South Eastern Community Connect

SECC

Cyber Security Policy

1. Purpose

South Eastern Community Connect (SECC) creates, receives, processes and stores information to deliver community-based services that support families, young people, seniors, volunteers, staff, donors, clients and community members across South Eastern Sydney. This information includes personal, sensitive, operational, financial, governance and service-delivery information. Its unauthorised disclosure, alteration, loss, misuse or unavailability may harm clients and staff, disrupt essential community services, damage public trust, breach legal or contractual obligations, or create financial and reputational loss for SECC.

This policy establishes SECC's overarching cyber security objectives, policy statements, governance expectations, and roles and responsibilities for protecting information assets. It is supported by operational procedures, technical standards, supplier requirements, incident response processes, privacy practices and staff awareness activities that together help SECC manage cyber security risk in a proportionate, practical and sustainable manner.

2. Scope

This policy applies to:

- all SECC business units, programs, community centres, service locations and outreach activities;
- all SECC employees, Board members, volunteers, students, contractors, consultants and temporary personnel;
- all suppliers, service providers, technology vendors, partner organisations and other third parties that access, store, process, transmit or support SECC information assets;
- all SECC information assets, including client and case records, aged-care and family-support records, youth program information, domestic and family violence support information, volunteer and donor records, finance records, HR records, email, collaboration platforms, websites, social media accounts, cloud services, mobile devices, endpoint devices, networks, backups and paper records that support digital systems.

This policy applies wherever SECC information assets are accessed or used, including SECC sites, home offices, outreach locations, community venues, mobile work environments, supplier premises and cloud-hosted environments. Personal devices may only be used for SECC business where authorised and managed in accordance with this policy and supporting procedures.

3. Cyber security objectives

SECC's cyber security objectives are to ensure that:

- information assets are protected against unauthorised access, misuse, loss, interference, disclosure, alteration and destruction in a way that is proportionate to their sensitivity, value and risk;
- client safety, privacy, dignity and trust are supported by secure handling of personal and sensitive information;
- SECC can continue delivering critical community services during and after cyber incidents or technology disruptions;
- cyber security risk is managed as an organisational risk, not only as a technical issue;
- staff, volunteers and third parties understand their cyber security responsibilities and report concerns promptly;
- security controls are improved over time using recognised Australian guidance, including the Australian Cyber Security Centre's Essential Eight, where appropriate to SECC's size, risk profile and technology environment;
- SECC complies with applicable legal, regulatory, contractual, funding, privacy and governance obligations.

4. Policy statements

4.1 Information is a valued organisational asset

SECC information must be created, collected, accessed, used, stored, disclosed, archived and destroyed with care. Information must be protected according to its sensitivity, operational value, legal requirements and potential harm if compromised. Client, service-user, child, family, youth, aged-care, domestic and family violence, staff, volunteer, donor and financial information must receive heightened protection.

4.2 Cyber security is a shared responsibility

All authorised users must comply with this policy and related procedures. Users must protect passwords and devices, use approved systems, follow privacy and information-handling requirements, complete required cyber security awareness training, and immediately report suspected cyber incidents, suspicious emails, lost devices, unauthorised disclosure, or weaknesses in security controls.

4.3 Governance and risk management

Cyber security risk must be managed within SECC's broader governance and risk management arrangements. Material cyber security risks must be recorded, assessed, assigned to accountable owners, treated in proportion to risk, and escalated to senior leadership and the Board where they may affect service delivery, privacy, safety, finances, reputation, legal obligations or strategic objectives.

4.4 Access management

Access to SECC systems and information must be granted based on business need, with people given only the level of access they need to perform their role. User access must be approved, recorded, reviewed periodically, and removed or changed promptly when a person changes roles, leaves SECC, completes volunteer duties, or no longer requires access.

4.5 Passwords and authentication

Users must employ strong, unique passwords or passphrases for SECC accounts and must not reuse SECC passwords for personal services. Passwords must not be shared, written in insecure locations, stored in browsers on shared devices, or sent through email or messaging platforms. A SECC-approved password manager may be used where authorised. Administrator credentials must be separately controlled, limited to authorised personnel, and used only for administrative tasks.

