Information Technology

Security Policy

**Umina SLSC**

**September 14, 2023**

**Contents** Page

[Contents 1](#_Toc144308926)

[1 Purpose 1](#_Toc144308927)

[2 Scope 1](#_Toc144308928)

[3 Roles and Responsibilities 1](#_Toc144308929)

[4 Policies 2](#_Toc144308930)

[5 Security awareness training 3](#_Toc144308931)

[6 Staff / Volunteer Screening 3](#_Toc144308932)

[7 Access Control 3](#_Toc144308933)

[8 Remote Access 3](#_Toc144308934)

[9 Termination 4](#_Toc144308935)

[10 Regular Reviews and Segmentation 4](#_Toc144308936)

[11 Risk Assessment 4](#_Toc144308937)

[12 Enforcement 4](#_Toc144308938)

[13 Revisions 4](#_Toc144308939)

[14 Document History 4](#_Toc144308940)

[15 Document Control Log 5](#_Toc144308941)

# Purpose

This policy aims to provide guidelines to protect Umina SLSC’s information systems, assets, resources, members, volunteers and staff from information security incidents and breaches and to ensure Umina SLSC’s alignment with governance, legal and compliance requirements.

# Scope

The scope of this policy (and a suite of related policies) covers all information resources across Umina SLSC computers, systems, applications, cloud infrastructure and physical information resources.

These policies apply to Umina SLSC volunteers, partners, staff and suppliers, including vendors, service provider partners, contractors, consultants and other temporary staff.

# Roles and Responsibilities

The following roles and responsibilities are used throughout this Information Security Policy and all the associated sub-policy documents.

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Club Executives | The Club Executives have ultimate responsibility for information security and risk management within Umina SLSC. This policy is endorsed at the executive level. |
| Club Officers | The Club Officers are required to oversee Umina SLSC’s compliance with policies and procedures regarding information security. |
| IT Resource | The IT Resource manages the security posture for Umina SLSC. The responsibilities include:   * Developing, maintaining and ensuring alignment and delivery of the Information Security Program and policies. * Selecting controls, technologies and procedures to manage information security risks. * Generating compliance and assurance reporting information. * Managing breaches and incidents regarding information and security within Umina SLSC. * Promoting security awareness within Umina SLSC. |
| Managed Service Provider / IT Resource | The following are the responsibilities of the Managed Service Provider or the IT Resource if there is no Managed Service Provider appointed:   * Infrastructure is managed securely, including servers, networks, cloud infrastructure, and other computing devices that host applications or information resources such as databases. * There are appropriate border defences in place for secure perimeter protection. * Remote access is provided securely. * Cryptographic keys are managed, handled and stored appropriately and securely. * Assistance with monitoring and controlling all access to Umina SLSC data. * Physical access to publicly accessible network jacks, wireless access points, gateways and handheld devices is restricted. * Securely resolving end-user IT issues. * Logical access to Umina SLSC information and resources, such as through accounts and passwords, abides by security requirements. * Users are provided with the ability to operate mobile devices securely * Management of risks and incidents conform to security policies. * Requirements for engaging, monitoring and working with vendors are complied with. |
| Patrolling Members | The following are specific responsibilities of all Umina SLSC patrolling members:   * Understand the consequences of their actions regarding computing security practices and act accordingly. * Embrace the “Security is everyone’s responsibility” philosophy to assist Umina SLSC in meeting its Surf Lifesaving goals. * Maintain awareness of the contents of the information security policies. * Upon hire, read and understand the Umina SLSC Information Security Policy and Acceptable Use Policy. |
| Members | The following are the specific responsibilities of all Umina SLSC members:   * Understand the consequences of their actions regarding computing security practices and act accordingly. * Embrace the “Security is everyone’s responsibility” philosophy to assist Umina SLSC in meeting its Surf Lifesaving goals. |

# Policies

This policy document is the master document, supported by other documents governing Information Security Management System compliance within the company. Below is a set of objectives or intent statements for each of the specific security policies; these serve only as a directive to the intent and content of each approach. The particular security policies override any statements below and should be reviewed by the audience before any activity on Umina SLSC’s information systems.

It is essential that staff thoroughly familiarise themselves with the policies associated with their duties.

|  |  |
| --- | --- |
| **Sub-Policy** | **Purpose** |
| IT Acceptable Use Policy | Rules for the acceptable use of information and assets associated with information processing facilities, including Internet and email. |
| Data Handling Policy | Ensure that appropriate assurance and integrity are in place for handling data and media and managing data encryption where required. |
| IT Incident Response Policy | Ensure that plans and procedures are defined for the controlled response to IT assets or services security incidents. |
| IT Incident Response Plan | Define the steps to be taken in the case of a security incident. |
| Business Continuity Plan | This plan aims to establish guidelines to enable the continuity of operations during a disaster. |

# Security awareness training

Umina SLSC has a formal security awareness program to make all staff and volunteers aware of the importance of Information Security. Umina SLSC educates staff and volunteers upon hire and at least annually.

