WEST COAST DISTRICT MUNICIPALITY

INFORMATION SECURITY POLICY (TECHNICAL POLICY)

INDEX

1 Introduction

1.1 Importance of Information Security

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. Council has become highly reliant on its information and information systems to meet citizens’ demand for service delivery, and administrative and operational efficiencies. The Council’s financial position and reputation is therefore directly linked to the success of its information systems.

With the ever changing technology landscape, also come many threats to information and information systems from employees, contractors, third parties, external parties and the environment alike. Some of these threats may be malicious, others may be accidental. It is therefore important to have appropriate information security controls in place to manage these threats to an acceptable threshold.

This document sets out the Information Security Policy of the Council. This particular policy is of a technical nature and should be read in conjunction with the abbreviated Information Security Policy developed for employees, contractors and third parties.

1.2 Information Security principles

Information Security at the Council will be founded on the following principles:

- Information Security controls will make business sense.
- Everyone has security responsibilities.
- Information will be protected in accordance with its confidentiality and value.
- Information includes electronic data, hardcopy information and conversations.
- Access to information systems will be restricted in terms of job descriptions and segregation of duties.
- Authorised users will be able to access information systems when they need to.
- The integrity of information will be protected from the moment that it is collected or created, whenever it is used, when it is stored and finally, when it is disposed of.
- Information security risks will be identified and managed accordingly.
- Information security incidents will be acted upon as appropriate.
- Users will be provided with a secure working environment.
- Disaster recovery plans will be maintained and tested on a regular basis.
- Security awareness will be promoted within the Council.
- The Council will meet applicable regulatory and legislative requirements.
- Third party service provider accessing information systems will implement appropriate controls.

1.3 Scope and applicability

This policy applies to everyone in the Council. Failure to comply with this policy may result in disciplinary action up to and including dismissal, civil or criminal action, or a combination of both.

Municipal Managers are ultimately responsible for Information Security.

2 Information Security Management System

2.1 Security organisation

2.1.1 Information Security is everyone's responsibility:

(a) Executive Management is ultimately responsible for Information Security and to provide for sufficient resources in this regard.

(b) Process and System Owners are ultimately responsible for Information Security in their respective areas, and as such have a duty to inform Information Security Managers of risks in their environments, as well as to assist them with defining the appropriate controls.

(c) Information Security Management takes responsibility for the day-to-day development and management of Information Security controls.

(d) IT Management are only ultimately responsible for Information Security in their capacity as Process and System Owners of IT services. However, Information Security Management and IT Management may be performed by the same resources.

(e) All employees, contractors and third parties have a duty to comply with the Information Security policies and to execute any particular security process or activities assigned to them.

(f) Audit functions provide assurance on Information Security controls, but are not responsible for Information Security.

2.1.2 Information Security related decisions will be made by the decision making bodies defined within the IT Governance Framework / IT Charter.

2.2 Security risk assessment

2.2.1 Information Security will be deployed using a risk-based approach. This will have several dimensions as explained below.

2.2.2 Information systems (applications or services) will be identified at an aggregate level and allocated an owner (usually the owner of the business process). The owner will classify each information system according to the following scheme (using one or more of the guidelines):

(a) Critical

- Information systems (or modules within information systems) that should only be accessed by specific users with the need to have access. The information system contains highly confidential information or enables the processing of transactions with a high fraud risk.
- The information system may also have special legal compliance requirements that could lead to significant consequences if not complied with.
- The availability of the information system is critical.

(b) Sensitive

- Information systems (or modules within information systems) that should only be accessed by specific users with the need to have access. The information system could contain confidential information or enable processing of transactions susceptible to fraud.

- The information system may also have special legal compliance requirements.
- The availability of the information system is important.

(c) Internal

- Information systems that should only be accessed by internal users, but do not contain confidential information and do not enable processing of transactions susceptible to fraud.
- The availability of the information system is not of great concern.

(d) Public

- Information systems that are available to the general public.
- Any unauthorised changes to the information present a low degree of impact to the organisation.
- The availability of the information system is not of great concern.

2.2.3 The classification of each information system must be used as a guideline when considering to deploy or not to deploy Information Security controls defined in this policy.

2.2.4 Assuming that an Enterprise Risk Assessment approach exists, the approach must include Information Security risks and be treated or managed accordingly.

