Information Security Policy

Last edited: 28 December 2019 11:05 AM

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.

Definitions

Term	Definition
adware	Software that automatically displays or downloads advertising material such as banners or pop-ups.
backdoor	A technique to bypass a computer system's security undetected in order to access a computer or its data.
bot (malicious bot)	Self-propagating malware that infects its host and connects back to a central computer. Malicious bots can then be used to spy on user activity, steal passwords, relay spam, open backdoors, or perform attacks on other computers, websites or resources.
data breach	An incident where personal and/or sensitive information has been accidentally or deliberately accessed and/or disclosed in an unauthorised fashion. Some common examples of data breaches include: • personal information accidentally mailed or emailed to the wrong recipients • a locked filing cabinet containing personal files is broken into or left unlocked and accessed by unauthorised persons • a computer or storage device used to store personal information is compromised as a result of a security breach, malware or poor security practices • personal information in printed form or on an insecure storage device is left in a public place • personal information accidentally or deliberately shared on social media.

malware	Software which is specifically designed to disrupt, damage, or gain authorised access to a computer system. Includes viruses, ransomware, spyware, adware and other.
patch	See "update".
phishing	Fraudulent emails purporting to be from reputable companies sent to fool users into revealing personal information such as passwords, bank account details or credit card numbers.
ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
spam	Also known as junk email, spam is unsolicited email usually to containing advertising, malware, or phishing.
update (or patch)	An update to a computer, tablet or smart phone operating system usually to correct security flaws (vulnerabilities) or correct errors.
virus	A type of malicious software that installs without the user knowing. A virus can replicate itself, modify computer programs, corrupt data, open backdoors, or install adware, bots or ransomware.
vulnerability	A flaw in a system that can leave it open to attack.

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.

Documents relevant to this policy

Privacy Act 1988 (Cth)

1.0 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.

2.0 General information security precautions

- 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.

3.0 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.

4.0 Avoiding 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.

5.0 Portable devices

- smart phones and mobile computers must not be left unattended in public
- smart phones and mobile computers must not be left in vehicles (locked or unlocked)
- smart phones and mobile computers must not be stored in checked-in baggage when flying
- portable storage devices (e.g. USB drives, USB flash drives) should be vetted and checked for viruses prior to their use
- portable storage devices require password protection if they are used to store any personal information (such as employee or participant information).

6.0 Social media

- 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.

7.0 Printed material

- 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.

8.0 Incidents

- a data breach or breach of privacy and confidentiality is an incident, follow the Manage incident 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.

9.0 Policy Version and Review Date

Version issue date:	28-12-2019
Policy owner:	Complex Behaviour Change Pty Ltd
Approval authority:	CBC Project Lead - NDIS Sandra Kay
Original approval date:	04 Feb 2019
Review date:	28-12-2021