NATIONAL DISABILITY COUNCIL

Information security

Introduction

Information security is important as we handle, transmit and store personal information on a daily basis. Under privacy laws, we are required to take reasonable steps to keep all personal information accessed safe from accidental or deliberate misuse. This policy aims to safeguard our information and our ICT (information and communications technology) resources from those with malicious intent.

Applicability

When

- Applies to all information and communications technology (ICT) used by the organisation including computers, computer networks, internet connections, smart phones and email
- Applies when unsolicited phone calls, emails or text messages are received.

Who

- Applies to all representatives including key management personnel, directors, full time workers, part time workers, casual workers, contractors and volunteers.

Personal information

All personal information, including that of participants and workers, must be:

- Stored securely with reasonable security precautions against misuse or unauthorised access (e.g. electronic information should be password protected, hard copies stored under lock and key)
- Readily accessible but only on a need-to-know basis
- Retained for the required time (7 years)
- Destroyed securely when no longer required
- Not shared with any third parties without correct consent.

General information security precautions

The following are recommended precautions for helping to keep information secure:

- Access to all personal information is strictly based on a need-to-know basis
- When sending group emails, use the ‘BCC’ field rather than the ‘To’ field so email recipients cannot see other recipients’ email addresses
- Always password lock computers when unattended (shortcut to password lock a Windows computer is “Windows key + L”)
- Operating system updates (also called "patches") must be installed promptly after they become available
- Active anti-virus software must be installed and kept up-to-date on all computers
- Internet modem routers must have security (i.e. firewall) enabled
- Internet modem routers and network security cameras must have a strong admin password
- WiFi networks must have strong passwords to gain access
- Only download or install software from trusted sources

- Mail servers should be configured to use encryption
- Computers should be configured so admin rights are restricted to key management personnel (i.e. so workers can't install software)
- When an employee leaves, their access to the organisation's computer network and email systems is removed promptly.

Passwords

Passwords are important for information security. The following are best practices for passwords:

- All computers which store or access personal information require unique and strong passwords to gain access
- Passwords must not be shared or reused between computers, users, or different applications (e.g. password for Facebook should be different to the password for Google mail which should be different to the computer login password)
- Passwords should not be left written on paper left lying around
- Passwords should be regularly changed i.e. every three months
- Always use strong passwords with a minimum of 8 characters which include a combination of:
    - Lower case letters (abcdefghijklmnopqrstuvwxyz)
    - Upper case letters (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
    - Numbers (1234567890)
    - Symbols (!@#$%^&*()-=_+,.<>/?'"[]{}|\` ~:;'")
- Do not use easy-to-guess passwords such as "123456", "password" or "qwerty" etc.

Avoiding scams and ransomware

To avoid being the victim of scams and ransomware:

- Do not pay the ransom if your computer is infected with ransomware
- Be aware of current scams targeting individuals and businesses by following government sites such as SCAMWATCH
- Be suspicious of any unsolicited emails or text messages purporting to be from government agencies, banks, delivery services or other similar organisations—check the sender's email address for clues (scammers will try to fool you with a very similar email sender's address) and delete any suspicious emails or look up the organisation's main phone number and call if unsure
- Be suspicious of unsolicited phone callers purporting to be from Telstra, Microsoft, the Australian Tax Office and do not provide any information, instead end the call—if unsure, look up their main number and call it to confirm
- Do not allow remote access to any computer or network resource by a third party unless it is arranged with a known and trusted IT services provider.

Portable devices

As a guide for portable device security:

- Do not leave smart phones and mobile computers unattended in public
- Do not leave smart phones and mobile computers in vehicles (locked or unlocked)
- Do not store smart phones and mobile computers in checked-in baggage when flying
- Check portable storage devices (e.g. USB drives, USB flash drives) for viruses prior to using them
- Use password protection on portable storage devices if they are used to store any personal information (such as employee or participant information).

Social media

As a guide for good social media practices:

- Only those authorised to do so should represent the organisation on social media
- Personal information and confidential company information must not be posted or shared on social media
- When an employee leaves, their access to the organisation's social media must be promptly removed.

Printed material

As a general rule:

- Personal information in printed format must be stored securely when not being used
- Personal information in printed format must not be left lying around
- When no longer required, printed material that contains personal information must be shredded or removed by a secure document destruction service.

Incidents

A data breach or breach of privacy and confidentiality is an incident, follow the Manage incident internally process to manage and resolve the incident.

Incidents where individuals are at serious risk of harm as a result of the breach must be advised of the breach and assisted with ways to reduce their risk of harm from the breach.

Incidents where individuals are at serious risk of harm as a result of the breach are reportable to the Office of the Australian Information Commissioner.