2.2.5 Risk assessments will be re-visited on a cyclic basis.

2.2.6 Vulnerability assessments and audits will be performed on information systems environments on a cyclic basis (as defined in other sections of the policy).

2.2.7 Security incidents will be reviewed to identify and resolve recurring problems (as defined in other sections of the policy).

2.3 Security policies

2.3.1 The Information Security risks will be treated by considering whether they are within the risk acceptable thresholds, failing which additional security controls should be deployed. This approach will be conducted in the following manner:

(a) The controls that will mitigate a risk will be selected from recognised good practices (e.g. ISO 27000 series) after due consideration and where this makes sense in the environment.

(b) The controls will be documented within Information Security policies, procedures, standards and plans.

(c) A strategy will be formulated and implemented to establish the desired controls over a period of time.

2.3.2 Information Security policies will be made available to all concerned and maintained on a cyclic basis.

2.4 Security awareness

2.4.1 All employees, contractors and third parties will attend appropriate awareness training and familiarise themselves regularly with updates in Information Security policies as relevant for their job function.

2.5 Security effectiveness reviews

2.5.1 The effectiveness of deployed Information Security controls will be reviewed at cyclic intervals and after security incidents. This will be done in the following manner:

(a) Information Security controls must be reviewed independently at planned intervals, or when significant changes to the environment occurs if a review makes business sense.

(b) Metrics will be defined and collected to measure the effectiveness of controls.

(c) Once a security incident occurs, the underlying reasons for the incident must be resolved to the extent that it makes sense in the environment.

(d) Management will consider the effectiveness of controls on a cyclic basis.

2.6 Legal and regulatory compliance

2.6.1 Information systems environments may be subject to legal and regulatory requirements (including cross-border requirements). Therefore the Council will ensure that these requirements are addressed in the following manner:

(a) Applicable legislation will be identified, recorded and kept up to date by enterprise compliance functions and through seeking advice from specialist IT legal advisors; and

(b) IT policies, procedures, standards and plans will be updated to give effect to these requirements in day to day use of IT and IT operations.

3 Employees, contractors and third parties

3.1 Prior and during employment

3.1.1 The Council will ensure that employees, contractors and third party users understand their responsibilities regarding information security. This will be done in the following manner:

(a) Security responsibilities will be defined and included in employment contracts (prior to employment) and / or end-user information security policies.

(b) Job descriptions will include any specific information security process or activities assigned to individuals.

(c) Employees, contractors and third party users must agree to their security responsibilities in writing or any other electronic form that is legally acceptable.

(d) Everyone in the Council will be provided with security awareness education and / or training relevant to their job function.

3.1.2 Background verification checks will be performed on all candidates for employment, contractors, and third parties where the job description entails access to sensitive information or duties where the potential for fraud is elevated.

3.2 Termination or change of employment

3.2.1 The Council will ensure that employees, contractors and third party users exit the organisation, or change employment responsibilities, in an orderly manner. This will be done in the following manner:

(a) Any assets no longer required will be recovered.

(b) Any information relating to the Council contained on personal equipment will be removed.

(c) Access rights will be removed or changed appropriately in a timely manner.

(d) In cases of management-initiated termination, access rights will be removed before termination at the discretion of management.

3.3 User access

3.3.1 The Council will prevent unauthorised access by users at an application level to information systems. This will be done in the following manner:

(a) Information systems will provide protection mechanisms from unauthorised access by any user, utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls;

(b) All users and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) will be uniquely identifiable by user.

(c) All changes to access rights (creation, modifications and deletions) will be made at the appropriate time based only on documented instructions, duly authorised by designated management individuals.

(d) User identities and access rights will be granted in terms of:

- Functional roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles; and

- Restrictions placed on access due to legal and regulatory requirements.

(e) All access to information, transactions and IT systems will be authenticated, at least through a user account and password. The following rules apply to passwords and log-on mechanisms:

- Passwords must expire every 90 days;
- Passwords must be at least 6 characters in length and contain at least one alpha-numeric combination;
- Passwords must not be included in any automated log-on process;
- The log-on process will not display the user password, nor will it assist the user in guessing the password;
- The number of unsuccessful log-on attempts will be limited to three;
- A record will be kept of previously used passwords to prevent re-use;
- Sessions will be set to time out after 15 minutes of inactivity;
- Passwords will be stored in protected form (e.g. encrypted or hashed); and
- Passwords will not be transmitted in clear text over the network (by implication insecure services such as ‘telnet’ are not allowed).

