow SLA: 8-hour first response Examples of Information Security incidents: - Observation of a moderate number of event precursors. - Event impacts: • Public data. • Single computer or very limited number. • No legal implications. No service disruption.

7. Process Overview

7.1. This process gives a framework for the OCA to respond to a Cyber Security Incident. It is not intended to cover every possible action or communication that may happen during an incident. In overview, the standard process is as follows:

- A wide range of parties (e.g. end user, service provider, IT Support Team) might potentially **identify a security incident** affecting OCA systems or data in the first instance.
- The **incident will initially be notified to the IT Support Team** within OCA via a variety of means including email, phone, face to face, but more commonly via the Service Desk ticketing system.
- The IT Support Team as the first contacted party **begin capturing more detailed incident-specific details** using the Service Desk tool.

7.2. For Critical, High and Medium incidents (see severity levels above) the IT Support Team will assemble in support of the IT Manager as necessary. The following parties are notified using the most appropriate method and form the basis of the IRT to grow if necessary, depending on the nature of the incident:

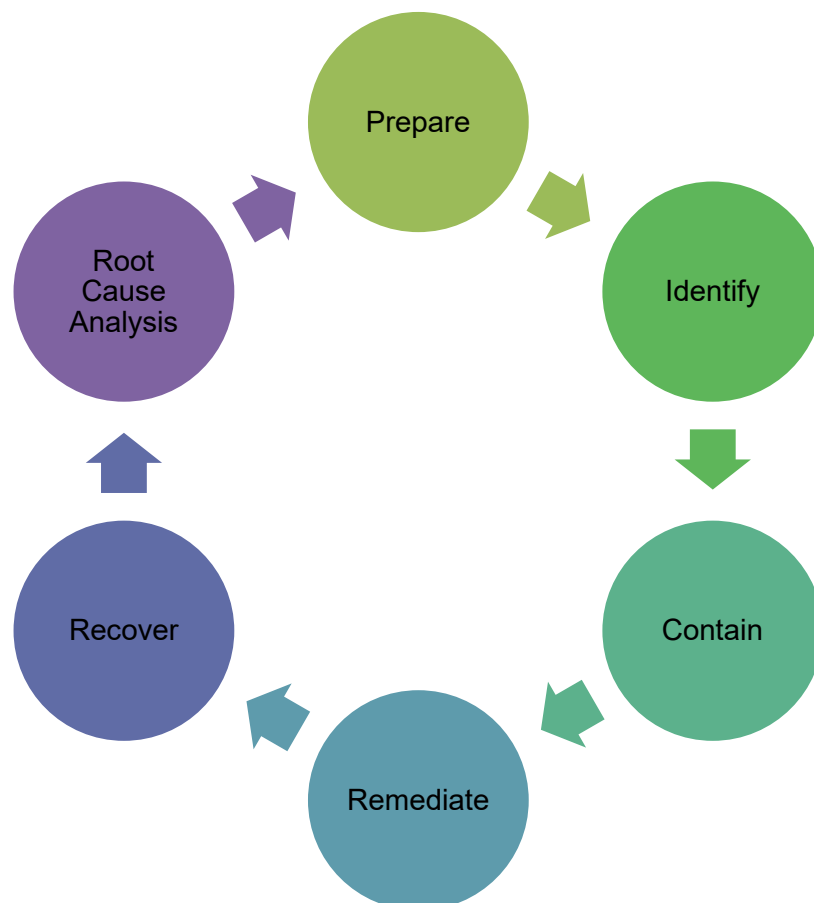
- Head of Technology and Innovation.
- IT Manager,

- Human Resources
- Senior Management.

The IT Manager coordinates activity across all parties relevant, (in consultation with the OCA management for Critical incidents). This includes:

- Directing and coordinating incident containment, eradication and recovery (with the appropriate support team).
- Escalating to wider OCA teams as required (e.g. HR, Communications, Legal etc.)
- Briefing the OCA management (assisted by the IT Manager).
- Coordinating the post-incident lessons identified remediation work, in order to prevent the recurrence of similar incidents

8. Process Detail



Incident Management Process Steps

8.1. Step1 – Prepare

Logging and Monitoring - For effective analysis of security events all OCA systems are monitored in line with the [Logging and Monitoring Policy](#).

