Cancer Council

Information Security Policy

January 2019

cancercouncil.com.au

Contents

1. Introduction 3
2. Application and Review .... Error! Bookmark not defined.
3. Definitions 3
4. Responsibilities 4
5. Physical and Environmental Security 4
6. Access Control 5
7. Protection Against Malicious Code 5
8. Acceptable Use of Information Assets 6
9. Vulnerability and Security Patch Management 6
10. Backup and Recovery 6
11. Change Control Procedures 7
12. Systems Acquisition, Development and Maintenance 7
13. Information Security Incident Management 7
14. Audit Logging and Monitoring 8
15. Asset Inventory 8
16. References / related documents 8

1. Introduction

1.1 Cancer Council NSW (**Cancer Council**) recognises that the security of its information systems and information assets is vital to its continued operation and success. The purpose of this policy is to address the security and protection of Cancer Council's IT resources and the information stored on them and to ensure that Cancer Council Workers are aware of their rights and obligations when using Cancer Council IT resources and the information stored on them.

1.2 This policy is based on international standard ISO27001, Information Security Management Systems Annex A – Control Objectives.

2. Definitions

2.1 In this policy:

information assets means all data created, collected or maintained by Cancer Council's Information Systems and includes data held by Cancer Council on behalf of other organisations;

information systems means all IT systems owned or operated by Cancer Council or held on Cancer Council's Premises, and includes the following:

- servers (physical and virtual) including file, application, email, database, backup, web and storage area network (SAN)
- gateways (physical and virtual)
- websites
- computers and workstations, either connected to a Wide Area Network (WAN), Local Area Network (LAN) or operating in stand-alone mode, and
- any device used to store, process or transmit data including fax machines, portable media, multi-function devices, tablets and smartphones.

premises means premises owned or occupied by Cancer Council;

secure environments mean the following environments situated at Cancer Council's premises located at 153 Dowling Street Woolloomooloo:

- IT Server Room Level 1
- IT Build Room Level 1
- Main Distribution Frame Room Level 1, and
- Cardholder Data Environments (CDE) as defined by PCI DSS (which includes the POS systems, eftpos machines and secure SFTP servers for receiving credit card details).

workers means any person Cancer Council employs or engages – including paid employees, volunteers, contractors, consultants, student and intern placements.

3. Responsibilities

3.1 This policy is owned by the Chief Information Office (**CIO)**. The CIO has overall responsibility for information security, policy documentation and the implementation of approved information security policies, standards and procedures. The CIO may delegate some duties to the IT Development and Operations Manager.

4. Physical and Environmental Security

4.1 Cancer Council information systems and infrastructure will be designed, implemented and operated in a manner that ensures adequate protection of information systems and information assets.

Physical Security

4.2 Information systems and information assets will be protected at all times from unauthorised access, theft, illegal use, illegal modification and intentional damage:

(a) physical access to network and communications, and authentication services facilities will be restricted to persons authorised by the CIO;

(b) access to information systems and information assets will be restricted to workers in accordance with the Access Control Guideline;

(c) the installation of any software or equipment on an information system or information asset is forbidden unless authorised by the CIO. Any unapproved equipment will be removed by IT;

(d) network documentation (including diagrams) must be classified as 'highly confidential' and access protected according to the Information Classification and Handling Guideline.

4.3 Access to secure environments will be:

(a) restricted using physical access controls such as a proximity card reader or passwords;

(b) restricted to authorised workers;

(c) subject to supervision to reduce the risk of malicious activity;

(d) removed upon termination of employment or when no longer required; and

(e) regularly reviewed and updated.

4.4 Access to secure environments will be monitored by Cancer Council.

Firewalls

4.5 Information systems and information assets will be protected by firewalls that comply with the Firewall Configuration Guideline.

4.6 Confidential information assets must be segregated from general access networks and additional controls must be placed in respect of them on information systems and applications. The following measures will be implemented, as a minimum, to reduce risk of unauthorised access or inappropriate use:

(a) a firewall must be used to protect all information systems and information assets containing content not of a public nature;

(b) all data packets and connection requests will be controlled by the firewall;

(c) only explicitly permitted traffic is allowed through the firewall. All other traffic is rejected;

(d) all traffic passing through the firewall must be captured, logged and audited;

(e) where possible, traffic passing through the firewall must be capable of being encrypted;

(f) packet filtering will be used with rules which keep the security risk to a minimum;

(g) all internet/web servers that require connectivity to Cancer Council's information systems and information assets must be approved; and

(h) all internet/web servers will have non-necessary services disabled.

Disposal of equipment and media

4.7 Information systems and information assets slated for retirement or destruction will first have all data or software destroyed or securely erased. If media containing confidential data is to be re-used, the data will first be securely erased.

4.8 Data will be retained and disposed of in accordance with the Data Retention Guideline.

5. Access Control

5.1 Information assets will be classified in terms of legal requirements, value, criticality and sensitivity in accordance with the Information Classification and Handling Guideline and may only be accessed, stored and transmitted in accordance with that Guideline.