(f) Users will be made aware of their security responsibilities relating to user access.

(g) Privileged user accounts will be segregated from normal user accounts and appropriately restricted.

(h) System user accounts will be protected as far as possible to avoid disclosure (e.g. using very long and complex passwords, encrypting program code containing clear text passwords etc.).

(i) All user accounts and related privileges will be reviewed on a cyclic basis.

(j) Default passwords received from suppliers of software packages or utilities must be changed after installation.

(k) Users may not use any utilities capable of overriding system security to access data directly, without authorisation or safeguards in place to prevent fraudulent activity.

(l) An audit trail of access to information systems will be maintained.

3.4 Mobile computing

3.4.1 The Council acknowledges that mobile computing is becoming a common way of working; however information security risks must be addressed accordingly. Therefore all methods of mobile computing and the devices must be approved prior to use and subjected to a risk and controls assessment. The risk and controls assessment must satisfactorily deal with the following:

(a) The likelihood of the device becoming lost or stolen must be reduced (e.g. security cables for notebooks, staff security awareness, staff acceptable usage policy etc.).

(b) The information on the device must not be compromised in the event of the device becoming lost or stolen (e.g. complex passwords, hard-disk encryption, information backups, remote data wipe, device lock-out, acceptable types of portable storage devices etc.)

(c) The device must have a secure means of connecting to other devices and to networks (e.g. VPN, protecting wireless access etc.).

(d) The access to business applications deployed to the device must be restricted (e.g. user access control, encryption, deploying business applications using terminal servers etc.).

(e) The types of portable storage devices permitted for storing business information must be defined.

3.4.2 Staff will be made aware of the fact that the Council owns business information on the mobile devices and reserves the right to enforce security measures and to confiscate the device and recover or delete the information remotely.

3.5 Information protection and leakage

3.5.1 All access to the Council’s information is generally forbidden unless expressly permitted.

3.5.2 The Council will take general steps to prevent the leakage of critical or sensitive information. This will be done in the following manner:

(a) Users will be provided with facilities for the secure disposal of storage media, IT equipment or paperwork containing Council information. Users will be made aware of their responsibility to use these facilities.

(b) All information on mobile storage devices or media, including backup tapes, must be protected (e.g. encryption or password protection) if it is at risk of being lost.

(c) Information in paper form must be protected if it contains sensitive information. Users will be made aware of their responsibility to consider if information in paper form is sensitive, in which case reasonable steps must be taken to safeguard it from disclosure. This includes paper left on copy machines, printers, facsimile machines etc.

(d) Any critical or sensitive electronic communications that passes over the Internet, or any other untrusted network, will be encrypted or password protected in an appropriate way.

(e) No-one is allowed to compromise the reputation of the Council through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.

(f) Automatic forwarding of electronic mail to external e-mail addresses is not allowed.

(g) Everyone must take appropriate precautions not to reveal sensitive information when making or taking phone calls.

(h) Everyone will be made aware that it is not allowable to leave messages containing sensitive information on answering machines.

(i) Facsimile and copy machines have inherent security risks, namely the ability to retrieve stored pages, accidental misdialling or malicious programming. Everyone will be made aware of due care to be taken when using these facilities with critical or sensitive information.

(j) Registering personal data, passwords or e-mail address on personal computers, software or public websites will not be allowed.

(k) Everyone will be made aware not to have confidential conversations in public places or open offices and meeting places with non-sound proof walls.

(l) Everyone will be made aware of the need to consider the security arrangements of information being sent via couriers, post or hand delivered.

(m) Information will be retained in accordance with regulatory, contractual or operational requirements.

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

3.6 Outsource partners

3.6.1 The Council will manage outsourced IT services to maintain the protection of information and the reliability of service delivery. This will be done as follows:

(a) Suppliers will be selected with due cognisance of their ability to maintain the protection of information and reliability of service delivery.