Incident Response Capabilities & Development - The IT Manager shall identify the resources required by their Support Team, including:

- The level of personnel resource required for the incident response function to respond effectively to the incident;
- The tools required for the IT Support Team to respond to incidents in a prompt, effective and consistent manner.
- Documentation requirements, in terms of plan/process/procedure documentation.

Personnel - The IT Manager shall ensure that a minimum of:

- Two members of the IT Support Team are available to respond to the incident as required (generally during office hours).

Training - The IT Team shall ensure that:

- An up-to-date organisation chart is maintained for the IT Support Team.
- Personnel within the incident response team undergo training to close any gaps identified within their knowledge to respond to an incident.

Testing - The IT Support Team and management shall ensure that:

- Training scenarios are developed for each incident type identified in this document.
- Each member of the incident response team participates in the handling of an incident of each identified type (either scenario based or real) each year.
- Testing incorporates an appropriate blend of:
 - Walkthroughs, where the relevant staff members are guided through the relevant incident handling process in 'slow time' in order to gain familiarity with the full range of scenarios and to identify potential improvements to documented processes.
 - Table-top exercises, where staff members are required to identify the appropriate steps to solve a scenario presented to them (without on-going assistance) in an office setting.

Assurance – The IT Support Team shall invite:

- The OCA management to attend incident response exercises and/or review the incident response process not less than annually.
- The OCA IT Support Team personnel to attend incident response exercises and/or review the incident response process not less than annually.

8.2. Step 2 – Identify

Incident Identification and Reporting - The incident will be identified in one of the following ways:

- Logs/alerts from monitoring systems.
- End user reporting an incident to the Service Desk (telephone, email, or ticket system).

Capture of Incident - The IT Support Team will enter the incident onto the appropriate service desk or works management system as appropriate.

8.3. Step 3 – Contain

Investigate & Analyse - The key objectives of the investigation phase are to:

- Identify the scope of the incident.
- Identify and seize all evidence relevant to the incident (devices, log files, access records, infected files, e-mails, firewall rule sets, configuration files, database tables, etc.).
- Identify the chain of events that resulted in the incident.
- Qualify and quantify any loss or damage.
- Identify the compromise method/mechanism used, and any policies violated.
- Identify the root cause.
- Identify potential victims, perpetrators and witnesses.
- Inform incident containment.

The initial analysis must provide enough information for the IT Support Team to contain, eradicate and recovery from the incident. If in doubt, the IT Support Team should assume the worst until additional analysis indicates otherwise.

The IT Support Team should promptly:

- Identify the approximate scope of the incident, in terms of:
 - Networks / network segments affected.
 - Systems affected.
 - Affected hosts (by hostname/IP).
 - Applications/services affected.
 - Data assets/types affected.
 - Any other relevant factors/dimensions.

Notify the IT Support Team that the incident has occurred. Specifically:

- Notify any service provider where the incident may affect the infrastructure they manage, or where assistance might be required in containing the incident.

The IT Support Team should promptly:

- Identify the event logs available from systems within the scope of the incident, or which may otherwise assist in its investigation, and obtain a copy for analysis if not already held centrally.
- Interrogate the relevant system log data to identify events relevant to the incident, leveraging support team assistance where necessary.
- Determine the incident's root cause, timeline and impact in terms of what, where, when, who, how and why.
- Confirm that the incident is in fact a Cyber Security Incident. If not, re-categorise the relevant tool ticket and re-assign as appropriate.
- Assess the incident type/category and extent of the incident's impact, using Appendix A.
- Confirm/refine the severity assigned to the incident, using the Severity Rating above and Appendix A.
- Escalate, if the incident severity appears higher than initially assigned.
- Review the appropriate OCA playbook for the incident type e.g.:
- In the case of a **malware infection**: perform research (e.g. using search engines and knowledge base) on the key symptoms and vulnerabilities exploited in order to identify the particular piece of malware, exploitation kit, etc. that may have been used. In addition, the Information Security Malware Incident Response Playbook should be followed.
 - In the case of suspected network breach/data loss the Information Security Data Breach/Loss Incident Response Playbook should be followed.
 - Update the key facts arising from incident analysis on the relevant incident ticket.
- Ensure evidence is collected and handled in accordance with Appendix B.
- Engage with third party forensics provider for evidence gathering and forensics work if required as soon as possible.

