RAWCS Cyber Security Policy

JUNE 2024

Table of Contents

1. Introduction

1.1 Who we are

1.1.1 Rotary Australia World Community Service Ltd (RAWCS) is a registered charity with the Australian Charities and Not-for-profits Commission (ACNC). We back doing good by supporting and facilitating a broad range of humanitarian and development projects, both in Australia and in developing countries. RAWCS administers three Tax Deductible funds:

1. **Rotary Australia Overseas Aid Fund (RAOAF):** This fund supports efforts by Rotary Clubs, Rotary Districts and other partners to deliver humanitarian assistance in developing countries. RAOAF focuses on both sustained development and immediate disaster response, working collaboratively with communities to deliver impactful, sustainable projects to meet identified needs.
2. **Rotary Australia Benevolent Society (RABS):** RABS supports Rotary Clubs, Rotary Districts and other partners to respond to specific community challenges within Australia. It offers an avenue for wider community involvement through tax-deductible donations. The Rotary Australia Compassionate Grants Projects within RABS uses matching funds from donations, such as those provided by Dick Smith's Trust, to assist Australians facing hardship.
3. **Rotary Australia Relief Fund (RARF):** This fund is dedicated to responding to national appeals and efficiently disbursing funds to appropriate aid projects. RARF's focus is on mobilising rapid support during national crises, such as natural disasters, providing a structured channel for public generosity to be transformed into effective aid. This fund acts as a hub for contributions from both Rotary and non-Rotary sources, ensuring swift and effective aid delivery to disaster-affected areas.

1.2 Purpose

1.2.1 The purpose of this policy is to ensure the security, integrity and protection of our computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

1.3 Scope and Governance

1.3.1 This policy applies to RAWCS and all of its administered funds and subsidiaries – referred inclusively within this policy as RAWCS.

1.3.2 This policy applies to all IT systems and websites of RAWCS, and to all users of these systems and websites, including RAWCS staff, volunteers, Board members, committee members, suppliers, donors and contractors. Within this policy all of these are represented by the term: "**users**".

1.3.3 Users must comply with all applicable laws and regulations, including but not limited to copyright laws, software licensing agreements, and data protection regulations.

1.3.4 This policy and its obligations extends to any persons who visit our premises, programs or activities within Australia and overseas.

1.4 Policy References

This policy supports our compliance with the following:

- *Privacy Act 1988* (Cth)
- Australian Privacy Principles, schedule 1 to the *Privacy Act 1988* (Cth)
- *Health Records and Information Privacy Act 2002* (NSW)
- Data Provisions Requirements 2010 (Cth)
- *Freedom of Information Act 1982*
- State and Territory Privacy Laws and Principles; State based Health Privacy Laws
- ACNC Governance Toolkit: Cyber Security
- ACFID Code of Conduct
- RAWCS Code of Conduct
- RAWCS Complaint Handling Policy and Procedure
- RAWCS Whistleblower Policy and Procedure

1.5 Definitions

Term	Definition
Cyber Security	An overarching term that captures the steps, measures and processes used to protect and defend the confidentiality, integrity, availability of data in an organisation's systems as well as protecting the systems themselves.
Cyber Risk	The potential loss or harm to an organisation from a cyber incident. The loss covers technical systems and infrastructure, use of technology or reputation of an organisation.
Cyber Resilience	An organisation's posture or ability to defend, adapt respond and recover from cyber threats and cyber incidents while maintaining continuous business operations. Cyber resilience includes the cyber culture of an organisation and how directors and employees take individual steps to build cyber resilience.
User	A person, organisation, or other entity which requests access to, and uses the resources of a computer system or network.
Personal Information	Information or an opinion about an identified person (or a person that can reasonably be identified), regardless of whether the information or opinion is true or recorded in a material form.
Sensitive Information	A subset of personal information, and may include, for example, a person's religious or philosophical beliefs, sexual orientation or health information.
Cyber Incident	An unauthorised cyber security event, or a series of such events, that has the potential to compromise an organisation's business operations. Cyber incidents cover the spectrum of events from accidental data losses, such as an employee misplacing a USB, to criminal attacks, issue motivated groups and state sponsored actors.
Data Breach	A data breach happens when personal information is accessed and/or disclosed without authorisation or is lost. For example, when: • a USB or mobile phone that holds an individual's personal information is lost or stolen; • a database containing personal information is hacked; • someone's personal information is sent to the wrong person.