Umina SLSC requires the team to write that they have read and understood the company’s security policy and procedures.

# Staff / Volunteer Screening

The current staff/volunteers and potential staff/volunteers in Umina SLSC are screened through a defined procedure that includes reference checks to minimise the risk of a data breach or exposure from internal sources.

# Access Control

Access to Umina SLSC systems is provided on the following basis:

* Access to Umina SLSC systems must be justified by a legitimate Surf Lifesaving requirement before approval.
* Where Multi-Factor Authentication is used, user identification must be verified in person before access is granted.
* Umina SLSC systems must identify and document corresponding ownership responsibilities.
* Access to confidential information is based on a “need to know” basis.
* Confidential data access must be logged.
* Access to the Umina SLSC network must include a secure log-on procedure.
* Workstations and laptops must force an automatic lock-out after a pre-determined period of inactivity.
* Documented user access rights and privileges to information resources must be included in Disaster Recovery plans whenever such data is not included in backups.
* For susceptible processes, such as bank transfers or major code releases, at least two people should be involved in the approval process – one to initiate the request and one to approve/implement it.

# Remote Access

Umina SLSC staff, volunteers, and authorised contractors can access company systems remotely if access is via company-provided devices and as long as the required security measures are applied, including Multi-Factor Authentication for administrative functions.

Remote access must only be made available for the duration. At the same time, a particular task is being performed, and the remote connection must automatically time out after a set time to ensure unauthorised access to company systems isn’t unknowingly provided to unauthorised users.

# Termination

Once Umina SLSC staff, volunteers or contractors are terminated from their employment or membership with Umina SLSC, all devices and data must be returned to the company before departure. Staff, volunteers, and contractors must refrain from taking copies of data with them.

# Regular Reviews and Segmentation

Regular reviews and segmentation form an information part of Umina SLSC Information Security policy and has the following guidelines.

* All access control lists and firewall rules are reviewed and approved at least every six (6) months.
* All User rights and controls, especially privileged rights, are reviewed and approved at least every six (6) months.
* Internet-facing and internal infrastructure is segmented and kept in separate zones.
* All data in a multi-tenant environment is segmented logically or physically so that data is accessed for a single tenant only, without inadvertently accessing another tenant's data (e.g., using unique identifiers or different schemas for each tenant).
* Data is wiped on the supplier’s devices upon termination of the Services.

# Risk Assessment

Umina SLSC will carry out an annual risk assessment that would identify significant strategic developments in the industry, emerging threats, & vulnerabilities to the business and IT assets of the company and report results in a formal risk assessment document.

# Enforcement

Each staff member or volunteer is expected to comply with this policy. If there is any failure to observe the procedure, disciplinary measures may be taken. The steps which may be taken will vary according to the breach and the circumstances of the violation. However, the right is reserved to terminate the membership or employment of any staff member or volunteer who breaches this plan via the [SLSA Complaints Resolution Policy](https://www.surflifesaving.com.au/wp-content/uploads/sites/2/2021/11/Policy-6.06-Complaints-Resolution-2022.pdf).

# Revisions

This policy document will be reviewed, tested, and periodically revised as risks, systems, and Surf Lifesaving practices change.

# Document History

|  |  |
| --- | --- |
| Title | Information Security Policy |
| Classification | Internal |
| Creation Date | September 14, 2023 |
| Last Review Date | September 14, 2023 |
| Author | Matthew Ingersole |
| Owner | Chief Information Officer |
| Document Number | P-01 |

# Document Control Log

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change Description | Updated by | Date |
| 0.1 | First Draft Version | Damien Cantelo | 01/08/2023 |
| 0.2 | Draft Revision | Damien Cantelo | 09/08/2023 |
| 0.3 | Draft Revision | Matthew Ingersole | 15/08/2023 |
| 0.4 | Draft Revision | Damien Cantelo | 25/08/2023 |
| 0.5 | Draft Revision | Damien Cantelo | 28/08/2023 |
| 0.6 | Draft Revision | Matthew Ingersole | 29/08/2023 |
| 1.0 | First Published Version | Damien Cantelo | 30/08/2023 |
|  |  |  |  |
|  |  |  |  |