WEST COAST DISTRICT MUNICIPALITY

INFORMATION SECURITY POLICY

(FOR EMPLOYEES)

BM/18/04/25/6.2.4

Executive Mayoral Committee – 25 April 2018

INFORMATION SECURITY POLICY (FOR EMPLOYEES)

1. Introduction

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the Municipality's ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

2. Policy overview

- West Coast District Municipality, hereafter referred to as "Council", holds a large quantity of information that could cause difficulties if it fell into the wrong hands or become inaccessible. Everyone needs to make sure that information is secure from the moment that it is collected or created, whenever it is used, when it is stored and finally, when it is disposed of. Furthermore, there is a legal duty to keep certain information secure and to use information systems in a certain way. Finally, everyone who uses electronic communications represents Council and must take special care to maintain the clarity, consistency and integrity of Council's corporate image and posture.
- This policy highlights the main duties that everyone needs to know and adhere to. For the purpose of this policy the terms "users" or "everyone" includes councillors, employees, contractors and third parties.
- All employees granted access to Council's information systems, Internet and e-mail access will be provided with a written copy of this policy and must sign the attached declaration; opting not to sign will be seen as not being in need of these facilities, where after all access rights will be terminated.

3. General policies

- Everyone must familiarise themselves and comply with this and other Council information security policies.

(i) Everyone will execute any particular security process or task assigned to them.

(ii) All information systems are owned by Council and users are only permitted to use the facilities for business use with limited incidental private use.

(iii) Everyone has a duty to protect Council records, whether it is for regulatory, contractual or operational requirements.

(iv) Everyone has a duty to report security incidents, weaknesses or non-compliance with the security policies as quickly as possible.

(v) It is not permitted to attempt to prove suspected security weaknesses.

4. Access to systems

(i) Access to information systems are forbidden, unless formally permitted.

(ii) Passwords must be kept secret and never be written down.

(iii) Never use obvious passwords such as a birth date or a pet's name.

(iv) Always select strong passwords i.e. at least 8 characters in length and a combination of alpha-numeric characters, with at least one uppercase/lowercase combination.

(v) Passwords must be changed immediately if they are suspected to have been compromised.

(vi) Passwords may not be stored in any automated log-on process, macro or function key.

(vii) Log off systems if they are not in use or when computers are left unattended, unless the computer has an automatic screen locking mechanism.

(viii) Never use another employee's account to access systems.

5. E-mail and Internet

(i) The Council will limit Internet and email access to those employees who demonstrate a legitimate business or educational need.

(ii) Everyone must be aware that the Council reserves the right to use monitoring tools and may produce periodic reports detailing individual use of the e-mail and Internet systems.

(iii) E-mail and Internet is only for business use with incidental personal use if it does not interfere with job functions.

(iv) Private e-mail messages may be received and sent by users, but should be kept to an absolute minimum and should not include attachments of massive data, graphics or media files.

(v) E-mail and Internet may not be used for any illegal or offensive activities.

(vi) Employees may not deliberately attempt to visit, view or download any material from a website containing sexual, discriminatory or illegal material, or material which may cause offence to others.

(vii) Employees may not compromise the organisation, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorised purchasing, etc.

(viii) Employees may not upload or email any software licensed to Council, or data owned or licensed by Council, without explicit written authorisation from the responsible member of the IT Committee for the software and data integrity of Council for that department.

(ix) No employee shall distribute the email address list of Council to a third party for marketing and/or advertising purposes, nor may it be used for chain mail or offensive marketing.

(x) No employee, other than the Municipal Manager or officials who are duly authorised by him, may speak, or write and/or sign documents, on behalf of Council. Employees may participate in newsgroups or chat forums in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves, unless otherwise authorised to speak on behalf of Council.

(xi) Employees are reminded that chat and newsgroups are public forums where it is inappropriate to reveal confidential Council information, customer data, trade secrets or any other material covered by existing Council secrecy policies and procedures.

(xii) The official e-mail address or any other form of identification that links the employee to the Council may not be used on social media (e.g. Facebook).

(xiii) Always consider whether an e-mail's contents are important enough to send it encrypted or password protected over the Internet.

(xiv) Electronic mail forwarding to external e-mail addresses is not permitted.

(xv) All mail messages must have the official signature attached.

(xvi) Never save personal data, official passwords or e-mail address on computers, software or public websites.

(xvii) Employees may not use any free Internet services (e.g. e-mail addresses or data storage) for official use unless previously authorised by IT as they may not be secure.

(xviii) Always be aware of statements in electronic mails that may be viewed by third parties as binding contracts.

(xix) Video and audio downloading should be avoided.

(xx) Employees should schedule communication-intensive operations such as large file transfers, video downloads, mass mailings and the likes for off-peak times. Large files must be compressed before sending or receiving.

(xxi) Employees may not use Internet facilities to download entertainment software or games, nor to play games against opponents over the Internet or network.

(xxii) Employees may only download software, with written authorization of the IT Committee, for direct business purposes and must arrange to have such software properly licensed and registered.

