



Information Security Policy

Cronulla Surf Life Saving Club

September 2026

Contents

Page

Contents	1
1 Purpose	1
2 Scope	1
3 Roles and Responsibilities	1
4 Policy	2
5 Security awareness training	3
6 Employee Screening and Background Checks	3
7 Mobile Device Management	3
8 Access Control	4
9 Remote Access	4
10 Employee Termination	4
11 Regular Reviews and Segmentation	4
12 Risk Assessment	5
13 Enforcement	5
14 Revisions	5
15 Document History	5
16 Document Control Log	5

1 Purpose

The purpose of this policy is to provide guidelines to protect Cronulla Surf Life Saving Club's (CSLSC's) information systems, assets, resources and employees/members/contractors from information security incidents and breaches, and to ensure alignment with legal and compliance requirements.

2 Scope

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

These policies apply to CSLSC partners, members, employees and suppliers including vendors, service provider partners, contractors, consultants and other temporary employees.

3 Roles and Responsibilities

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

Role	Responsibilities
Board of Directors	The Board of Directors has ultimate responsibility for information security and risk management within CSLSC. This policy is endorsed at the executive level.
ICT Officer	The ICT Officer is required to oversee CSLSC's compliance with policies and procedures regarding the security of information. Additionally, the ICT Officer leads the security policy development, policy lifecycle, and security framework. More specifically, the ICT Officer's 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 CSLSC. • Promoting security awareness within CSLSC.
Service Desk Manager	SDM of the MSP who have been given responsibility for certain sign-off responsibilities including the ICT Officer.
MSP	The following are responsibilities of the MSP: • Infrastructure including servers, networks, cloud infrastructure and other computing devices that host applications or information resources such as databases are managed securely. • There are appropriate border defences in place for secure perimeter protection. • Remote access is provided in a secure manner.

	• Cryptographic keys are managed, handled and stored appropriately and securely. • Assistance with monitoring and controlling all access to CSLSC data is provided to the ICT Officer. • Physical access to publicly accessible network jacks, wireless access points, gateways and handheld devices is restricted. • Resolving end user IT issues in a secure manner. • Logical access to CSLSC information and resources, such as through accounts and passwords, abides by security requirements. • Users are provided with the ability to securely operate mobile devices • Management of risks and incidents conform to security policies. • Requirements for engaging, monitoring and working with vendors are complied with.
Director Administration	Due to their direct and constant relationship with existing employees, as well as their unique position of having the first and last interactions with new / terminated employees, the Director Administration has an important role with regards to CSLSC information security. The following items are the ongoing responsibility of HR: • Assist the ICT Officer with publishing and disseminating CSLSC information security policies and acceptable use guidance to all relevant system users, including vendors, contractors and business partners. • Perform background checks on potential employees who will have access to sensitive information. Background checks should include criminal, employment and education checks. • Verify that employees attend a security awareness training upon hire and at least annually. • Consult with the ICT Officer to administer sanctions and disciplinary action relative to violations of the Information Security Policy. • Notify the MSP as per formal process when any employee is terminated. • Maintain all Security Awareness and Acceptable Use Policy sign-off in employee files.
Employees/Members /Contractors	The following are specific responsibilities of all CSLSC users: • Understand what the consequences of their actions are with regard to computing security practices and act accordingly. • Embrace the "Security is everyone's responsibility" philosophy to assist CSLSC in meeting its business goals. • Maintain awareness of the contents of the information security policies. • Upon hire, read and sign CSLSC information security and Acceptable Use Policy.

4 Policy

This policy document is the master document, which is supported by other documents governing Information Security Management System compliance within CSLSC. 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 policy, the specific security policies override any statements below and should be reviewed by the audience prior to any activity on CSLSC's information systems.

It is important that employees/members/contractors thoroughly familiarise themselves with the policies associated with their duties.

Sub-Policy	Purpose
Acceptable Use Policy	Rules for the acceptable use of information and assets associated with information processing facilities including internet and email.
Data Handling Policy	To ensure that an appropriate level of assurance and integrity is in place for the handling of data and media as well as the management of data encryption and cryptographic keys.
Incident Response Policy	This policy ensures that plans and procedures are defined for the controlled response to security incidents for CSLSC information or technology assets or services.
Business Continuity Plan	The purpose of this plan is to establish guidelines to enable continuity of CSLSC's operations in an event of a disaster

5 Security awareness training

CSLSC has a formal security awareness program to make all employees/members/contractors aware of the importance of Information Security. CSLSC educates employees/members/contractors upon hire/joining/contracting and at least annually (including training, emails, posters and meetings).