(b) Security and service delivery requirements for information systems will be included in contract conditions with IT outsource partners. The following will be included as a minimum:

- Service measurement
- Adherence to IT governance requirements (e.g. compliance with IT policies, compliance with laws, asset protection, privacy, authorised access, managing privileged access, confidentiality, security awareness, change management etc.)
- Ownership of data and security responsibilities should there be exchange of data between the parties
- Ownership of source code, escrow agreement, intellectual property rights and copyright
- The right to audit
- Management of sub-contracted suppliers
- Obligation to maintain documentation
- Any requirements for the supplier to screen its staff or to do background checks prior to employment or prior to being deployed to the contract
- Conditions for renegotiation/termination of agreements
- Dispute resolution
- Normal termination and transition support

(c) IT outsource partners will not be granted access to the network before the contract has been signed.

(d) IT outsource partners will be made aware of security responsibilities.

(e) Critical IT controls processes will be integrated with those of IT outsource partners (e.g. change management, incident management etc.).

(f) IT contracts with IT outsource partners will be monitored to ensure compliance with contract conditions.

(g) IT outsource partners will be subjected to independent IT audits.

3.7 Customer access

3.7.1 Should it be necessary to give customers or the public access to its information systems or assets, the risks will be managed as follows:

(a) A contract will be entered into by the Council and its customers or the public.

(b) The contract terms must address the risks associated with the sensitivity of information systems or assets that will be affected, including the legal requirements to protect such information.

(c) The contract terms must be defined by experienced IT legal advisors, tailored for each circumstance. The following must be included as a minimum:

- Ownership of information systems and assets;
- The safeguarding of assets and return of assets;
- The information security responsibilities of both parties (e.g. safeguarding of passwords, malware protection etc.);
- The right to monitor and revoke access;
- Legal compliance matters;
- Intellectual property rights and copyright; and
- Limitation of liability of the Council.

(d) The contract terms must be displayed to the user in an appropriate manner, and as stipulated by IT legal advisors.

(e) Customers or the public will not be granted access to the Council's information systems until they have agreed to the contract in a manner stipulated by IT legal advisors.

(f) All customers or the public accessing information systems must be uniquely identified.

(g) Access must be granted using an approach commensurate with the risks of granting such access.

(h) The Information systems that customers or the public will be allowed to access must be suitably segregated by network controls to prevent unauthorised access to the Council's internal network.

4 Information systems

4.1 Development and maintenance

4.1.1 Information security requirements must be included in the requirements definition when developing new information systems or when acquiring off the shelf software. The development and selection of software must consider these information security requirements, unless compensating controls can be implemented to address the perceived information security risks.

4.1.2 All changes to information systems (including infrastructure and networks) will be controlled through change control. This will include the following controls, at a minimum:

(a) All change requests will be logged and approved by the owners of the information systems.

(b) All change requests must be accompanied by an information security impact analysis.

(c) Emergency changes must follow the same process, only quicker. Documentation may be updated at a later stage.

(d) All changes must be tested in a secure test environment that is representative of the production environment.

(e) The test environment must be separate from the production information systems.

(f) The change must be tested and accepted by the initiator, prior to deployment.

(g) The release of a change must be performed in a planned manner to ensure success and fallback if required.

4.1.3 Test data must be protected in the same manner as production data, ideally by removing sensitive details beyond recognition. This is particularly relevant to data affected by legislation e.g. personal information.

4.1.4 Access to program source code and / or system documentation must be restricted to prevent the introduction of unauthorized functionality or disclosure of sensitive information.

4.1.5 Outsourced software development must be supervised and monitored to ensure quality of the code and to prevent the introduction of malicious code. Software must be tested by the Council prior to release into production.

4.2 Information input and processing

4.2.1 The Council will ensure that information input and processing in IT systems is valid, complete, accurate, timely, and secure (i.e., reflects legitimate and authorised business use), through the following:

(a) Access rights within information systems will ensure that transactions are created by authorised individuals only, including where appropriate, adequate segregation of duties regarding the origination and approval of transactions.

(b) Information systems will authenticate the originator of transactions and information systems will verify that he/she has the authority to originate the transaction.

(c) Information systems will validate input data according to defined validation rules.

(d) Information systems will capture source information, supporting evidence and the record of transactions, and retain the data in accordance with prevailing data retention policies.

(e) Information systems will maintain the integrity and validity of data through processing.

(f) Information systems will maintain the integrity of data during unexpected interruptions in processing and confirm data integrity after processing failures.

(g) Information systems will present errors and exceptions to users to facilitate their correction.