(xxiii) Employees may not use the Internet to attempt to gain access to computers, files, services etc.

(xxiv) The policy statements above are equally applicable to instant messaging services.

(xxv) Misuse of the Internet and e-mail facilities may lead to permanent disconnection of a user by order of management and may result in disciplinary steps against such an employee.

6. Unauthorised software or other information products

(i) Using or installing unlicensed software or other information products is not permitted.

(ii) Everyone must comply with the license terms and conditions stated by publishers.

(iii) Software may only be acquired from known and reputable sources.

(iv) Employees must retain licenses, master disks, manuals or other evidence that provides proof of ownership of software or other information products.

(v) Employees may not breach copyright law by copying materials in full or part from copyrighted materials (e.g. books, articles, trademarks, source code etc.)

7. Computer viruses

(i) Everyone must be aware of the risk of viruses and always follow safe computing practices, such as:

- i. Do not use any devices for official use that do not have anti-virus software.
- ii. Do not interfere with the operation of anti-virus software.
- iii. Do not download and launch files or software from external networks, e-mails or removable media unless absolutely necessary for official purposes. If such a need arises, always scan the files or software first for viruses before use.
- iv. Do not visit websites that are not reputable.
- v. Heed warnings from IT management relating to virus alerts.

(ii) In the case of virus detection, discontinue work and report the incident immediately.

8. Information on paper

(i) Everyone has a duty to safeguard documents that contains confidential information.

(ii) Desks must be kept clear of confidential documents or removable media.

(iii) Always consider the security arrangements when sending confidential information via couriers, post or by hand delivery.

(iv) Employees should print confidential information in secure areas.

(v) Confidential information may not be left unattended on printers, copiers or fax machines.

(vi) Fax machines and copiers offer the ability to retrieve other employee's stored pages and are prone to accidental misdialling or malicious programming. Always consider if it is really necessary to use these facilities on confidential information.

(vii) Confidential paper must be disposed of in the established secure process.

9. Talking and making phone calls

(i) Always consider whether it is appropriate to discuss confidential matters over the phone or to leave confidential messages on voice mail.

(ii) Users must restrict access to their voice-mail service.

(iii) Never have confidential conversations in public places or open offices and meeting places with non-sound proofed-walls.

(iv) When responding to requests for information from external parties (e.g. law enforcement) always verify the identity of the person requesting the information and confirm authorisation and the proper way of documenting the information, before releasing such information.

10. Personal phones, tablets etc.

(i) Employees may only use authorised mobile devices for official use and only if they comply with the device's security standard.

(ii) Council owns any official information on personal mobile devices and reserves the right to enforce security measures and to confiscate the device and recover or delete the information manually or remotely.

11. Access to the network

(i) Wireless connections to the network may not be established without approval.

(ii) Remote access to the network may only be used for official and legal purposes.

(iii) Personal 3G connections may not be used on official hardware unless it is authorised by IT.

12. Travelling or working from home

(i) Employee's security responsibilities extend outside normal working hours and premises and continue after employment has ended.

(ii) When travelling or working from home, take due care not to lose or have your equipment stolen. Never leave equipment in public places and always keep your network password confidential.

(iii) All requirements imposed by insurance policies on equipment security must be complied with.

13. Memory sticks, CDs, portable hard disks etc.

(i) Removable media must be encrypted or password protected if it is taken off-site and at risk of being lost or stolen.

(ii) Removable media may not be thrown away, but given to IT to be securely disposed.

14. IT equipment

(i) IT equipment owned by Council must be returned if it is no longer needed. This includes changing employment.

(ii) Any official information contained on personal equipment must be removed in the event of changing employment.

15. Backups

(i) Employees are responsible for their own backups if they choose to save data to PCs, laptops or mobile devices. Save copies of data to the file servers, which are regularly backed up.

16. Protection of personal information

(i) Personal information may not be collected and stored by anyone unless safeguarded in accordance with legislation.

17. Security of the premises

(i) Everyone has a responsibility to protect the security of premises by keeping security doors closed, keeping keys and access cards safe, and to follow visitor entry and exit protocols.

(ii) No equipment, information or software may be taken off-site without prior authorisation.

18. Systems development

(i) Employees may not perform any changes to systems, develop new systems, or acquire new package software, outside of the established change control process.

(ii) The use of desktop applications (e.g. spreadsheets or databases) for a specific purpose is discouraged if it makes better sense to develop a formal system on a server.

(iii) If an employee chooses to use desktop applications for an important purpose, the following safeguards must be considered:

- i. The functionality must be tested.
- ii. The versions of the desktop application must be managed.
- iii. Access to the application and its functionality must be appropriately restricted.
- iv. Access to the file server directory, PC or laptop must be restricted.
- v. The data must be backed up regularly.
- vi. Data captured into the application must be validated and checked.

18. Acceptance of policy

Signed on this ____ day of ______________ 201_.

____
Employee Signature

____
Employee Name