Information Technology

Incident Response Plan

**Umina SLSC**

**September 14, 2023**

Contents Page

[1 Purpose 1](#_Toc144307903)

[2 Scope 1](#_Toc144307904)

[3 Incident Response Process 1](#_Toc144307905)

[4 Roles and Responsibilities 2](#_Toc144307906)

[4.1 Staff and Volunteers 2](#_Toc144307907)

[4.2 Club Executive 2](#_Toc144307908)

[4.3 IT Resource 2](#_Toc144307909)

[4.4 Managed Service Provider 3](#_Toc144307910)

[5 Revisions 3](#_Toc144307911)

[6 Document History 3](#_Toc144307912)

[7 Document Control Log 4](#_Toc144307913)

# Purpose

This policy ensures that plans and procedures are defined for the controlled response to IT security incidents for Umina SLSC’s information or technology assets or services.

# Scope

This Policy applies to all volunteers, members, permanent staff, temporary workers, or third-party vendors who manage or use Umina SLSC’s Information Technology infrastructure and applications.

This document forms part of the Umina SLSC Information Security Policy, and any terms or definitions from that document apply here.

# Incident Response Process

The following steps are to be followed in the case of a cyber incident.

Incident

Initial Responder

Club Executive

IT Resource

Sensitive data or financial impact?

Resolution

Yes

Club Board

SLSNSW

SLSA

Remediation

Close

# Roles and Responsibilities

The Incident Response Team will vary depending on your organisation's size and the incident's severity. The below roles are considered the core of what would be needed for an Incident Response Team.

## Staff and Volunteers

If staff or volunteers observe any unfamiliar activity on their devices, they shall immediately disconnect the system from the network and report the incident to their supervisor and the IT Resource. The following steps outline the actions to be taken by staff and volunteers upon encountering an incident:

* Report any unfamiliar activity on servers/desktops/applications to their supervisor by email, phone, or verbal communication.
* The supervisor shall assess the situation and escalate to the Club Executive if it appears to be a potential cyber incident.
* Staff and volunteers shall comply with the directions given by the Club Executive and IT Resource to facilitate a quick response, repair the system, restore the service, and analyse the incident.

## Club Executive

The Club Executive shall oversee the incident management process within their teams. They shall:

* Respond quickly to incidents reported by individuals.
* Inform the IT Resource at the earliest depending upon the magnitude of the incident
* If the incident does NOT involve the loss of personal or sensitive information or does not have any significant impact on the individual or the team, they shall:

1. Repair the system and restore the services.
2. Document the resolution for future reference.

* If the incident DOES result in the loss of personal or sensitive information or critical data or has any potentially severe impacts, the Club Executive shall:

1. Inform the IT Resource.
2. Document the details of the incident and the actions taken.
3. Follow the defined response plan outlined in this document. If the incident spans multiple functions, the Club Executive may seek guidance from the IT Resource and Club Board.

* The Club Executive must test the security incident response process at least annually.

## IT Resource

The Club Executive must appoint a suitably qualified IT Resource to act as the technical point of contact for all IT responsibilities and computer incidents, including the following:

* Coordinates activities with the Club Executive.
* Documents the personal or sensitive information that might have been breached
* Guides the investigation of customer and employee personal information privacy issues.
* Assists in developing appropriate communication with impacted parties.
* Assesses the need to update privacy policies, procedures, and practices due to the breach.
* In case of incidents that could result in an information system's failure or loss of service, the IT Resource shall immediately take necessary steps to mitigate the attack or failure and resume the benefits as early as possible.
* It may be possible for an attacker to exploit vulnerabilities in the system and gain unauthorised access to information processing assets due to vulnerabilities in the network/servers/desktops/devices. The IT Resource shall patch the servers/desktops/devices upon discovering such an attack and document the incident for future reference. The matter shall be escalated per the severity of the attack.
* Whenever any abnormal network utilisation is detected, the IT Resource shall act depending on the associated threat severity.
* The IT Resource will conduct a root cause analysis and take prudent steps to ensure the same problem does not re-occur. The findings will be shared with all concerned to prevent a recurrence.

## Managed Service Provider

A club or branch may engage an external IT Managed Service Provider (MSP), who may either act as the IT Resource or support an IT Resource. They will be engaged where necessary to provide more in-depth technical functions:

* Act as an escalation point for the identification and resolution of an IT incident
* Analyses network traffic for signs of denial of service or other external attacks
* Runs tracing tools such as sniffers, TCP port monitors, and event loggers
* Looks for signs of a firewall breach
* Contact an external Internet service provider for assistance in handling the incident
* Takes action necessary to block traffic from a suspected intruder
* Ensures all service packs and patches are current on mission-critical computers
* Ensures backups are in place for all critical systems
* Examines system logs of critical systems for unusual activity
* Review systems to ensure compliance with information security policy and controls
* Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
* Report any system control gaps to management for corrective action

# Revisions

This plan will be reviewed, tested, and periodically revised as risks, systems, and business practices change.

# Document History

|  |  |
| --- | --- |
| Title | Incident Response Plan |
| Classification | Internal |
| Creation Date | September 14, 2023 |
| Last Review Date | September 14, 2023 |
| Author | Matthew Ingersole |
| Owner | Chief Information Officer |
| Document Number | P-05 |

# Document Control Log

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change Description | Updated by | Date |
| 0.1 | First Draft Version | Damien Cantelo | 28/08/2023 |
| 0.2 | Draft Revisions | Matthew Ingersole | 29/08/2023 |
| 1.0 | First Published Version | Damien Cantelo | 30/08/2023 |
|  |  |  |  |
|  |  |  |  |