2.26 Cyber-Security

Effective Date: 29 October 2021
Version 1.0

Industry Standards
National Disability Standards: Standard 6
Attendant Care Industry Standard (2018): Level 2.4
NDIA Practice Standards and Quality Indicator: Core Module 2.4

Purpose

The purpose of this policy is to outline how Community Connections Australia (CCA) will preserve the security of its data and technology infrastructure.

As part of CCA's Information Management System the organisation recognises the importance of maintaining confidentiality for company, personal and staff records (data). All staff members are obligated to protect this information and avoid security breaches.

Policy Statement

Community Connections Australia (CCA) adopts a proactive management approach towards cyber security by providing protection against malicious and accidental threats and is based on the principle that *cyber security is everyone's business*.

Scope

This policy applies to all CCA staff members.

Policy Principles

1. When CCA staff members access their company emails or company accounts (such as Carelink or Xero) they are introducing security risk to CCA's data.

2. To ensure they maintain the highest level of security staff members are to:
   - Keep all devices password protected.
   - Choose and upgrade a complete antivirus software.
   - Ensure they do not leave their devices exposed or unattended.
   - Install security updates of browsers and systems monthly or as soon as updates are available.
   - Log into company accounts and systems through secure and private networks only
   - Avoid using other people's devices or lending their devices to others.
   - Ensure all company information is stored on the secure google storage system and not on their local devices
   - Only install CCA approved software on their workplace device

3. When new staff members join CCA they will be given access to CCA's domain via a ccoz email. They will be required to set up 2 factor authentication for accessing the ccoz email.

4. CCA staff members will keep emails safe by:
   - Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
   - Be suspicious of clickbait titles (e.g. offering prizes, advice.)

- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- using an appropriate disclaimer statements on emails sent from their CCOZ email address

5. If a staff member isn't sure that an email they received is safe, they are to refer the matter to a Senior Manager.

6. CCA staff members will manage passwords properly by:
   - Choosing passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
   - Remembering passwords instead of writing them down. If a staff member needs to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
   - Not sharing passwords with any other person
   - use different passwords for different access to systems

7. Information (data) is to be transferred securely to avoid security risks. Staff members must:
   - Avoid transferring sensitive data (e.g. customer information, staff records) to other devices or accounts unless absolutely necessary.
   - Share confidential data over CCA's network/ system and not over public Wi-Fi or private connection.
   - Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.

8. To reduce the likelihood of security breaches, CCA instructs all staff members to:
   - Turn off their screens and lock their devices when leaving their desks.
   - Report stolen or damaged equipment as soon as possible to a Senior Manager.
   - Change all account passwords at once when a device is stolen.
   - Report a perceived threat or possible security weakness in CCA's systems.
   - Refrain from downloading suspicious, unauthorised or illegal software on their company equipment.
   - Avoid accessing suspicious websites.

9. CCA staff can access personal emails through work devices- this is a privilege and overuse of this will mean the privilege is withdrawn

10. needs to know about scams, breaches and malware so as to better protect its infrastructure. For this reason staff members are to report perceived attacks, suspicious emails or phishing attempts as soon as possible to a Senior Manager who will refer the matter to our IT Department. The matter will be investigated promptly, the issue resolved and a company-wide alert will be sent when necessary.

11. When working at home or remotely CCA staff members must follow this policy's instructions. Since they will be accessing CCA's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Approved: .... Date: October 2021
(Chief Executive)

Refer to CCA Table of Contents for related policies and procedures.

Document History

Note: Reviewed and rewritten policies and procedures took effect on 1st December 2016. For preceding policies and for revision history prior to this date, contact the Company Secretary.

Version Number	Review Date	Revision Details
1	2021	Original Policy *(refer to previous Policy 6.14 and 6.40)*

Next Review Date: October 2024

Definitions

Ensuring you understand and practice good cyber security is the best way to combat cyber threats. Here you will find information about common online security risks, with simple advice on what you can do to protect yourself and your family.

Data spill

Sometimes personal information is released to unauthorised people by accident or as the result of a security breach. For example, an email with personal information can be sent to the wrong person, or a computer system can be hacked and personal information stolen. These are known as data breaches or data spills.

Hacking

Refers to unauthorised access of a system or network, often to exploit a system's data or manipulate its normal behaviour.

Identity theft

When a cybercriminal gains access to your personal information to steal money or gain other benefits. They can create fake identity documents in your name, get loans and benefits or apply for real identity documents in your name, but with another person's photograph.

Malicious insiders

Can be employees, former employees, contractors or business associates who have legitimate access to your systems and data, but use that access to destroy data, steal data or sabotage your systems. It does not include well-meaning staff who accidentally put your cyber security at risk or spill data.

Malware

Malware (short for 'malicious software') is software that cybercriminals use to harm your computer system or network. Cybercriminals can use malware to gain access to your computer without you knowing, in targeted or broad-based attacks.

Phishing – scam emails

A way that cybercriminals steal confidential information, such as online banking logins, credit card details, business login credentials or passwords/passphrases, by sending fraudulent messages (sometimes called 'lures').

Ransomware

A type of malicious software (malware) that makes your computer or its files unusable unless you pay a fee. It can get onto your device in the same way as other malware or a virus.

Scams

Online scams are sophisticated messages, often using professional-looking brands and logos to look like they come from a business you already know. This can make it difficult at first sight to know what is real and what is fake.