6 Employee Screening and Reference Checks

The current employees and potential employees in CSLSC are screened through a defined procedure that includes reference checks to minimise the risk of attacks from internal sources.

7 Mobile Device Management

CSLSC employees and authorised contractors/members are permitted to access Confidential or Restricted data from BYOD and corporate devices once they have received a copy of all IT policies. CSLSC may provide devices such as laptops and mobile phones for to accessing Confidential or Restricted data. All devices must implement appropriate security controls, including multi-factor authentication (MFA)

Upon termination of employment, membership, or contractual engagement, or when a device is retired from service, all CSLSC data must be securely and permanently erased from the device. Users of Bring Your Own Device (BYOD) equipment are responsible for removing all CSLSC data from their personal devices when their association with CSLSC ends or when the device ceases to be used for CSLSC business.

8 Access Control

Access to CSLSC systems are provided on the following basis:

- Access to CSLSC systems must be justified by a legitimate business requirement prior to approval.
- Where Multi-Factor Authentication is used, user identification must be verified in person before access is granted.
- CSLSC systems must have corresponding ownership responsibilities identified and documented.
- Access to confidential information is based on a “need to know” basis.
- Confidential data access must be logged.
- Access to the CSLSC 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 highly sensitive processes, such as bank transfers or major code releases, there should be at least two people involved in the approval process – one to initiate the request and one to approve / implement it.

9 Remote Access

CSLSC employees, members and authorised contractors are allowed to access CSLSC systems remotely, as long as access is via CSLSC-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 while a particular task is being performed, and the remote connection must automatically time-out after a set time to ensure unauthorised access to CSLSC systems isn't unknowingly provided to unauthorised users.

10 Termination

Once CSLSC employees, members or contractors are terminated from their employment with the CSLSC, all devices and data must be returned to the CSLSC prior to departure. Employees, members and Contractors are not permitted to take copies of data with them and their access to Confidential and Restricted data must be limited during their notice period to ensure no data leaves the CSLSC.

11 Regular Reviews and Segmentation

Regular reviews and segmentation forms an information part of CSLSC Information Security policy and has got following guidelines.

- All access control lists and firewall rules are reviewed and approved at least every six (6) months.
- All User rights and controls specially privilege 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 multi-tenant environment is segmented either logically or physically such 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 supplier's devices upon termination of the Services.

12 Risk Assessment

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

13 Enforcement

Employees, members or contractors are expected to fully comply with this policy. If there is any failure to observe the policy, disciplinary measures may be taken. The measures which may be taken will vary according to the breach and the circumstances of the breach. However, the right is reserved to immediately terminate the employment of any employees who is in serious breach of this policy or terminate the membership or contract of any member of contractor in serious breach of this contract.

14 Revisions

This policy document will be reviewed, tested, and periodically revised annually or as risks, systems and business practices change.

15 Document History

Approved by the Board on (date of effect)	21/09/2026
Due for review on	21/09/2027
Responsible Officeholder for policy	Director Administration
Related legislation/SLSA or SLSNSW or CSLSC policy	
Policy Number	
Signed by Acting Director of Administration (on behalf of Board)	 Annette Tasker (Sep 24, 2026 11:38:42 GMT+10)

16 Document Control Log

Version	Details	Date
1.0	Initial draft	September 2026
2.0	Review, update terms and definitions specific to CSLSC	20/09/2026

CSLSC Information Security Policy v2

Final Audit Report

2026-09-24

Created:	2026-09-24
By:	Kim Grunert (kim.grunert@cronullasurfclub.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA9bvQUpsD14MlhvUAAI1TXSKQVZ_p5fIL

"CSLSC Information Security Policy v2" History

-  Document created by Kim Grunert (kim.grunert@cronullasurfclub.com)
2026-09-24 - 1:34:39 AM GMT
-  Document emailed to annette.tasker@cronullasurfclub.com for signature
2026-09-24 - 1:35:10 AM GMT
-  Email viewed by annette.tasker@cronullasurfclub.com
2026-09-24 - 1:38:20 AM GMT
-  Signer annette.tasker@cronullasurfclub.com entered name at signing as Annette Tasker
2026-09-24 - 1:38:40 AM GMT
-  Document e-signed by Annette Tasker (annette.tasker@cronullasurfclub.com)
Signature Date: 2026-09-24 - 1:38:42 AM GMT - Time Source: server - Signature Appearance Selected: MOBILE_DRAW
-  Agreement completed.
2026-09-24 - 1:38:42 AM GMT