CYBERSECURITY IN THE WORKPLACE

POLICY NUMBER: NDIS GOV 29

INTENT

The intent of this policy is to establish clear principles and procedures to protect Real Living Options Association Inc's digital systems, networks, devices, and data, particularly personal and sensitive information of NDIS Participants and employees, from cyber threats, data breaches, and unauthorised access.

DEFINITION

Cybersecurity: *Protection of internet-connected systems (hardware, software, data) from cyber threats*

Personal information: *Data that identifies or could identify an individual (e.g. name, address, NDIS number)*

Sensitive information: *Information about a person's health, disability, or support needs*

Data breach: *Unauthorised access to, disclosure of, or loss of personal or sensitive information*

POLICY STATEMENTS

- Real Living Options Association Inc. is committed to ensuring as far as practicable:
    - The confidentiality, integrity, and availability of organisational data.
    - Complying with the Privacy Act 1988 (Cth), Australian Privacy Principles (APPs), and NDIS Practice Standards
    - Maintaining a risk-based, proactive approach to cybersecurity
    - Educating staff and volunteers on safe digital practices
    - Responding quickly and transparently to cybersecurity incidents

PROCEDURES

- Access to systems and data is provided based on roles and responsibilities.
- Multi-factor authentication (MFA) must be used for cloud systems and sensitive applications.
- Shared accounts are prohibited unless explicitly approved with secure controls.
- Organisation-issued devices must have antivirus software, firewalls, and security patches updated regularly.
- Devices must be locked or logged out when unattended.
- Participant data must only be accessed, used, and stored as necessary for the delivery of service.
- Cloud storage providers must be based in Australia or meet Australian data protection requirements.
- Staff must not open suspicious attachments or click on unknown links.

- Use only approved email accounts for communication with Participants or stakeholders.
- Only authorised software may be installed or used.
- Software and operating systems must be updated regularly to protect against vulnerabilities.
- Office staff will receive cybersecurity training including:
    - Password safety
    - Phishing awareness
    - Privacy obligations
    - How to report a suspected breach
- All suspected or actual cybersecurity incidents must be reported immediately to the General Manager. These may include:
    - Loss or theft of a device
    - Unauthorised access to systems or files
    - Phishing or hacking attempts
    - Accidental email of participant data to the wrong recipient
- In the event of a breach, the following response must be followed:
    - Identify and contain the breach.
    - Assess the risk and potential harm.
    - Notify affected individuals, the NDIS Commission, and the Office of the Australian Information Commissioner (OAIC) if applicable.
    - Investigate root cause and take corrective actions.
    - Record the incident and review procedures.

DELEGATIONS

Management Committee

- Monitor risk exposure and ensure resources are allocated to manage cyber risks.
- Ensure notification to the NDIS Commission and other regulators if a significant incident occurs.

General Manager

- Oversee the implementation of cybersecurity procedures.
- Ensure all office staff receive cybersecurity training.
- Manage contracts and agreements with IT vendors and cloud providers.
- Ensure compliance with regulatory reporting obligations.

All Staff

- Follow cybersecurity procedures at all times.
- Report suspicious activity or data breaches immediately.
- Use work devices and platforms securely and professionally.
- Maintain strong passwords and do not share login credentials.

RELATED DOCUMENTATION

NDIS Code of Conduct
NDIS GOV 20 Use of AI in the Workplace
NDIS SER DEL 7 Privacy, Dignity and Confidentiality

REFERENCES

Privacy Act 1988 (Cth)
NDIS Act 2013
NDIS (Provider Registration and Practice Standards) Rules 2018
Australian Cyber Security Centre (ACSC) Guidelines

AMENDMENTS/REVIEWS