A balance must be maintained between investigation (taking the time to fully understand what happened) and restoring any loss of service to users and operations.

The IT Support Team shall decide, as part of the Investigate / Analyse step whether the severity and nature of the incident is such that external Forensic support should be initiated.

Incident Containment - The objective of the Contain step is to prevent the incident from getting worse (in either scope or severity). This typically comprises isolating affected systems from unaffected systems, in order to stop the incident from spreading.

The incident handling team should:

- Back up the system(s) affected. Specifically:
 - If there is evidence that the incident is malicious in nature, ensure that data is backed up forensically (as per Appendix B). If there is too much data in-scope to back all of it up to forensic standards, then focus on backing up the data most directly relevant to the incident forensically.
- Seize any affected physical storage media (e.g. hard disks or removable media), if possible, without having a significant and lasting impact on critical services.

8.4. Step 4 – Remediate

The objective of the remediate step is to:

- Correct the incident by addressing its symptoms (e.g. healing malware infections or correcting access control lists).
- Prevent its immediate reoccurrence by addressing its root cause. For example: changing firewalls and/or router rule sets, moving the target host to a different network segment and/or IP address, or constraining access to the target data to the minimum possible subset of users and locations.

The incident handling team shall:

- Take those actions identified that are appropriate for the type and precise circumstances of the incident.
- Take such additional actions as are appropriate for the type and precise circumstances of the incident, with appropriate authorisation (e.g. by the IT Manager) for high-impact or high-risk eradication actions.

8.5. Step 5 – Recover

8.5.1. Restore the System to Normal Operation

The primary objective of the recovery phase is to restore the affected system(s) to fully operational status.

The IT Support Team shall:

- Liaise with the forensics provider (if provider assistance is required) to ensure that all evidence gathering work has completed prior to attempting to restore the system to operation.

- Decide the conditions under which the affected system(s) can be restored to normal operation. For example: it may be better to leave systems offline while operating system upgrades and patches are installed to prevent the recurrence of critical vulnerabilities.
- Restore the system; e.g. by re-imaging the affecting devices using the relevant build image and restoring data from cleansed / last known good backups.
- Verify that the system has been restored successfully, and that no further traces of the incident are evident.
- Continue to monitor the affected systems closely subsequent to recovery, to detect any recurrence of incident symptoms.

8.5.2. Ticket Closure

When the incident appears to have been resolved the incident handling team shall:

- Update the incident documents and tickets with a summary of the salient points.
- Contact the user/engineer that raised the incident to confirm that the incident has been resolved to their satisfaction

8.6. Step 6 – Root Cause Analysis

The primary objectives of the Review & Learn step are to identify:

- How similar incidents might be prevented from happening in future.
- What change in security posture might be appropriate to minimise risk in a manner proportionate to risk, cost and usability. Immediately upon the closure of the relevant incident document or ticket, the incident handling team shall document:
- The incident resolution within an appropriate knowledge base article and notify the SLT members of the updated knowledge base item via e-mail.
- Any workarounds or temporary measures put in place, and when they should be reviewed. This information should be shared with the IRT and Service Desk.

The IT Support Team shall conduct a formal post-incident review following any severe or major Cyber Security Incident (Critical or High). The post-incident review describe:

- The incident in overview.
- The impact on OCA and its students, in terms of both severity and breadth.
- The incident timeline in terms of key events; including the time elapsed between detection and resolution of the incident.
- The apparent root cause of the incident.
- Whether the incident was caused by a control failure.
- A summary of the actions taken to manage the incident.

- Any temporary solutions put in place, and the extent to which they are likely to be effective and sustainable.
- The extent to which there is a risk that the incident might recur.
- Recommended changes to, or the introduction of additional, security controls in light of the incident.
- Recommended changes to logging and monitoring arrangements as a result of the incident. An assessment of the effectiveness of the incident handling response.
- Any changes recommended to the Incident Response Procedure as a result of the incident.