(h) Information systems will protect the information during transmission, and maintain authenticity and integrity during transmission or transport.

(i) Information systems will verify the accuracy and completeness of output.

(j) Information systems will handle output in an authorised manner and deliver to the appropriate recipient.

(k) Notwithstanding any automated controls as stated above that are embedded into information systems, the end-to-end municipal business processes will be sufficiently controlled by management with manual controls to ensure that only valid, complete, accurate, timely and secure transactions are inputted.

4.3 Electronic commerce systems

4.3.1 The Council allows the deployment of information systems offering online transactions or electronically publicly available information. However, the following security implications of such systems must be addressed as a minimum prior to deployment using specialist's advice:

- The system must not accept transaction input from unauthorised users, services or systems;
- The activities of users, services or systems must be restricted within the system;
- Business rules must be embedded into the system to ensure non-repudiation, completeness and accuracy of transaction input and processing;
- Technical controls must be embedded into the system to prevent errors such as incomplete transmissions, duplicated transactions etc.
- The system must not be exposed to application-level security vulnerabilities (refer OWASP for examples);
- The infrastructure supporting the system must be security hardened to prevent circumvention of application level security;
- Sensitive information being stored or in transit must be protected from unauthorised disclosure.
- The system must have adequate availability and performance;
- Unauthorised access to the internal network beyond the application must be prevented;
- Transaction flow between the system and back-office information systems must be protected and secure;
- Sensitive security information about the system must be protected from disclosure;
- The website must be protected against phishing attacks;
- All activities must have an audit trail;
- Website contents must comply with legal and regulatory requirements; and
- The terms and conditions between trading partners committing both to limitation of liability and security responsibilities.

4.3.2 Browser-based applications must be tested for application level security vulnerabilities if they are deployed on the Internet, prior to go live and then again at regular intervals.

4.4 Desktop applications

4.4.1 The Council acknowledges the proliferation of desktop applications (e.g. spreadsheets or databases), but its use is discouraged for critical information processing. In the event that this form of information processing is in use for critical information processing, the following safeguards must be considered on a case by case basis:

- Testing the functionality and using version control;
- Access controls to the application itself and where it is stored;
- Access controls to powerful functionality within the application itself;
- Input validation checks; and
- Information backup.

5 IT facilities, infrastructure and networks

5.1 IT facilities and server rooms

5.1.1 The Council will protect IT facilities and server rooms against environmental risks to ensure the continuity of normal operations. This will be done in the following manner:

(a) IT facilities and server rooms will be situated and constructed to minimise and mitigate susceptibility to environmental threats.

(b) Environmental threats (e.g., fire, water, smoke, humidity) will be monitored by specialised devices.

(c) Eating, drinking and smoking in server rooms will not be allowed. Stationery and other supplies posing a fire hazard may not be stored in server rooms.

(d) IT facilities will be protected against power fluctuations and outages.

(e) Where practical, IT facilities will have more than one source for dependent utilities (e.g. power, telecommunications, water etc.).

(f) IT facilities and equipment will be managed to vendor specifications and health and safety regulations.

(g) Server rooms will have a separate physical entrance.

(h) Cabling outside of server rooms will be organised and protected against damage and tampering.

(i) Equipment and media may not be taken off-site unless authorised, and any items taken off-site must be recorded.

(j) Equipment and media taken off-site must be protected from theft or damage, taking into consideration suitable security and environmental control measures.

5.1.2 Work areas outside of IT facilities will be protected with physical access control (e.g. working in secure areas) if the nature of information being processed warrants such measures.

5.1.3 All information on storage media on equipment scheduled for disposal or re-use must be securely erased or destroyed in a manner that prevents retrieval.

5.1.4 Virtual server environments must be secured as follows:

(a) Access to the virtual server management console (or equivalent) must be restricted to authorised virtual server administrators.

(b) Each virtual server must be treated as a physical server and protected using the same information security controls.

(c) Hypervisors must logically separate virtual servers to promote information security controls across multiple server environments.

(d) The communications between virtual servers must be encrypted.

(e) The number of virtual servers must not exceed management’s ability to a point where the administrator can no longer manage them effectively, or to a point where resource overload occurs.

5.2 IT assets

5.2.1 The Council will protect the IT assets that support information systems. This will be done in the following manner:

(a) All IT assets (hardware and software) will be accounted for and managed throughout its lifecycle in an asset register.

