ROTARY AUSTRALIA WORLD COMMUNITY SERVICE

IT & Website Security Policy

Purpose

The purpose of this policy is to ensure the security and integrity of the IT systems and websites of RAWCS, and to protect the data and information of RAWCS, its staff, volunteers, Rotarians, Rotary clubs and districts, and other stakeholders from unauthorized access, use, modification, disclosure, or destruction.

Scope

This policy applies to all IT systems and websites of RAWCS, and to all users of these systems and websites, including directors, employees, volunteers, consultants, contractors, partners, donors, and visitors.

Policy Statement

RAWCS is committed to maintaining the highest standards of IT and website security, and to comply with all relevant laws, regulations, and contractual obligations. RAWCS recognizes the importance of safeguarding the confidentiality, integrity, and availability of its IT systems and website, and the data and information stored or processed on them.

RAWCS will implement appropriate technical, physical, and administrative measures to prevent, detect, and respond to IT and website security incidents, and to minimize the impact and risk of such incidents. RAWCS will also provide regular training and awareness programs to its users on IT and website security best practices and responsibilities.

RAWCS will maintain the access of all managers, supervisors and Rotary personnel to their areas of responsibility on our websites but will endeavour to restrict access to essential personnel only. Access must be granted to ensure RAWCS can operate efficiently but is also aware our sites need to be as secure as we can be.

Roles and Responsibilities

All users of RAWCS IT systems and website are responsible for complying with this policy and the related procedures and guidelines. Users must:

- Use the IT systems and website only for authorized purposes and in accordance with the RAWCS Code of Conduct – Directors, RAWCS Code of Conduct – Other Personnel and RAWCS Fraud Control and Corruption Policy.
- Protect their login credentials and devices from unauthorized access or use and report any suspected compromise or loss immediately to the IT Manager.
- Use strong and unique passwords and change them regularly or when prompted by the system.
- Use secure and encrypted communication channels, such as VPN, SSL, or HTTPS, when accessing or transmitting sensitive or confidential data or information.
- Avoid opening or downloading any suspicious or unsolicited emails, attachments, or links, and report any phishing or malware attempts to the IT Manager.
- Follow the backup and recovery procedures for their data and information and store them in the designated locations or systems.
- Report any IT or website security incidents or vulnerabilities to the IT Manager as soon as possible and co-operate with the investigation and resolution process.

IT Manager

The IT Manager is responsible for overseeing and managing the IT and website security of RAWCS, and for implementing and enforcing this policy and the related procedures and guidelines. The IT Manager must:

- Maintain an inventory of all IT systems and website assets and classify them according to their sensitivity and criticality.
- Ensure that RAWCS websites are made as secure as possible by only allowing access to essential users of each site.
- Conduct regular risk assessments and audits of the IT systems and website and identify and address any security gaps or weaknesses.
- Implement and maintain appropriate security controls and tools, such as firewalls, antivirus, encryption, backup, authentication, authorization, logging, monitoring, and alerting.
- Establish and test the incident response and disaster recovery plans for the IT systems and website and co-ordinate the response and recovery activities in the event of an incident.
- Provide regular training and awareness programs to the users on IT and website security best practices and responsibilities.
- Review and update this policy and the related procedures and guidelines periodically, or when there are significant changes in the IT systems and website or the security environment.

Compliance and Enforcement

Any user who violates this policy or the related procedures and guidelines may face disciplinary action, up to and including termination of employment or contract, suspension or revocation of access rights, legal action, or referral to law enforcement authorities. 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.

Review and Approval

This policy and the related procedures and guidelines will be reviewed and approved by the RAWCS Board of Directors annually, or as required. Any changes or amendments to this policy or the related procedures and guidelines will be communicated to all users and stakeholders.