The output of the post-incident review shall be documented as follows:

- In a report using the templated incident report.

The IT Manager shall:

- Conduct a post-incident debrief with each of the teams/parties named in the Incident Report within 2 weeks (preferably 1 week) of its publication, to discuss improvement objectives and to answer any queries arising.
- Conduct a debrief with each member of the IT Support Team that handled the incident in order to identify both positive areas of individual performance and any individual learning points to be developed.
- Where relevant, derive training scenarios and other training materials using the incident documentation.
- Update the Incident Response Policy (this document) and all relevant playbooks with any changes to the incident management process as a result of lessons learned from the incident.

8.7. Documentation During an Incident

The incident handling team shall, for each incident which it is called upon to handle:

- Document details regarding the current status of the incident and the actions currently underway within the system being used.
- Document major occurrences in relation to each incident within the relevant system. For example:
 - The incident moving from one incident handling phase to another.
 - Additional instances of the incident being reported
 - Changes to incident type or severity.
 - Updates requested by, and/or provided to, the user who raised the incident or other key stakeholders.

8.8. Post-Incident Documentation

At the conclusion of each incident, the IT Support Team shall:

- Summarise the key details within the relevant system.
- Collate all incident handling documentation relevant to a given incident within an appropriate area that is only accessible to authorised persons.
- Ensure key offline documentation is referenced by file name or hyperlink from the relevant system.
- Document an incident report for each Critical and High incident.
- Ensure that all evidence relating to a given incident is stored securely for at least 12 months after incident recovery.

9. Escalation Process

- 9.1. Incident escalation is a matter of perpetual analysis, re-evaluation of incident severity, and re-assessment of the extent to which efforts to manage an incident have been successful. The incident escalation process follows the chain of command in an upward fashion.

10. Communication

10.1. Communication with IT Support Team

The primary means of communicating groups involved in incident investigation or resolution are:

- Updating the IT ticketing system for documentation and audit purposes.
- Creating a Google Workspace 'Chat Space' and monitoring activities via this space. This will ensure all activities are documented and can be used for post incident reporting.
- Email Distribution Groups. All members of the IT Support Team should be part of the email distribution group to allow incident communications.
- For an incident involving failure of internal communications tools (Google Meet/Email/MS Teams) then telephone/mobile should be used for communications.

10.2. Communication with OCA Staff – Use email communications

For incidents relating to specific users the incident handling team shall:

- Update the user that raised the incident with regards to the incident status and progress on a periodic basis.
- Update the user that raised the incident upon the incident's resolution.

10.3. Communication with HR – Face to Face or Group Chats or All Departments

- 10.3.1. For incidents that potentially involve malicious action by employees or loss of employee data the HR team should be engaged to implement their relevant processes as follows:

- Disciplinary/Remediation process where an employee may have been involved in the creation of the security incident.

10.4. Communication with Students

- 10.4.1. The IT Support Team should normally communicate with students via the Head of Technology and Innovation. A communication will be drafted for release by the Head of Technology and Innovation to all students informing them of the situation and how much this affects them.
- 10.4.2. Depending upon the severity and urgency of the incident, the Head of Technology and Innovation may either send the communication directly (in the case of High or Critical incidents), or may alternatively request that the Communications team issue the communication.

11. Appendices

Appendix A – Information Security Categories

Appendix B – Evidence Collection

Appendix C – Incident Response Checklist

Appendix A – Information Security Categories

Top Level	Sub-Categories	Baseline Rating*
Malware Outbreak	Ransomware	Critical
	Malware – generic Command and Control APT	Varies based on number of affected users
Network Intrusion/system breach/system misuse	1. Breach of corporate networks and/or critical systems 2. Breach of Website – defacement 3. Account Compromise – Standard User 4. Account Compromise – Admin User	Critical Medium High Critical
Loss of Asset	1. Lost system not encrypted 2. Loss and/or theft of encrypted laptop 3. Loss and/or theft of encrypted mobile phone 4. Loss and/or theft of encrypted removable media	High Medium Medium Medium
Phishing	1. Phishing email with malicious link/attachment received	High
	2. Phishing email with malicious link/attachment accessed/opened	Critical
Denial of Service	1. Unavailability of critical assets resulting from Denial of Service (DoS) attacks	Critical
	2. Unavailability of Website resulting from Denial of Service (DoS) attacks	Low
Other	1. Generic security incident	Low

