

Cyber Incident Response Management

BITS Technology Group Pty Ltd

Action	Name	Title
Prepared By	Muhammad Nauman Mustafa	Cyber Security Engineer
Reviewed By	Blair Munro	Head of Technology
Approved By	Bernard Mangelsdorf	Chief Executive Officer

Version	Date	Description of Change	Updated By
1.0	25 Feb 2025	Initial policy creation	Muhammad
1.1	26 March 2025	Incident reporting was added	Muhammad

1. Purpose

The purpose of this incident response plan is to outline the key activities and processes that employees need to follow in the event of a cyber incident. This plan aims to ensure a swift and effective response to minimise the impact of the incident and facilitate a quick recovery.

2. Scope

This plan applies to all employees, contractors, and third-party users who have access to the organisation's information systems and data.

3. Definitions

- **Incident Response Team (IRT):** A group of individuals responsible for managing and coordinating the response to cyber incidents. This team includes key employees, service providers, and law enforcement representatives.
- **Incident Response Team Lead:** The individual responsible for leading the Incident Response Team and making critical decisions during a cyber incident.
- **Cyber Incident:** Any event that threatens the confidentiality, integrity, or availability of an organisation's information systems, networks, or data.
- **Business Continuity Plan (BCP):** A plan that outlines procedures for maintaining business operations during and after a disruptive event, such as a high-priority cyber incident.
- **Accelo:** A platform used for logging and managing incident tickets, tracking actions taken, and documenting communications related to cyber incidents.

4. Roles and Responsibilities

The Incident Response Team (IRT):

- **Incident Response Team Lead**
Name: Blair Munro
Work Email: blair.munro@bitsgroup.com.au
Mobile: 0400499644
Personal Email: blairmunro@gmail.com
- **Services Manager**
Name: Jesse Whitton
Work Email: jesse.whitton@bitsgroup.com.au
Mobile: 0422380933
Personal Email: jesse.whitton@gmail.com
- **Security Engineer**
Name: Muhammad Nauman Mustafa
Work Email: muhammad.mustafa@bitsgroup.com.au
Mobile: 0410425044

Personal Email: muhammad.nauman.mustafa@gmail.com

- **Consultant**

Name: Bernard Mangelsdorf

Work Email: bernard.mangelsdorf@bitsgroup.com.au

Mobile: 0438129766

Personal Email: bernardmangelsdorf@gmail.com

- **Media Manager**

Name: Kahlia Mangelsdorf

Work Email: kahlia@bitsgroup.com.au

Mobile: 0420760095

Personal Email: kahlia.anderson@gmail.com

- **Client Communication Lead**

Name: Jake Whittle

Work Email: jake.whittle@bitsgroup.com.au

Mobile: 0422047673

Personal Email: jake.whittle@hotmail.com

- **Law Enforcement Representative**

Name: ACSC ReportCyber service

Contact Information: <https://www.cyber.gov.au/report-and-recover/report> and fill out the report. (as required)

5. Incident Response Plan

The Incident Response Team (IRT) is responsible for managing and coordinating the response to cyber incidents. The team includes key employees, service providers, and law enforcement representatives. When an incident is reported, the Incident Response Team Lead would:

- Determine based on the impact of incident (affecting 5 users or more else, best judgement).
- Classify the incident as high priority, medium priority or low priority.
- Low priority incident would be investigated by cyber security engineer and reported in Accelo ticket
- Medium / high priority incident tickets would be handled by IR Team Lead or assigned (as required).
- High priority incident ticket might also invoke Business Continuity Plan as deemed necessary.

The incident response process is divided into six phases:

5.1 Preparation

- Develop and maintain the incident response plan.
- Conduct regular training and awareness programs for employees.
- Ensure all systems are up-to-date with the latest security patches and updates.

- Maintain an inventory of critical assets and their security controls.
- Establish communication protocols and contact lists for internal and external stakeholders.

5.2 Identification

- Detect and identify potential security incidents through monitoring and alerting systems.
- Validate the incident by gathering and analysing relevant data.
- Classify the incident based on its severity and impact.
- Document the initial findings and notify the Incident Response Team.
- The evidence of the compromise have to be preserved in terms of screenshots/documentations/VM's snapshot where required.

5.3 Containment

- Implement short-term containment measures to prevent the incident from spreading.
 - Disconnect affected systems from the network.
 - Disable compromised accounts.
 - Block malicious IP addresses and domains.
- Develop and implement long-term containment strategies.
 - Apply patches and updates.
 - Reconfigure firewalls and access controls.
 - Monitor affected systems for signs of further compromise

5.4 Eradication

- Identify the root cause of the incident.
- Remove malicious code, unauthorised access, or other threats from affected systems.
- Apply necessary patches and updates to prevent recurrence.
- Conduct a thorough scan of the systems to ensure all threats have been removed.

5.5 Recovery

- Restore affected systems and services to normal operation.
 - Reconnect systems to the network.
 - Restore data from backups.
 - Verify the integrity and functionality of restored systems.
- Monitor systems for any signs of residual threats.
- Conduct a thorough review to ensure all issues have been resolved

5.6 Lesson Learnt

- Conduct a post-incident review to analyse the response and identify areas for improvement.
- Document the incident, response actions, and lessons learned.
- Update the incident response plan based on the findings.
- Share the lessons learned with relevant stakeholders to improve future responses.

6. Communication Plan

- Notify key stakeholders, including management, employees, and affected customers, about the incident.
- Provide regular updates on the status of the incident and response efforts.
- Coordinate with external service providers and law enforcement as needed.
- Ensure all communications are clear, accurate, and timely.

7. Documentation and Reporting

- Maintain detailed records of the incident, including timelines, actions taken, and communications. Each incident would be logged in Accelo as ticket.
- Prepare an incident report summarising the incident, response actions, and outcomes.
- Submit the incident report to management and relevant authorities as required.
- Store all documentation securely for future reference and compliance purposes.

8. Compliance

This cyber incident response plan must be readily available to all employees. It will be accessible through the company's document management portal, employee handbook, and during onboarding sessions. Also, the policy should be available in hard copy on-premises as well as a hard copy stored in a secondary accessible location.

Employees are encouraged to review the policy regularly and stay informed about any updates as compliance to this policy is mandatory.