FINANCE, AUDIT AND RISK COMMITTEE

27 MARCH 2019

AGENDA ITEM B3

DATA SECURITY AND RISK REGISTER

Purpose of Report

This report discusses the issue of data security for Council staff and elected members.

Recommendations

Officers recommend that the Committee:

1. *Receive the data security and risk register report.*
2. *Agree recommendations on how to improve data security to safeguard confidential or sensitive Council correspondence.*
3. *Agree changes to the Information and Technology (IT) policy N600.*
4. *Agree to add the issue of data security on mobile devices to the Risk register.*

1. Background

Officers have become aware of a potential breach of confidentiality relating to USB stick which was misplaced with sensitive Council information on it and without any password protection or encryption.

Fortunately, the USB stick in question was located within a couple of weeks of notification so the sensitive information has been contained in this case.

This has raised the issue of data sticks and other mobile storage devices without protection posing a significant reputational risk to Council.

Officers recommend that some changes be made to policy and practice to ensure this does not happen again.

2. Summary

Officers have reviewed the Information and Technology Policy N600 in light of a USB stick being temporarily misplaced recently.

The policy now requires mobile devices such as USB sticks, laptops and hard drives to be passworded or encrypted to reduce the risk of inappropriate access to sensitive Council information.

Officers have also taken this opportunity to alter the wording regarding the IT system administrator which will be an internal role from 1 April 2019.

The proposed changes are shown as tracked changes in the attached IT Policy N600 at Appendix 1.

Officers also recommend that this matter be added to the Risk register. The updated Risk Register is attached at Appendix 2.

3. Appendices

Appendix 1 - IT Policy N600

Appendix 2 - Risk Register – Operational and Strategic

Contact Officer: Jennie Mitchell, Group Manager Corporate Support

Appendix 1 - IT Policy N600

INFORMATION AND TECHNOLOGY POLICY

1 Introduction

This policy sets out guidelines for South Wairarapa District Council (SWDC) personnel regarding the use of information technology at SWDC.

2 Purpose of Information Technology

- Information and technology (IT) is provided to support the organisation's core business, to simplify how work is done and make it easier for people to access and use information
- IT systems should facilitate access to the wealth of information collected throughout the sector and provide flexibility for future organisational and technology changes.
- IT systems should improve the operational efficiency and productivity of all staff.

3 Purpose of this Policy

- To provide direction for the responsible use of Email, Internet and telecommunications services by Council staff.
- To protect Council from threats to its information system from viruses ~~and~~ unauthorised software, and inappropriate access to Council information.
- To protect users against unreasonable exposure to risk, objectionable material and allegations of impropriety.
- This policy provides direction and guidance on appropriate uses of the Councils communications infrastructure including Email, web data and telecommunications.

4 Electronic Communications

Electronic communications (phone, mobile phone, photographic/video or Internet based) are council's property and part of the public record, and as such, must be retained or disposed of in accordance with the Archives New Zealand Electronic Record Policy and the SWDC Retention and Disposal Agreement, in accordance with the Public Records Act.

4.1 Legal status

Electronic communications may be used as evidence in a court of law. This includes deleted material and private mail obtained from system backups. (Electronic Transactions Act 2002).

4.2 Context

Electronic communication must be undertaken in a manner which contributes to the safe, effective and accountable operation of the SWDC.

The Electronic communication systems must be kept clear of unchecked and unnecessary mail.

4.3 Scope

These policies apply to all staff and to any other person authorised to have access to the SWDC information systems.

4.4 Appropriate Use - Email

a. Staff may only use their own email address to send or receive emails.

b. Use of the email and Internet is permitted and encouraged for business purposes which support the goals and objectives of the SWDC.

c. The Email and Internet are to be used in a manner that is consistent with SWDC's normal standards of business conduct and communication and as part of the normal execution of an employee's responsibilities.

d. Examples of appropriate use include:

- Email communication with colleagues within SWDC or in other Agencies or other business contacts.
- Conducting research for SWDC projects.
- Retrieving news stories or other information of general work related interest.

e. Staff may utilise the email facility for brief messages of a non-official nature, on an occasional basis. For this purpose, a file involving more than one normal page of text would be significant. Employees who choose to use this privilege do so in the knowledge of and consent to the SWDC's monitoring policy set out above.

f. Users should take all sensible measures to reduce the size of attachments being sent by email, pdf or zip or use hyperlinks when sending internal emails.