(b) The asset register will reflect, at a minimum, a description of the asset, the owner and location information.

(c) The asset register will be verified through cyclic physical checks or automated software audits.

(d) The asset register (or other repository) will reflect any specific security, legislative or availability requirements relating to an IT asset and controls will be deployed accordingly.

(e) Asset replacement will be planned in accordance with lifecycle strategies.

5.3 IT operational procedures

5.3.1 IT operational schedules and procedures will be developed and used to ensure that operational tasks are performed reliably and consistently (e.g. media handling, execution of jobs, backups, error handling etc.).

5.4 Network security

5.4.1 The network must be protected from malicious traffic on other networks by firewalls and / or virtual private networks.

(a) Firewalls must be configured securely in accordance with vendor recommendations, at a minimum to:

- Deny network traffic by default, and fail secure;
- Filtering of specific types or sources of network traffic;
- Block or restrict communication protocols that are prone to abuse or “denial of service attacks; and
- Limit the disclosure of information about the network at the network level.

(b) Firewall configurations must be security tested regularly and the rules manually reviewed to ensure that it remains secure and unnecessary rules removed.

(c) Critical information systems should ideally be isolated from other information systems on the network.

5.4.2 Only authorized devices will be allowed to have access to the network:

(a) Access to network devices must be restricted to authorised network staff.

(b) Network devices must be configured in a secure manner in accordance with vendor recommendations and security tested regularly, at minimum removing unnecessary services, changing vendor supplied passwords and keeping the devices up to date with vendor supplied updates.

(c) Network access points must be protected by locating them in secure environments or by disabling them when not in use.

(d) All third party network connections must be authorised, documented and have an owner. Third party connections must be disabled or decommissioned when no longer required.

(e) Third party connections must be configured in a secure manner in accordance with vendor recommendations and security tested regularly, at a minimum to:

- Verify the source of external connections;
- Restrict access to certain parts of the internal network or information systems; and
- Protecting information transmitted across the network connection (e.g. using encryption).

(f) All external devices (e.g. laptops) wanting to connect to the internal network must be authorised and meet the minimum security requirements of malware protection, patch updates and personal firewalls.

(g) Remote maintenance by vendors on information systems must be governed by contract terms, activity must be logged and access revoked after maintenance is complete. Remote diagnostic and configuration ports must be physically and logically security hardened according to vendor recommendations and security tested regularly.

(h) Wireless access to the Council network will be protected through:

- authorising all wireless networks;
- security hardening wireless networks according to vendor recommendations and security tested regularly;
- separating wireless networks from the internal network through filtering devices (e.g. firewall);
- protecting networks by using encryption without known vulnerabilities; and
- detecting unauthorised wireless access points using scanning software.

5.4.3 Hosts and network systems must be subject to penetration testing on a cyclic basis, from outside of the network, as well as from within. This can be done by IT management using security scanning tools, however an independent review performed by specialists in this field should augment IT management self-assessments.

5.4.4 Security-related events will be logged and monitored on hosts and networks using intrusion detection mechanisms to detect activity typically associated with unauthorised access attempts, known attack patterns or other malicious activity.

5.5 Network services

5.5.1 Access to network services will be restricted to authorised users:

(a) User access to all network services will be authorised and the capability of users to connect to the services will be restricted accordingly.

(b) Users will be provided with guidelines for the safe and authorised business use of network services (e.g. e-mail, Internet etc.)

(c) The acceptable use of network services will be monitored.

(d) Network services must be used and configured in a secure manner in accordance with vendor recommendations and security tested regularly.

(e) Remote access by users will be authorised, authenticated (e.g. Radius or TACACS+) and logged. Remote access facilities must be security hardened according to vendor recommendations and security tested regularly.

(f) Remote working by employees at off-site or personal locations will only be allowed if suitable security safeguards are in place to prevent theft of equipment, unauthorised disclosure of information and unauthorized remote access to the Council's network.

5.6 Telephony and conferencing

5.6.1 Telephony and conferencing facilities will be restricted as follows:

(a) VoIP networks will be protected by separating VoIP traffic from other network traffic, security hardening of devices, encrypting sensitive traffic and monitoring event logs.

(b) Access to voice-mail and voice-mail operator consoles will be restricted to the authorised user by using a password, which is different from the supplier standard passwords.