Notifiable Data Breaches Scheme	Any organisation or agency the *Privacy Act 1988* covers must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved. Examples of serious harm include: • identity theft, which can affect your finances and credit report; • financial loss through fraud; • a likely risk of physical harm, such as by an abusive ex-partner; • serious psychological harm; • serious harm to an individual's reputation.
Phishing Scam	An attempt by scammers to trick you into giving them your personal information, such as your bank account details or passwords.

2. Principles

2.1 Guiding Principles

2.1.1 **Govern:** Identifying and managing security risks.

2.1.2 **Protect:** Implementing controls to reduce security risks.

2.1.3 **Detect:** Detecting and understanding cyber security events to identify cyber security incidents.

2.1.4 **Respond:** Responding to and recovering from cyber security incidents.

3. Policy Commitments

3.1 Security and Access

3.1.1 RAWCS is committed to maintaining the highest standards of IT and website security, and to comply with all relevant laws, regulations, and contractual obligations. We will implement appropriate technical, physical, and administrative measures to prevent, detect, and respond to IT and website security incidents, and to minimise the impact and risk of such incidents.

3.1.2 Users must keep passwords secure. Accounts must not be shared, and no other people may be permitted to use the account. Passwords should not be readily accessible in the area of the computer concerned. Authorised users are responsible for the security of their passwords and accounts.

3.1.3 Access to sensitive information should be on a need-to-know basis. Users are only authorised to access data and systems required for their role responsibilities. RAWCS will keep, at all times, an up to date register containing access information of each individual.

3.1.4 Attempting to access unauthorised areas of the IT systems or using another user's account without permission is strictly prohibited.

3.1.5 User log-on IDs and passwords will be deactivated as soon as possible if person is no longer engaged or employed by RAWCS.

3.1.6 Users must use extreme caution when opening email attachments received from unknown senders; these may contain viruses, malware or Trojan horse code.

3.1.7 Users who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their manager/supervisor immediately. The user shall not turn off the computer or delete suspicious files.

3.1.8 Users must not themselves breach security or disrupt network communication on the RAWCS systems or elsewhere. Security breaches include accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties.

3.2 Data Protection

3.2.1 Users must respect the privacy of sensitive and confidential information. Unauthorised disclosure or sharing of such information is prohibited.

3.2.2 All critical business data must be regularly backed up. Users are responsible for ensuring their data is stored in approved locations.

3.3 Software and Hardware

3.3.1 Only authorised IT personnel may install software on company systems. Users must not install unauthorised software.

3.3.2 RAWCS hardware is to be used for business purposes only. Personal devices should not be connected to company networks without approval.

3.3.3 Computers being deaccessioned (whether for sale, reuse or disposal) shall not be released until all data has been securely deleted.

3.4 Internet and Email

3.4.1 Internet access is provided for business purposes. Users should refrain from accessing inappropriate or non-business-related websites.

3.4.2 Users shall not download unauthorised software from the internet onto their PCs or workstations

3.4.3 Use the RAWCS email responsibly. Avoid sending confidential information via unsecured channels and be cautious of phishing attempts.

3.5 Cyber Risk Management

3.5.1 We shall ensure cyber security strategy and risk management are standing items for RAWCS board meetings.

3.5.2 The Website and Technology Committee shall provide advice to the Board on all matters related to the website, networking and associated computer technology.

3.5.3 Our Response Plan in the event of a cyber security incident and/or data breach is at Appendix 1

3.6 Training

3.6.1 RAWCS will provide regular training and awareness programs to its users on IT and website security best practices and responsibilities.

4. CONSEQUENCES OF VIOLATION

4.1 RAWCS reserves the right to monitor and audit the use and activity of its IT systems and website, and to investigate any suspected or reported breaches of this policy or the related procedures and guidelines.

4.2 Violations of this policy may result in disciplinary action, including but not limited to warnings, suspension, or termination. Legal action may be taken in cases of severe violations.

5. Roles and Responsibilities

Roles	Responsibilities
National Board of Directors	• Ultimate accountability for our organisational policies • Guiding governance and culture of RAWCS through strategic leadership • Approving this policy and holding the Chief Executive Officer (CEO) accountable to how effectively this policy is implemented. • Ensuring appropriate systems are in place to bolster cyber resilience and respond to cyber incidents.
Website and Technology Committee	• Provides advice to the Board on all matters related to the website, networking and associated computer technology. • Reviews and recommends to the Board, management strategies relating to website technology and their alignment with RAWC's overall strategy and objectives. • Reviews and monitors strategies for developing or implementing new technologies and systems. • Reviews and monitors the effectiveness of the IT Risk Management and Security plans and include advising the Board Audit and Risk Management Committee on matters of Technology Risk and Security.
CEO	• Ensuring that our people are aware of this policy • Advising the board breaches of this policy and ensuring any breaches are dealt with appropriately • May authorise individuals with responsibility for cyber security issues in RAWCS to monitor the organisation's equipment, systems and network traffic at any time for security and network maintenance purposes.
IT Manager	• Responsible for overseeing and managing the IT and website security of RAWCS, and for implementing and enforcing this policy.