4.6 Email, internet and acceptable use

SECC systems must be used in a lawful, ethical and professional manner consistent with SECC's mission, values and service obligations. Users must exercise care with links, attachments, requests for payment, requests to change

bank details, requests for client information, and urgent or unusual instructions. Suspicious emails or messages must be reported using the approved reporting pathway. SECC email and collaboration systems must not be used to store excessive personal information beyond business need or to transfer sensitive information through insecure channels.

4.7 Devices, endpoints and mobile work

SECC-managed devices must be configured securely, patched regularly, protected by endpoint security controls, encrypted where possible, and locked when unattended. Users must take reasonable steps to physically protect laptops, phones, tablets, removable media and paper records, particularly when working remotely, travelling, delivering outreach services, transporting clients, or working in shared community spaces. Lost or stolen devices must be reported immediately.

4.8 Cloud services, applications and data storage

SECC information must be stored only in approved systems and repositories. New cloud services, software, mobile applications, artificial intelligence tools, online forms, databases and collaboration platforms must be assessed before use to ensure that information security, privacy, access control, backup, data ownership, data location, supplier support and exit arrangements are appropriate. Sensitive client information must not be entered into public AI tools or unauthorised online services.

4.9 Data protection, backup and retention

SECC must maintain appropriate backup and recovery arrangements for critical systems and information. Backup arrangements must be protected from unauthorised alteration or deletion and tested periodically. Information must be retained and disposed of in accordance with legal, contractual, operational and records-management requirements. Secure disposal methods must be used for devices, storage media and paper records containing SECC information.

4.10 Vulnerability, patch and configuration management

SECC, with support from its IT provider where applicable, must maintain a practical program for identifying and treating cyber security vulnerabilities. Systems must be patched within timeframes that reflect the severity of the vulnerability, exposure of the system and operational risk. Unsupported software, unsupported devices and insecure configurations must be remediated, isolated, replaced or formally accepted through the exception process.

4.11 Supplier and third-party security

Suppliers that host, process, support or access SECC information must be subject to appropriate due diligence and contractual requirements. Supplier arrangements should address confidentiality, privacy, access control, incident notification, data location, subcontracting, business continuity, backup, audit rights, service availability, secure disposal and return of SECC information at contract end. Suppliers must notify SECC promptly of cyber incidents that may affect SECC systems, information or services.

4.12 Incident management

SECC must maintain a cyber incident response process that enables rapid reporting, triage, containment, investigation, recovery, communication and post-incident improvement. Suspected cyber incidents must be reported immediately to the nominated internal contact or helpdesk. Incidents involving personal information must be assessed for privacy impact and, where applicable, for notification obligations under the Notifiable Data Breaches scheme. Incident records must be retained to support learning, insurance, reporting, legal obligations and continuous improvement.

4.13 Security awareness and training

SECC must maintain a cyber security awareness program that is practical and relevant to community service delivery. Training should address phishing, passwords, multi-factor authentication, safe remote work, privacy, secure handling of client information, scams targeting vulnerable people, safe use of mobile devices, reporting obligations and specific risks faced by staff and volunteers working with families, young people, seniors and people experiencing domestic and family violence.

4.14 Physical security

Physical access to SECC work areas, records, devices, network equipment and storage areas must be controlled according to risk. Visitors must be managed appropriately. Paper records and devices containing sensitive information must not be left unattended in public or shared areas. Printed material must be collected promptly and securely disposed of when no longer required.

4.15 Privacy, dignity and safety by design

Cyber security controls must support SECC's community-service mission and must be implemented in a way that protects privacy, dignity, safety and service continuity. Where services involve vulnerable clients, children, young people, older people, culturally and linguistically diverse communities, carers, or people experiencing domestic and family violence, system design and information-sharing practices must consider the risk of harm that could arise from unauthorised disclosure, unsafe contact, identity exposure or service disruption.

5. Roles and responsibilities

The following responsibilities apply unless superseded by an approved governance document, delegation, contract or position description.