Appendix B – Evidence Collection

B.1. Introduction

Evidence is a subcomponent of Forensics. The primary reason for gathering evidence during an incident is to resolve the incident. However, evidence may also be a mandatory requirement for legal proceedings and is collected and preserved for detailed forensics and analysis as well as court proceedings. These cases include unauthorised access, data modification, and inappropriate usage. In response to these events, the IRT will collect evidence and thoroughly document how evidence and compromised systems, were collected, recorded, stored and protected. The procedures in this appendix are not necessarily intended to be followed step-by-step. Forensic Investigations are very delicate procedures that must be performed by qualified personnel. It is intended to provide awareness for those who may be involved in a forensic investigation and as a prompt for suitably trained forensics professionals.

B.2. Forensics Requirements

The Incident Management Procedure requires that:

- Any forensic work must only be performed on copies of the evidence material in order to protect its legitimacy. Any work duplicating the information must be carried out by an appropriately qualified forensics specialist to preserve the integrity of the evidence (including physical evidence such as fingerprints). A third party (independent of the technician carrying out the operation) must be present to witness the duplication process, and a full record of every step taken must be logged.
- The IT Support Team must coordinate with the Legal Team to collect electronic files and paper documents required to support a legal investigation or evidence discovery proceedings.
- All evidence in the forensic investigation of a security incident must be:
 - Collected using appropriate digital forensics procedures.
 - Secured.
 - And supported by a documented chain of custody.
- The original of any digital or physical evidence must be moved immediately to an appropriate secure location (e.g. a data centre, locked cabinet or other physical location with enhanced access control)."

B.3. Preparation

The IT Manager shall:

- Educate IT Support Team personnel to not act on behalf of or at the direction of a law enforcement agency.

B.4. Principles

The key principles that apply are that:

- No action taken by OCA employees, third parties or law enforcement agencies should change data held on a computer or storage media which may subsequently be relied upon in court.
- In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- The person in charge of an investigation has overall responsibility for ensuring OCA's adherence to the law and these principles.

B.5. Procedures

The incident response team shall:

- Collect and protect data related to incidents that may form the basis of a subsequent investigation, prosecution or legal action.
- Collect evidence such that it should be admissible in any legal proceedings.
- If necessary, as third-party forensic team will be scoped to provide forensic support;
- Minimise the risk of sensitive information being released inappropriately by ensuring that access to incident data is properly controlled and managed.
- Encrypt e-mails and attachments pertaining to an event or incident such that only the sender and intended recipients are able to read them.

B.6. Identification

The incident response team shall identify all devices on which relevant information can be stored, for inclusion within the scope of the investigation. This includes servers, desktops, laptops, tablets, smartphones, wearable devices such as smart-glasses or smart-watches, and USB memory devices (which may resemble or be built into other items).

B.7. Seizure

The incident response team shall:

- Seize and search devices (exhibits) that may contain crucial evidence.
- Log all decisions made with regard to which items and devices to seize and which not to seize, including rationale.

B.8. Preservation

Electronic evidence, like other types of evidence, is fragile. It is important to preserve the evidence in a manner which does not threaten the integrity of the data.

No action taken by OCA employees, third parties, or law enforcement agencies should change data held on a computer or storage media which may subsequently be relied upon in court.

Note: booting a system, installing software or performing maintenance changes data.

Where possible, a forensic image or a forensic clone of the device must be made:

- **Forensic Image.** A forensic image is an exact 'bit for bit' copy of the data from a device, stored in a file. It is typically obtained via a hardware write blocking device. Forensic images are typically stored as an: E01 – Expert Witness or 'dd' Raw format. Allowance should be made for such processes as they can be time consuming.
- **Forensic Clone.** A forensic clone is an exact 'bit for bit' copy of all of the data from a device to its equivalent location on another device.

When duplicating information, an independent third party must be present to witness the process, and a full record of every step must be logged.