5.2 Confidential information will be protected by security systems such as encryption and/or protected physical links when in transit.

6. Protection Against Malicious Code

6.1 Workers are not permitted to install, run, copy, store, distribute or develop any form of malicious code on information systems or in respect of information assets.

6.2 Anti-virus and other software will be implemented on information systems and information assets to detect and remove viruses and other malicious software in line with the Antivirus Guideline and must not be disabled. Malicious code on information systems and information assets will be removed in accordance with the Malware Removal Guideline. Phishing and spam events will be managed in accordance with the Phishing and Spam Guideline.

7. Acceptable Use of Information Assets

7.1 All workers using information systems and information assets must comply with P08 - IT Acceptable Use Policy.

Passwords

7.2 Workers are required to use complex passwords. Password sharing is not permitted.

Mobile Computing

7.3 Workers must be diligent in their efforts to information systems and information assets especially when working from a remote location. Workers must only use Cancer Council approved devices and facilities to connect to Cancer Council's network.

Removable Media Handling

7.4 Removable media such as USB drives are not permitted unless exempted due to a valid and specific business need. Media containing Cancer Council data or information must be secured by encryption and protected at all times and information must be removed from media once no longer required.

8. Vulnerability and Security Patch Management

8.1 Information systems and information assets must be "hardened" (a process of strengthening the security) by disabling unnecessary software and services.

8.2 Information about technical vulnerabilities to information systems and information assets will be obtained and managed in accordance with the Vulnerability Management Guideline. Internal and external network vulnerability scans will be performed regularly and after any significant change to the network.

8.3 Security patches for identified technical vulnerabilities in information systems and information assets will be managed in accordance with the Patch Management Guideline.

9. Backup and Recovery

9.1 Routine procedures will be established for making back-up copies of data and testing their timely restoration to maintain the integrity and availability of information systems and information assets.

9.2 Those routine procedures will include:

(a) hard copy and virtual backups that must be stored offsite, or in another physical location or cloud to the source data;

(b) system backups performed before and after major changes to either the operating system, system software or applications;

(c) regular tests of backup media and key corporate systems backup data to verify that systems can be recovered from backup; and

(d) requests for data backup via the completion of an IT Service Desk request.

10. Change Control Procedures

10.1 Changes to information systems and information assets will be monitored, verified and approved in accordance with the Change Control Guideline.

11. Systems Acquisition, Development and Maintenance

11.1 Cancer Council will acquire information systems and information assets only through known and reputable sources. Acquisitions of information systems and information assets will be in accordance with the P10 - IT Purchasing Policy.

Third-Party Suppliers

11.2 Engagements with external parties providing IT services (including cloud providers), will be managed according to the Third Party Management Guideline.

System Requirements

11.3 Software development must follow secure design principles – e.g. Open Web Application Security Project (OWASP) guidelines.

12. Information Security Incident Management

12.1 Information security incidents will be reported and managed in accordance with the P11 - IT Information Security Incident Response Policy. Workers are responsible for reporting suspicious events and potential security incidents to the IT service desk as soon as possible. In the event of a serious incident, the IT Development and Operations Manager must be alerted.

12.2 Data breaches will be responded to in accordance with the P17-FSO Data Breach Response Plan.

13. Audit Logging and Monitoring

13.1 IT Department monitors usage of systems and maintains audit logs to provide sufficient information for an after-the-fact security investigation. Third-party providers assist in this process. Logs are actively monitored or manually reviewed for suspicious events.

13.2 Logging and monitoring of logs will comply with the Log Management and Auditing Guideline.

14. Asset Inventory

14.1 An inventory of information systems and information assets will be maintained by the CIO.

15. Application and Review

This policy was last updated in November 2018 and will be reviewed on or before September 2021. It replaces all other versions of this Policy This policy may be reviewed and varied from time to time in accordance with the relevant legislation requirements and to meet the ongoing needs of the organisation.

This policy applies to all Cancer Council workers, including casual employees and contractors, and volunteers. Non-compliance may result in disciplinary action, including termination of employment. Whilst they are required to comply with this policy, which may be updated and amended from time to time, it does not form part of any employee's contract of employment or other contract and does not create or confer any entitlement, legal right or enforceable benefit.

16. References / related documents

- P03 - Bring Your Own Device Procedure
- P11 - IT Information Security Incident Response Policy
- P13 - FSO Record Retention Policy
- P08 - IT Acceptable Use Policy
- P10 - IT Purchasing Policy
- P17- FSO Data Breach Response Plan
- Access Control Guideline
- Antivirus Guideline
- Change Control Guideline
- Data Retention Guideline

- Firewall Configuration Guideline
- Information Classification and Handling Guideline
- Key Management Guideline
- Log Management and Auditing Guideline
- Malware Removal Guideline
- Patch Management Guideline
- Phishing and Spam Guideline
- Third Party Management Guideline
- Vulnerability Management Guideline