Role	Responsibilities
Board / governing body	Approve or endorse cyber security governance arrangements; oversee material cyber risks; ensure cyber security is considered as part of organisational risk, service continuity, privacy and reputation; support adequate resourcing for proportionate cyber security controls.
Chief Executive Officer and senior leadership	Lead implementation of this policy; assign accountable owners; ensure cyber security risks are visible in organisational risk reporting; approve risk treatment priorities; support a culture where staff and volunteers report cyber concerns without delay.
Policy owner / Privacy Officer / delegated executive	Maintain this policy and related procedures; coordinate privacy and cyber incident assessment; ensure staff awareness activities occur; report significant risks and incidents to senior leadership; coordinate policy exceptions and reviews.
IT managed service provider or internal IT support	Implement and maintain approved technical controls; manage accounts, patching, backups, endpoint protection, system monitoring and recovery activities within agreed service levels; provide technical advice; report incidents and vulnerabilities promptly to SECC.
Managers and program coordinators	Ensure team members, volunteers and contractors understand information-handling and reporting obligations; approve access based on role need; identify service-specific risks; support incident response and business continuity within their programs.
All staff, volunteers, contractors and authorised users	Use SECC systems and information only for authorised purposes; protect passwords and devices; handle information according to sensitivity; complete required training; report suspected incidents, scams, phishing, lost

	devices, unauthorised access or control weaknesses immediately.
Suppliers and third parties	Protect SECC information in accordance with contracts, privacy obligations and this policy; restrict access to authorised personnel; notify SECC promptly of incidents; return or securely destroy SECC information when no longer required.

6. Monitoring and reporting

The effectiveness of this policy and supporting controls will be monitored through proportionate governance, operational and assurance activities. At a minimum:

- material cyber risks will be recorded and reviewed through SECC's organisational risk management process;
- significant cyber incidents, privacy incidents and control weaknesses will be reported to senior leadership and, where material, to the Board;
- access to key systems will be reviewed periodically, with priority given to systems containing client, staff, volunteer, donor, finance or service-delivery information;
- backup and recovery arrangements for critical systems will be tested periodically;
- cyber security awareness completion and incident-reporting trends will be monitored;
- supplier security issues will be reviewed during procurement, contract renewal or following an incident;
- this policy will be reviewed at least annually or earlier following a material cyber incident, significant service change, technology change, legal change or audit finding.

7. Exceptions

Exceptions to this policy may be requested where strict compliance is not technically feasible, would cause disproportionate service impact, or where an alternative control provides an equivalent or better risk outcome. Exceptions must be documented, risk assessed, time limited, assigned to an accountable owner, and approved by the policy owner or delegated authority. High-risk exceptions must be escalated to senior leadership and, where appropriate, the Board. Exceptions must not be used to avoid legal, privacy, safety or contractual obligations.

8. Definitions

Term	Definition
Availability	Information, systems and services are accessible and usable when needed for authorised business purposes.
Confidentiality	Information is protected from unauthorised access, use or disclosure.
Cyber incident	An event that may compromise the confidentiality, integrity or availability of SECC information, systems or services.
Cyber security	Measures that protect information, systems and services from unauthorised access, misuse, interference, loss, disruption, alteration or disclosure.
Information asset	An identifiable collection of information or a resource that supports information use, including records, databases, applications, devices, systems, people, processes and facilities.
Integrity	Information is accurate, complete and reliable and has not been altered without authorisation.
Least privilege	Users are given only the access necessary to perform their authorised role or task.
Multi-factor authentication	Authentication that requires two or more different factors, such as a password plus a code, authenticator app or security key.

Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Sensitive information	A subset of personal information requiring higher protection, which may include health information, case notes, family circumstances, cultural background, vulnerability indicators, safety information and other information requiring special care.
Third party	Any external organisation or individual that provides services to, or accesses information for, SECC, including suppliers, contractors, consultants, partner organisations and technology providers.

9. Related documents and guidance

This policy should be read alongside SECC's approved internal policies, procedures, contracts and governance documents. Relevant external references and guidance include:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles;
- Office of the Australian Information Commissioner guidance on privacy and the Notifiable Data Breaches scheme;
- Australian Cyber Security Centre guidance, including the Essential Eight maturity model;
- Australian Charities and Not-for-profits Commission governance expectations and obligations applicable to registered charities;
- SECC Privacy Policy and client information-handling procedures;
- SECC incident response, business continuity, records management, acceptable use, remote work, volunteer, HR and procurement procedures, where applicable;
- Relevant funding agreements, service standards, insurance requirements and supplier contracts.

10. Document control

Document ID	SECC-CSP-001
Version	1.0
Policy owner	Chief Executive Officer/ delegated Policy Owner
Approval authority	Board or delegated Executive authority
Approval date	28 September 2026
Next review date	12 months from approval, or earlier after a material incident or technology change
Contact email	secc@secc.sydney