When dealing with servers, it may not be possible to forensically image an entire network of servers for a number of reasons:

- The server may have to stay online 24/7.
- The size of the server and amount of data.
- Applicable time constraints.

In these situations, consideration should be given to the use of forensic software to access the live network and to carry out actions, such as:

- Examining the contents of servers and workstations.
- Capturing selective and/or volatile data.
- This can be achieved while still preserving the integrity of the evidence.

When performing forensics on a network, consideration should be given to using the backups. Back-ups can provide a good copy of the system. They can also allow an investigator to identify files added or deleted to a system by comparing files from different back-ups. Back-ups may also present file time/date information that can demonstrate when files/directories were last accessed, modified or created.

When using back-ups, the following potential issues should be considered:

- Availability for the appropriate date/time
- Compatibility and restoration
- Dates and times changed

- Limited life span.

B.9. Extraction

The incident handling team shall:

- Ensure that data manipulation occurs on a copy of the relevant data where possible
- (rather than on live system data or an evidential copy).
- Consider using techniques such as file signature/hash analysis to de-duplicate data.
- Given the tremendous amount of information that can be stored on electronic media,
- this is a critical element of the investigation.
- Identify any keywords likely to expose data of relevance to the investigation, and search on such terms.
- Identify any metadata attributes (e.g. file types or dates and times) that may enable data
- to be further filtered to that relevant to the investigation.
- Consider that relevant data might take many different forms, including:
 - Documents (word processing, spreadsheets, etc.).
 - Databases.
 - User account information.
 - Images.
 - E-mails.
 - Audio.
 - Video.
- Consideration should be given to information that may not be immediately accessible for the following reasons:
 - Installed software.
 - Connected devices.
 - System boot/shutdown.
 - User logon/logoff.
 - Print data.
 - Temporary files.
 - Clock changes.
 - File access.
 - Most Recent Used (MRU) lists.

B.10. Reporting

Forensic reports should show a structured methodology and include:

- Objectives.
- Chain of Custody.
- Data verification.
- Tools and methods used.
- Interpretation of findings.
- Summary.
- Glossary.

The forensic report should be distributed only to those who initiated the report.

Appendix C – Evidence Collection Sheet

Evidence Collection		
Incident ID: Name: Title: Date:		
Step	Action	Time of Action
1.0	Acquire evidence from a system of interest as soon as it becomes suspect that an incident may have occurred.	
2.0	Establish Safeguards	
2.1	Use a write blocker program to prevent the host from writing to its hard drives.	
2.1	Use a write-protected CD that contains trusted commands and all dependent files so that all necessary commands can be run without using the affected host's commands.	
2.3	Copy or save ALL evidence to write protectable or write once media.	
3.0	- Acquire dynamic evidence - Note: volatile information that may not be recorded in a file system or image backup. Caution: risks are associated with acquiring information from the live system. Any action performed on the host itself will alter the state of the machine to some extent. Also, the attacker may currently be on the system and notice activity.	
3.1	Issue only the minimum commands needed for acquiring the dynamic evidence without inadvertently altering other evidence.	
3.2	Document how far the local clock deviates from the actual time	
4.0	After acquiring volatile data, immediately make two full disk images to a sanitised write-protectable or write-once media.	
4.1	- Use forensic software to make two full disk images to preserve all data on the disk, including deleted files and file fragments. - Note: It may be necessary to acquire and secure the original disk as evidence; the second image can then be restored to another disk as part of system recovery.	

4.2	• Label these images and securely store one of the images to be used strictly as evidence. • Note: All evidence must be tagged and stored in a secure location.	
5.0	• Copy supporting log files from other resources to a sanitised write protectable or write-once media.	
5.1	• Store one copy as evidence. The second copy may be restored to another system for further analysis.	
5.2	• Create a message digest for log files and other pieces of digital evidence • Note: Message digests should be generated using software and a message digest algorithm.	
5.3	• Document the local clock time and deviation on each logging host.	

12. Document Control

Document Control	
Title:	Incident Response Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

12.1 Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
1.0	05/11/2025	Dean Humphreys	Final revisions approved and version updated to 1.0 for release