(c) Conferencing facilities (e.g. teleconferencing, video conferencing) will be protected from unauthorised access by requiring a unique password for each conference.

5.7 Malware protection

5.7.1 The Council will protect itself against malware (e.g. viruses, worms, spyware, spam etc.) as follows:

(a) Malicious software protection tools will be installed and activated, with up to date malicious software definition files.

(b) Protection software will be centrally distributed and managed to ensure consistent and up-to-date protection.

(c) New potential threats will be identified and managed e.g. by reviewing vendor's products and service advisories.

(d) Incoming traffic, such as email and Internet downloads, will be filtered.

(e) Users will be made aware through policy of what constitutes safe computer use.

5.8 Vulnerability management

5.8.1 The Council will configure its infrastructure and networks securely. This will be done in the following manner:

(a) Security baselines will be established for all platforms that support critical or sensitive information systems.

(b) The platforms will configured in accordance with the baselines, failing which exceptions to the baselines will be documented with a valid business reason and the compensating controls.

(c) The platform configurations will be validated against the baselines on a cyclic basis using manual or automated means.

(d) Deviations from the baselines will be investigated and corrected, or treated as an exception.

5.8.2 Devices such as printers and multifunction devices have similar security risks as servers. These security risks must be understood and managed through a secure technical configuration.

5.8.3 The Council will patch its information systems in a timely manner to ensure that security vulnerabilities cannot be exploited. This will be done in the following manner:

(a) Contacts with software suppliers and specialist security interest groups will be established to ensure that early warnings of security alerts, advisories, and patches pertaining to attacks and vulnerabilities are identified.

(b) Security patches will be tested and applied in a timely manner and the complete deployment of patches to all affected information systems will be monitored.

(c) Alternative methods will be established to protect information systems if it is not possible to apply patches or no solution is available for a known vulnerability.

5.9 Cloud computing

5.9.1 Storing or processing of information using cloud based services must be controlled in the following manner:

(a) Prior to the use of cloud computing services, a risk assessment must be undertaken that considers the criticality of the information to be stored and processed in the cloud, legal risks, contract risks, and the nature of the cloud service provider’s reputation and control environment.

(b) Following the risk assessment, any special security requirements to protect information in the cloud must be identified and managed by the Council itself (e.g. encryption of data in the cloud, or through the contract with the cloud service provider.

(c) The Council must remain abreast of the control environment of the cloud service provider and to respond to any changes made that could impact the initial risk assessment.

5.10 Intellectual property rights

5.10.1 The intellectual property rights of software or other information products that the Council uses will be protected. This will be done in the following manner:

(a) Software or other information products will only be acquired from known reputable sources.

(b) Awareness will be raised with users of the importance to protect intellectual property rights.

(c) Asset registers will contain all assets with requirements to protect intellectual property rights.

(d) Materials will be licensed and proof of evidence of ownership of materials (e.g. licenses, master disks, manuals etc.) will be retained.

(e) The Council will seek to compare purchased licenses against the installed base on a cyclic basis.

6 Business continuity

6.1 Disaster recovery

6.1.1 The Council will be able to recover from a disaster that affects information systems, in the timeframes acceptable to the business, but with due consideration of the likelihood of a disaster weighted against the cost of preparing to respond to a disaster. This ability will be developed as follows:

(a) The critical business processes and supporting IT services will be identified with the help of key stakeholders.

(b) A business impact analysis will be conducted to evaluate the impact over time of a disruption to the critical business processes, thereby producing the minimum acceptable time required to recover the processes.

(c) The potential scenarios and likelihood of their giving rise to disasters affecting the supporting IT services will be identified.

(d) Strategies will be identified that could reduce the likelihood and impact of an IT disaster through improved prevention and increased resilience.

(e) The resource requirements and costs for each strategic option will be identified and the most appropriate option selected and approved by management.

(f) Disaster recovery plans will be developed that contain underpinning detail of the strategic recovery options that contain the disaster scenarios and recovery strategies, procedures, resource requirements, skill levels, data backup arrangements, and roles and responsibilities.

(g) The plans must consider a design of technology for availability, as well as design for recovery.

(h) Critical end-user data (e.g. spreadsheets) will be included in backup arrangements.