National Manager Projects & Volunteers	• Ensuring all project participants are aware of, and comply with this policy. • Fostering a culture of integrity by actively promoting and supporting whistleblowing channels to report unethical behaviour or policy violations.
All our People	• Ensuring that your actions are in line with this policy. • Not encouraging others (directly or indirectly) to breach this policy. • Reporting any breach to your manager/supervisor.

6. Policy Distribution

6.1 This policy will be available on our website and disseminated to all our people, visitors and partners.

6.2 We will ensure that all our people, visitors and partners are notified of and made aware that they are required to comply with the policy.

7. Review

7.1. We are committed to continuous improvement to our policy, procedures and practices. This policy will be reviewed at least every three years by the CEO and approved by the National Board of Directors to ensure it is working in practice and updated to accommodate changes in legislation or circumstance.

7.2 Feedback on this and other safeguarding policies is openly encouraged from our people, partners, stakeholders and the communities we work with. Feedback, as well as emerging good practice and collaborative lessons learnt across the development sector, will be used to strengthen this and related policies and procedures.

8. More information

8.1. If you have a query about this policy or need more information, you can contact us via:

- email: info@rawcs.org.au
- phone: +61 2 8833 8306
- post: Rotary Australia World Community Service Ltd
  25/1 Maitland Place
  Maitland Place
  Norwest NSW 2153
  Australia

Name	**Policy Template**
Policy Category	**Board**
Version Number	**Version 1**
Approval Date	**20 July 2024**
Details of Approval Authority	**National Board of Directors**
Policy Owner	**CEO**
Frequency of Review	**3 years**
Next Review Date	**20 July 2027**

Document Revision History

Version	Date	Author	Description

Appendix 1: Responding to a data breach

A data breach is when protected information is accessed or disclosed without authorisation.

Step	Action	Person responsible
1. Identify	Report the actual or suspected data breach immediately to the CEO.	The individual who discovers the actual or suspected breach.
	Decide whether an actual or suspected data breach has occurred. [Use the OAIC guide to identify if an eligible data breach has occurred or not].	IT Manager and/or CEO
	Appoint someone as the response co-ordinator if an actual data breach has occurred.	IT Manager and/or CEO
	The individual who discovered the breach should take note of the following details, and pass the information to the co-ordinator: • The time and date of the actual or suspected data breach • The type of information involved • Ways the data breach can be contained	The individual who discovers the actual or suspected breach.
2. Investigate	Investigate the breach and assess: • The information involved in the data breach; • The cause of the breach; • The extent of the breach; • People who have been, or may be, affected; • The extent of the harm; • The need to notify the people affected, and what information they need to know.	IT Manager or CEO or appointed independent investigator

Step	Action	Person responsible
3. Assess	Assess each threat identified from the breach based on the information gathered during the investigation. This assessment should consider whether: • there has been any loss, misuse or disclosure of information; • there is a risk of harm to individuals because of the breach (for example, has it revealed personal or sensitive information?); • actions have been taken to reduce the risk of harm; • there is a need to notify affected people or relevant regulators	IT Manager/CEO/appointed Investigator
	Record the details of the assessment and keep it filed (physically or electronically). Make sure people who need to see it get a copy or can access it easily.	IT Manager/CEO/ appointed Investigator
4. Notify	Notify the affected people, organisations and regulators. Consider whether: • The notification needs to happen within a set timeframe • The notification needs to be in a particular format (for example, an email or a letter) • Your charity wants to publish a public notification on its website or social media pages	CEO
5. Review	Review the data breach and the response. Record the findings and make a list of recommendations for improvements. Make sure the review covers the following: • an understanding of how the breach occurred; • updates to processes for managing information and data to prevent another breach occurring; • updates to systems or technology if the breach was due to a technical vulnerability; • updates to other relevant policies and procedures to reflect changes; • user training for dealing with the private and confidential information	IT Manager and CEO