Country Universities Centre
NORFOLK ISLAND

Cyber Safety & Security Policy

1. Purpose

The purpose of this Policy is to outline the principles, responsibilities, and processes for ensuring the confidentiality, integrity, and availability of digital information, systems, and networks at the Country Universities Centre Norfolk Island (CUCNI). It aims to safeguard sensitive information, protect against cyber threats, and comply with relevant Australian legal and regulatory requirements.

2. Scope

This policy applies to CUCNI:

- Staff,
- Board members,
- Software and hardware used to store and present information,
- Electronic communication networks.

3. Policy

A. Information Security Principles

All information managed by CUCNI is classified based on its sensitivity to ensure that appropriate levels of protection are applied. Access to information and systems is strictly limited to what is necessary for each user's role, in adherence to the principle of least privilege. Regular risk assessments are conducted to identify potential threats and vulnerabilities, allowing the implementation of effective controls and mitigations. Rather than relying on a formalised framework, CUCNI follows a structured process of ongoing evaluation and refinement to enhance its information security practices, ensuring alignment with industry standards and legal compliance.

B. Data Classification and Handling

To ensure appropriate protection of information, CUCNI classifies data based on its sensitivity and establishes handling protocols for each category:

1. **Public Data**: Information intended for public access, such as marketing materials, which requires minimal security controls.
2. **Internal Data**: Non-public information, such as internal emails and operational guidelines, which requires controlled access.
3. **Confidential Data**: Information that could harm the organisation or individuals if disclosed, such as staff records and financial data, which requires encryption and limited access.
4. **Highly Confidential Data**: Critical data, such as system passwords and legal records, which requires strict access controls, encryption, and multi-factor authentication.

All data must be handled in accordance with these classifications to ensure consistent protection and compliance with regulatory requirements.

C. Responsibilities

All staff are responsible to complete mandatory cyber security training annually. Blue Sky IT are responsible for monitoring CUCNI's systems for vulnerabilities, suspicious activity, and threats, and for taking timely action to address these issues. The Centre Manager is responsible for creating a

culture of cybersecurity awareness, ensuring compliance with all protocols, and updating procedures as significant changes arise in the regulatory or threat landscape.

D. Staff Accountability

CUCNI holds all staff accountable for upholding cybersecurity responsibilities. Staff are informed of these responsibilities during onboarding and through regular updates. System activity is actively monitored to detect and address any issues of non-compliance. Staff may report errors without fear of retribution, enabling corrective action and learning. Deliberate violations of this policy may result in disciplinary action.

E. Awareness and Training

Comprehensive onboarding training is provided to all new staff to familiarise them with CUCNI's cyber security policies and procedures. CUCNI provides periodic refresher training in cyber security to all staff, covering topics such as identifying and avoiding phishing attempts, securing personal and organisational devices, and maintaining strong password practices. Awareness campaigns are conducted periodically to reinforce the importance of cyber vigilance and to update staff on the latest threats and preventative measures. Reminders are given to change passwords regularly and report suspicious activities.

F. Access Management

Login credentials are created and assigned to users, individually wherever possible and sharing of credentials is strictly prohibited to prevent unauthorised access. Multi-factor authentication is mandatory for accessing sensitive systems including Salesforce, Microsoft Office and Xero, providing an additional layer of security beyond passwords. When employment or contractual arrangements end, access to accounts, systems, and data is revoked to prevent further access.

G. Incident Management

CUCNI responds to cyber security incidents promptly to identify, contain, eradicate and recover from cyber incidents. Any suspected or confirmed security breaches, including phishing attempts, malware infections, or unauthorised data access, must be reported immediately to Blue Sky IT and the Centre Manager. A risk incident log is maintained to document incidents and response, which is reviewed by the CUCNI Board to analyse the root causes, identify gaps in existing controls, and implement corrective actions to prevent recurrence.

H. System Maintenance

All software and systems used by CUCNI are supported by Blue Sky IT with the latest security patches and updates to address known vulnerabilities. Where possible and practical regular vulnerability scans are performed to identify and prioritise remediation of potential weaknesses. End-of-life hardware and software are securely decommissioned, with data permanently wiped or destroyed to prevent leaks.

I. Network Security

CUCNI employs firewalls and intrusion detection or prevention systems to safeguard its networks from unauthorised access and malicious traffic. Regular network security audits and penetration tests are conducted to ensure compliance with established security standards.

J. Social Engineering Threat Mitigation

CUCNI is proactive in mitigating the risks of social engineering attacks by implementing targeted strategies. Staff are trained to recognise phishing emails, fraudulent phone calls, and impersonation attempts, equipping them with the skills to respond effectively. Staff are required to report suspected social engineering incidents immediately to their supervisor for immediate investigation and resolution. Verification protocols are strictly enforced for sensitive requests, such as financial transactions or password resets, ensuring additional safeguards against deception-based attacks.

K. Remote Work Security

CUCNI recognises the importance of maintaining cybersecurity for remote work arrangements. Staff wishing to use personal devices for remote work are required to have up-to-date antivirus software, operating system patches, and encryption enabled to protect against vulnerabilities, and connect to CUCNI systems through multi-factor authentication (MFA). Public Wi-Fi networks must be avoided for accessing CUC systems. Sensitive information is prohibited from being stored locally on personal devices unless explicitly authorised, and any authorised data must be promptly removed after use.

L. Compliance

CUCNI strives to continuously improve the maturity level with the Australian Cyber Security Centre (ACSC) Essential Eight Strategies, a set of baseline strategies to mitigate cyber threats. CUCNI ensures compliance with Maturity Level 1 as a minimum. The organisation also adheres to the Notifiable Data Breach scheme under the *Privacy Act 1988* (Cth), which requires the timely notification of individuals affected by eligible data breaches. Periodic audits are performed to confirm adherence to relevant cyber security standards, regulations, and policies.

M. Third-Party Compliance

To safeguard the integrity and security of CUCNI systems, CUCNI regularly monitors and reviews the compliance and performance of its third-party IT provider Blue Sky IT including:

- **Annual Compliance Audits**: Conduct regular audits to ensure adherence to cybersecurity and data protection standards.
- **Security Measures Validation**: Confirm that the provider implements robust security measures, such as:
    - Data encryption for storage and transmission.
    - Multi-factor authentication for system access.
    - Regular penetration testing and vulnerability assessments.
- **Documentation and Reporting**: Require the provider to submit regular compliance reports demonstrating adherence to contractual obligations and industry standards.
- **Issue Resolution**: Address identified risks or vulnerabilities promptly through a structured improvement plan, monitored by CUCNI.
- **Service Agreement Review**: Periodically review and update service agreements to reflect changes in regulatory or organisational requirements.

4. Resources

- Australian Cyber Security Centre - Essential Eight Strategies
- *Cyber Security Act 2024* (Cth)
- *Privacy Act 1988* (Cth)