(i) Evidence will be obtained that key suppliers and outsource partners have effective disaster recovery plans in place.

(j) The disaster recovery plans must be tested on a regular basis to exercise the plans and to validate the effectiveness of the plans.

(k) The disaster recovery plans will be updated in the event of major changes to the IT environment.

(l) The disaster recovery plans will be reviewed on a regular basis to ensure that it remains relevant.

(m) Everyone involved in the success of the disaster recovery plans will be given relevant training, as well as being involved in testing of the plans.

(n) The adequacy of disaster recovery plans must be assessed after invocation of the plans in the event of a real disaster.

(o) Disaster recovery plans will be aligned with available business continuity plans.

6.2 Information backup

6.2.1 The information backup arrangements that would underpin disaster recovery plans will be defined within disaster recovery plans including data required to recover, retention periods, backup schedules, backup types, location of data sources, and on-site and off-site storage of backups including physical and environmental protection of off-site locations.

6.2.2 Backup data will be tested periodically using test restores.

6.2.3 Everyone will be made aware that they are responsible for the backup of critical or sensitive data on personal computers or mobile devices under their control. For this purpose, file servers will be made available that will be backed up.

6.2.4 Consideration must be given to the ability to access media in the future in a time when technology changes, as well as the possibility of deterioration of media used for storage of records.

6.3 Capacity and performance

6.3.1 The Council will maintain adequate capacity and performance of its information systems through cyclic capacity planning and through continuous automated monitoring of information systems from defined capacity and performance thresholds. Known capacity and performance problems will be treated as IT incidents.

7 Security incident management

7.1 Information systems monitoring

7.1.1 Information systems and infrastructure will be monitored to detect and respond to security events affecting normal operations. This will be done in the following manner:

(a) Information systems and infrastructure that needs to be monitored will be identified.

(b) Events will be logged on the information systems and infrastructure, with due consideration of risk and performance.

(c) Any activity involving privileged access by an administrator will be logged.

(d) Events will be correlated and responded to, either by automated toolsets or through manual review and response.

(e) Security incidents will be logged when activity outside of normal operations is identified.

(f) Event logs will be protected against tampering.

(g) The clocks IT infrastructure will be synchronised with an agreed accurate time source.

7.1.2 The follow Security standards are only applicable to computer and network access:

(a) Maximum Password Age - 40

(b) Minimum Password Length – 6 characters

(c) Password Complexity – enabled

(d) Minimum Password age – 30

(e) Password History – 5

(f) Lockout threshold – 3

7.2 Security incident and problem management

7.2.1 Security incidents will be managed, thereby restoring normal operations in a timely manner. This will be done using the following approach:

(a) All incidents will be logged and documented, recording all relevant information (including classification and priority) so that they can be handled effectively and a full historical record can be maintained.

(b) Security incident escalation rules and procedures will be defined, especially for major incidents.

(c) Everyone in the Council will be made aware of their responsibility to report suspected security weaknesses or incidents.

(d) Security incidents will be escalated, diagnosed and resolved.

(e) A procedure must be maintained to collect evidence in line with computer forensic evidence rules, if the incident will lead to criminal prosecution or disciplinary action.

(f) Security incidents will be analysed on a cyclic basis to establish trends and identify patterns of recurring problems or inefficiencies.

7.2.2 The Council will prevent security incidents from reoccurring by dealing with the root causes of such incidents. This will be done in the following manner

(a) Recurring problems will be identified through incident reporting or other resources.

(b) Permanent solutions or workarounds for problems will be identified, tested, applied and recorded for future knowledge.

8 Information Security references

The following works were consulted in the drafting of this policy. The policy complies with these resources where it makes business sense.

ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements
http://standards.iso.org/ittf/licence.html
http://www.iso.org/iso/catalogue_detail?csnumber=42103

ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management
http://www.iso.org/iso/catalogue_detail?csnumber=50297

ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management
http://www.iso.org/iso/catalogue_detail?csnumber=42107

CobiT 5 : A Business Framework for the Governance and Management of Enterprise IT, 2012
CobiT 5 : Enabling Processes, 2012
http://www.isaca.org

King III Code of Governance Principles - Chapter 5
http://www.iodsa.co.za/downloads/documents/King_Code_of_Governance_for_SA_2009.pdf

RiskIT Framework for Management of IT Related Business Risks, 2009
http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx