Policy Bank

INSTITUTE OF COMMUNITY DIRECTORS AUSTRALIA
Knowledge Connections Credentials

ourcommunity.com.au
Where not-for-profits go for help

Cyber Security Policy

Last updated April 2015

Policy number	[insert number]	Version	[insert number]
Drafted by	[insert name]	Approved by Board on	[insert date]
Responsible person	[insert name]	Scheduled review date	[insert date]

1. Introduction

1.1 While [Organisation] wishes to foster a culture of openness, trust, and integrity, this can only be achieved if external threats to the integrity of the organisation's systems are controlled and the organisation is protected against the damaging actions of others

2. Purpose

2.1 This policy sets out guidelines for generating, implementing and maintaining practices that protect the organisation's cyber media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

2.2 This policy applies to employees, contractors, consultants, and volunteers at [Organisation], including all personnel affiliated with third parties, to all equipment owned or leased by [Organisation], and to all equipment authorised by [Organisation] for the conduct of the organisation's business

3. Policy

3.1 While [Organisation] wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the organisation's systems remains the property of [Organisation]. Because of the need to protect [Organisation]'s network, the confidentiality of information stored on any network device belonging to [Organisation] cannot be guaranteed, and [Organisation] reserves the right to audit networks and systems periodically to ensure compliance with this policy.

3.2 Information in the possession of the organisation shall be classified into different grades depending on its degree of confidentiality. Particularly sensitive information will receive special protection.

3.3 Employees and volunteers will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

3.4 Breach of this policy by any employee may result in disciplinary action, up to and including dismissal.

Policy Bank

INSTITUTE OF COMMUNITY DIRECTORS AUSTRALIA
Knowledge Connections Credentials

ourcommunity.com.au
Where not-for-profits go for help

Cyber Security Procedures

Procedure number	[insert number]	Version	[insert number]
Drafted by	[insert name]	Approved on	[insert date]
Authorised person	[insert name]	Scheduled review date	[insert date]

1. Responsibilities

1.1 It is the responsibility of the CEO to ensure that:

- staff are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately;
- a cyber security officer is appointed.

1.2 It is the responsibility of the cyber security officer to ensure that:

- the CEO is kept aware of any changes to the organisation's cyber security requirements;
- a report on the organisation's cyber security is submitted annually to the board.

1.3 It is the responsibility of all employees and volunteers to ensure that:

- they familiarise themselves with cyber security policy and procedures;
- their usage of cyber media conforms to this policy.

1.4 In the event of any uncertainty or ambiguity as to the requirements of the cyber security policies or procedures in any particular instance, employees and volunteers should consult their supervisor.

2. Processes

Monitoring

2.1 The CEO may authorise individuals with responsibility for cyber security issues in the organisation, including the cyber security officer, to monitor the organisation's equipment, systems and network traffic at any time for security and network maintenance purposes.

Confidentiality

2.2 Following consultation with the cyber security officer, the CEO shall from time to time issue cyber security procedures appropriate to different levels of confidentiality.

2.3 The organisation shall classify the information it controls in the organisation's computer system files and databases as either non-confidential (open to public access) or confidential (in one or many catogories).

2.4 The cyber security officer is required to review and approve the classification of the information and determine the appropriate level of security that will best protect it.

System taxonomy

Security level	Description	Example
Red	This system contains confidential information – information that cannot be revealed to personnel outside the company. Even within the company, access to this information is provided on a "need to know" basis.The system provides mission-critical services vital to the operation of the business. Failure of this system may have life-threatening consequences and/or an adverse financial impact on the business of the company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information
Green	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access server and application(s). Management workstations used by systems and network administrators.
White	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
Black	This system is externally accessible. It is isolated from RED and GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public web server with non-sensitive information.

Data taxonomy

Security level	Description	Example

Red	Client data allowing financial exploitation or identity theft Organisation data allowing banking or financial exploitation	Client credit card and banking data Organisational credit card and banking data Client details that would facilitate phishing
Green	Client data allowing address or email exploitation Organisational intellectual property that has financial or reputational consequences	Addresses that would facilitate spamming Information that the organisation sells Internal emails
Black	Publicly accessible data	Non-sensitive information

Access control

2.5 Individuals shall be assigned clearance to particular levels of access to the organisation's information resources, and shall access only those recourses that they have clearance for. Access control shall be exercised through username and password controls.

Computer security

2.6 All PCs, laptops and workstations should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

2.7 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.

2.8 System level passwords should be changed quarterly; user level passwords should be changed every six months. User accounts will be frozen after three failed log-on attempts. Log-on IDs and passwords shall be suspended after 30 days without use.

2.9 Users who forget their password must call [the IT department] to get a new password assigned to their account. The user must identify themselves by [e.g. employee number] to [the IT department].

2.10 Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorised users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

2.11 Users will not be allowed to log-on as system administrators. Users who need this level of access to production systems must request a special access account as outlined elsewhere in this document.

2.12 Employee log-on IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the organisation. Supervisors/managers shall immediately and directly contact the IT manager to report change in employee status that require terminating or modifying employee log-on access privileges.

2.13 Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the company and require the permission of the organisation's cyber security officer. Monitoring of the special access accounts shall be undertaken via the periodic generating of reports to the cyber security officer showing who currently has a special access account, for what reason, and when it will expire. Special accounts will expire in 30 days and will not be automatically renewed without written permission.

2.14 All computers and devices used by the user that are connected to the [Name of Organisation] internet/intranet/extranet, whether owned by the user or [Name of Organisation], shall be continually executing virus-scanning software with a current virus database approved by the cyber security officer.

2.15 Malware protection software must not be disabled or bypassed, nor the settings adjusted to reduce their effectiveness.

2.16 Automatic daily updating of the malware protection software and its data files must be enabled.

2.17 All email attachments must be scanned. All documents imported into the computer system must be scanned. Weekly scanning of all computers should be enabled

2.18 A record of the antivirus and anti-malware software should be kept.

2.19 Desktop computers in areas of public access should be physically secured by cables and padlocks.

2.20 Where possible, sensitive data should not be removed from the organisation's premises without specific authorisation.

2.21 Where this is not feasible, data on laptops that may leave the organisation's premises should be protected by full disk encryption.

2.22 Alternatively, staff who need access to sensitive data offsite should be given remote access privileges subject to adequate safeguards.

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

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

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

2.26 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 [organisation designee] immediately. The user shall not turn off the computer or delete suspicious files.

2.27 Users must not themselves breach security or disrupt network communication on the organisation's 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. "Disruption" includes network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

2.28 Users shall not attach unauthorised devices to their computers unless they have received specific authorisation from their manager or the company IT designee.

Optional

2.29 Only authorised devices may be connected to the organisation's network(s). Authorised devices include PCs and workstations owned by company and compliant with the configuration guidelines of the company. Authorised devices also include network infrastructure devices used for network management and monitoring.

2.30 Users shall not attach to the network non-company computers that are not authorised, owned or controlled by company.

2.31 Users shall not attach to the network any unauthorised storage devices; e.g. thumb drives, writable CDs

3. Related Documents

- Confidentiality Policy
- Acceptable use of Electronic Media Policy
- Technology Procedures Manual

Policy Bank

INSTITUTE OF COMMUNITY DIRECTORS AUSTRALIA
Knowledge Connections Credentials

ourcommunity.com.au
Where not-for-profits go for help

About this document

This policy sample has been developed by the Institute of Community Directors Australia (ICDA) and is free for any not-for-profit organisation to download and use, so long as it is for a non-commercial purpose and that the organisation is not paying a consultant to carry out this work. Click here for our full copyright guidelines.

Important notes

You can't (or shouldn't) rely on these sample policies and procedures alone. They're a starting point, but you will have to adapt them to suit your own language and requirements.

Most samples include both policies and procedures (the policies provide guidance on standards, while procedures give instructions on implementing standards). We recommend adopting policies at a board level, while procedures can be developed/signed off by the organisation's CEO.

We use the term 'board' to cover boards, committees of management, or anybody that has final authority in your organisation. And the term 'CEO' extends to executive directors, or your chief administrator. You should change the terms in these policies to match those used in your organisation.

Other policies

There are numerous policies available on the Community Directors website. You can hunt for what you need with our site search function.

Make a deposit

If you have some great policies that your organisation thinks would be of use to other groups, email them to service@ourcommunity.com.au. We'll review them, amend them so that they're applicable to the greatest number of not-for-profits possible, push them into our format, and load them up.

Join us!

ICDA is a best-practice governance network for the directors serving on Australia's 600,000 not-for-profit boards, committees and councils, and the senior Workers who support them.

ICDA members get access to a range of educational, capacity building and networking opportunities that build knowledge, connections and credentials.

If you appreciated this free policy, we would appreciate your ongoing support by joining ICDA from only $65 p.a

The benefits of membership

1. Receive 'responsible person' status – ICDA members are recognised by the ATO under 'responsible person' rules
2. Recognition – three membership post-nominal options, providing community and professional recognition for educated and engaged not-for-profit members
3. Capacity building publications – current trends, issues and emerging areas of risk via member-only newsletters governance help sheets
4. Policy alerts – receive notification when changes are made to governance, human resources, financial management, values and communications policies you've downloaded through the Policy Bank
5. Preferential member pricing – members receive discounts for the Festival of Community Directors events and online Compact Courses
6. Alumni events – access to deep connections and a vibrant network of believers and doers. There's an online forum, as well as regular invitations to events like Communities in Control Conference
7. Access to forums, networks, information and opportunities – boost your confidence (and competence) and open career doors
8. Budget-friendly – for as little as $65 a year you get all the benefits outlined above and so much more.

Legal advice at a pre-agreed price

Please note that this is a template policy for guidance only. For assistance in tailoring this policy to suit your organisation, or for legal advice at a pre-agreed price or training in this area, please do not hesitate to contact Our Community's preferred legal supplier Maddocks.

E: NFPHelp@maddocks.com.au | W: https://maddocks.com.au