4.5 Personal Use - Internet

a. Staff may utilise the internet facilities for personal use, provided the data transmission involved is not of a significant nature. Employees who choose to use this privilege do so in the knowledge of and consent to the SWDC's monitoring policy set out above.

b. Your job comes first. Unless you are an authorized Social Media Manager, don't let social media affect your job performance.

c. Employees are not allowed to disclose SWDC financial, operational or legal information, or any information that pertains to ratepayers and other customers.

d. Dishonorable content such as racial, ethnic, sexual, religious, and physical disability slurs are not tolerated

e. Proper copyright and reference laws should be observed by employees when posting online.

f. Employees are allowed to associate themselves with SWDC when posting but they must clearly brand their online posts as personal and purely their own. SWDC should not be held liable for any repercussions the employee's content may generate.

4.6 Other Matters

a. Users must abide by all software licensing agreements, copyright laws and other applicable regulations.

b. Email is an insecure method of communication and must be treated with caution. Care should be taken to ensure that e-mail sent out is addressed correctly. It should be noted that E-mail does not provide any guarantee of delivery.

c. Users must only access internet from computers they are logged into using their own username.

d. Staff may not download any software onto SWDC Computers without approval from their Manager/Team Leader and the IT department.

~~d.~~e. Staff and elected members utilising mobile storage devices such as hard drives, USB sticks or laptops to store Council information must ensure these are passworded or encrypted to reduce the risk of unauthorised access to sensitive or confidential Council information.

4.7 Information Sourced from the Internet

a. The presence of information on the Internet does not mean that there is a right to copy. Information may only be copied where the author has expressed or implied authorised copying can occur.

b. Staff should not include any information protected by copyright in any Internet publication unless permission has been officially provided.

c. Users should be aware that information on the Internet may be inaccurate or untimely and there is a danger that opinions may be presented as facts. All information should be validated before using for business purposes.

4.8 Social Media including Facebook

a. SWDC staff participating online should participate in the same way as they would with other media or public forums such as speaking at conferences.

b. Staff should seek authorisation to participate in social media on behalf of SWDC. They should not disclose information, make commitments or engage in activities on behalf of SWDC unless they are authorised to do so.

c. Staff need to remember that participation online results in their comments being permanently available and open to being republished in other media.

d. Staff need to stay within the legal framework and be aware that defamation, copyright and privacy laws, among others, apply.

e. If using social media in a personal capacity, staff should not identify their employer when doing so would bring your employer into disrepute

f. Staff should keep in mind that even social media sites restricted to 'friends' are in effect public, as they cannot control what friends do with the information.

g. Staff should always make sure that they are clear as to whether they are participating in an official or a personal capacity. They need to be aware that participating online may attract media interest in them as an individual, so they need to proceed with care regardless of what capacity they are acting in.

5 Prohibited Activities

a. Staff may not use the Internet or email for inappropriate purposes. Examples of inappropriate use include:

- Storing, uploading or downloading software or electronic files for personal use.
- Accessing, transmitting, storing, uploading or downloading material which is obscene, objectionable or likely to be offensive.
- Gambling
- Conducting illegal activities
- Soliciting for personal gain or profit or conducting any personal commercial or commercially related activities
- Making or posting indecent remarks and proposals or conducting any form of harassment
- Uploading or downloading commercial software in violation of its copyright
- Downloading any software or electronic files without reasonable virus protection measures in place
- Passing off their own views as representing those of the SWDC.
- Playing and/or downloading games.
- Sending electronic "chain letters" .

6 Responsibilities

a. The Information Technology (IT) system administrator and Contractor ~~is~~are responsible for:

- Ensuring that the policy and guidelines governing Email and Internet access meet good information management practices and IT security requirements
- Ensuring the availability of support resources to handle Email and Internet user access/installation requirements
- Ensuring the continued availability of the LAN and connections between the LAN and the gateway through which the Internet is accessed
- The management of Email and Internet service availability and security.
- Ensuring adequate virus protection is present on the servers.
- Ensuring all existing IT equipment and software is up to date and fit for purpose and fully functional.
- Ensuring that storage is maintained at reasonable levels.

b. Staff are responsible for:

- Adhering to the email and Internet policy.
- Immediately informing the IT system administrator~~contractor~~ of any virus detection alerts or spam email.
- Immediately reporting any weaknesses or breaches as soon as they become aware of them.
- Validating and authenticating information retrieved via email and/or from the Internet before it is used for business purposes.
- Ensuring that they log out of the Internet once they have completed their search.
- Ensuring that all e-mail that they send outside the SWDC has the SWDC e-mail disclaimer displayed.
- Ensuring information stored on USB sticks, hard drives and laptops are passworded or encrypted to reduce the risk of unauthorised access to sensitive or confidential Council information.
- Users must not share their password, user identification or other secure information.

7 Recommended Practices for Retention and Disposal of E-Mail and Internet Material

a. The person who has the most responsibility for the topic covered should print or file the following:

- Messages which formerly would have resulted in a file note being made.
- Messages that contribute to a greater understanding of significant documents / events.
- Formal communications between employees, for instance, minutes and submissions.
- Messages requesting, authorising or commenting on the expenditure of money or other resources, or any action involving such expenditure.
- Messages containing instructions of a significant nature, including notifications of changes of policy, and establishment of precedents.

b. Delete without filing the following:

- Routine, short term messages.
- Non-work material, and circulated material sent for information purposes only.

Keep the amount of electronic mail stored in the system to a minimum. That is, always empty deleted items on exiting, save important sent mail and / or attachments, and review e-mail messages on a regular basis.

8 SWDC Website

8.1 Introduction

The SWDC website has been established as a mechanism for communicating key information with ratepayers and other stakeholders.

Group Managers are responsible for the quality and integrity of the information on the website. The policies and guidelines for the use of the website are designed to ensure that SWDC staff are aware of their responsibilities and roles and appropriate usage.

8.2 Scope

These policies and guidelines will apply to all SWDC staff and contractors assigned access rights to the website.

8.3 Policy

a. The use of the website is intended exclusively for work undertaken for or by the SWDC.

b. Access to the website is confined to SWDC staff and approved contractors working for the SWDC.

c. Staff must agree to the policies and guidelines.

d. Sensitive or confidential information must not be exchanged via the website.

8.4 Responsibilities

a. SWDC Staff:

- Adhere to the policies and guidelines for website use and information disclosure.

b. SWDC Management:

- Provide and assure the quality of content for inclusion on the website.
- Copyright on internal and external publications must be clearly identified and adhered to.
- Standard quality controls should apply to information loaded onto the website.
- Develop and disseminate polices and guidelines for the use of the website.

c. IT system administrator and contractor:

- Manage the infrastructure for website access and usage, including security.
- Manage user identification and authorisation.

d. Website Developer (contractor):

- Maintain the structural integrity of the website.
- Training and support to users where needed and approved.

9 Facsimile and Telephone Policy

All staff must use facsimiles and telephones including mobile phones in a manner which is consistent with the SWDC standards of conduct and communication and as part of the normal execution of an employee's responsibilities.

In addition, as public servants, we are expected to maintain high standards of ethical and professional behaviour which is not only defensible, but must be seen to be beyond reproach.

9.1 Appropriate Use

Staff must at all times comply with the law governing the use of telephones and facsimile equipment and should be aware that certain improper uses could constitute a criminal offence.

In addition to the requirements laid down by law, the *SWDC* prohibits the use of *SWDC* facsimiles or telephones for:

a. Obscene or objectionable communications.

b. Harassment.

c. Conducting gambling or distribution of "chain letters".

d. Conducting any illegal activities.

e. Soliciting for personal gain or profit or conducting any personal commercial or commercially related activities.

9.2 Personal Use

The SWDC incurs the cost of the telephone system and facsimile machines in order to conduct official business. They are not provided for personal use and, because such personal use incurs an unplanned cost for the business, it is a privilege. Occasional and brief personal use is permitted, provided that the calls are local and no long distance charges are incurred. For this purpose SWDC defines the local area as including the SWDC Boundaries.

Private toll calls, including local calls to mobile telephones, charged to the SWDC are prohibited (except in circumstances set out below). Any such calls must be made "collect" or utilising a calling card or the transfer charges facility. In the event of an emergency situation where it is not possible to utilise such services an employee may, with prior approval from a group manager, manager or team leader, place a private toll call provided arrangements are made immediately thereafter to ascertain the costs and make reimbursement to SWDC.

9.3 International Toll Calls

Any international telephone calls for official purposes must be approved in advance by immediate Manager.

10 Mobile Phones

Personal use is permitted within the package provided. Expenditure outside this will need to be reimbursed by the employee to SWDC.

11 Breach of Policy

Any breach of this policy, either in terms of not observing prohibitions, limits on personal use or requirements to receive appropriate authorisation is "misuse or unauthorised use of SWDC property". As such it constitutes misconduct under SWDC's discipline and dismissal policy.

12 Monitoring Rights

SWDC will at the discretion of the Chief Executive or a member of the Management Team, monitor, access, retrieve, read and disclose communication as necessary to verify compliance with this and other policies, in particular to detect and investigate inappropriate use. SWDC may also access communications as necessary to meet urgent business needs or when the employee is unavailable and timing is critical.

Appendix 2 - Risk Register – Operational and Strategic

OPERATIONAL RISK MANAGEMENT as at March 2019

Risk Identification			Risk Assessment		Risk Management				
Risk Category		Risks	Likelihood H/M/L	Impact H/M/L	What are we already doing about it? (mitigating factors)	What more can we do about it?	Timescale	Person Responsible	Reviewed Level of Risk
Operations	Customer Service	Dissatisfied customers, increased staff turnover, difficulty recruiting staff	M	M	Standard Operating Procedures (SOPs) completed for all roles, Assertiveness training for all staff	Training, SOP's, Reiterate expectations, improve internal comms	On-going	Group Managers	
	Insurance	Fails to meet issue	L	H	Annual review, Group insurance with MDC and CDC	Risk assessment, review what else could be covered, stay abreast of 60/40 LAPP review	Annually	CEO & GMCS	
	Document Management System	Loss of information, difficulty in answering OIA, failure to meet legislative requirements	M	H	K drive reorganised to reflect paper filing system - partially rolled out. Scanning building files to electronic	Continue to roll this out, Continue with scanning of other files	On-going	CEO, GMCS	
	Legislative Change/Compliance	Cost and complexity	M	H	Keeping abreast changes, Attending training, Incorporating in plans and policies as soon as known	Complete legislative compliance review Increase awareness of obligations Communicate policy change	On-going	CEO, Group Managers	
General	Transitioning change	Dissatisfied customers, Cost, Increased staff turnover	M	H	Communication	Engage with staff Implement Change plans as required	On-going	CEO, Group Managers	
	Poor culture, morale, customer perception	Dissatisfied customers, reputation	M	H	Need to ensure we continue to improve as a business and make gains for the community, Code of conduct	Best Council, Internal comms	On-going	CEO, Group Managers	
	Bribery	Organisational reputation	L	M	Code of Conduct	Reiterate expectations		CEO, GMCS	
Finance	Cost Management	Loans, missed opportunities	H	M	There are a lot of cost pressures around rates and this will remain for many years. Reduced depreciation funding via rate. Lowered interest via LGFA. Follow policies esp delegations	Work on more shared services and synergies with other Tas, Regular financial reporting	On-going	CEO, Group Managers	
	Debt Management/Interest	Loans, unnecessary cost, cash flow, bad debt write offs	M	H/M/L	Finance Strategy & Policies. Interest rates low at the moment, LGFA fixed interest rates reduce risk. Some risk whereby if the LGFA defaults, the borrower Councils will/may have some liability. The risk of default is low in our view. Systems in place for debt management reduces risk of bad debts.		On-going	CEO & GMCS	
	Efficient v Effective v Cost	Perception/reputation	M	H	Statutory Obligation	Continue to ensure all know the cost drivers and ensure we look at the best way to do things	On-going	CEO/Council	
	Water leaks - waivers if leak is fixed but water still lost	Water loss/bad debts	M	M	Follow up with overdue accounts/spinning meters	Look into smart meters		GM Infrastructure	
	Balancing rates affordability with requirements and expectations	Perception/reputation	H	M	Publicised policies and covenants	Comms manager - tell the stories	On-going	CEO/Council	
	Fraud	Payroll Fraud, False Invoicing, Intercepting revenue, removing books without issuing, false expense claims	L	H	Complete fraud review Review cash management procedures Separation of duties Mail cleared in open space Financial delegations policy	Implement findings from fraud review	On-going	CEO/Audit & R WP/GMCS	
	Health & Safety Incident	Death, Serious Injury, Reputation, Legal Costs	M	H	Training Staff Carrying out site inspections Providing protective equipment required Inducting Staff	Training in new Legislation when adopted to fully understand responsibilities	On-going	GM P & E	
	Managing Staff Turnover/Staff Cover		H	M	Turnover offers opportunities - need to assess reasons for turnover	Procedures Succession Planning	On-going	CEO	

HR		Reputation, Knowledge base, continuity, customer service, Wellbeing	M	M	Police checks Reference checks Performance management system Clear job descriptions for every position Ensure all council property returned Provide exit interview Track all leave and lieu	Ensure at least two members of staff can carry out all functions Have standing operating procedures for all roles	On-going	All Managers	
	Staff working long hours and/or not taking holidays	Morale, accuracy, health, safety and wellbeing of staff	H	M	Policy for Managing Time in lieu & Annual leave Use of the sign out board		On-going	All Managers	
	Time bandits - personal and business discussions in shared office space	Productivity, customer service	H	M	Monitor productivity		On-going	All Managers	
	Taking unnecessary leave or leave at inappropriate times	Customer service, culture	H	M	Managers to manage leave approvals appropriately		On-going	All Managers	
	Keys - being used by unauthorised people.	Reputation, fraud	L	M			On-going	All Managers	
	Cars being used for personal errands	Reputation, cost	L	L	Policy	Reiterate to staff	On-going	All Managers	
	Personal Grievance - bullying, abuse, discrimination	Culture, Stress, productivity, legal costs	M	M		Review HR Policy, Staff member with HR portfolio, Manager Training	On-going	CEO	
Infrastructure	Change in funding of Cape Palliser Road	Cost, resource	H	M	Reducing by 8% pa from 2018/19 until reaches 52%. Rural roading reserve in place to partially cover this.		2019 to 2024	GM Infrastructure	
	Earthquake buildings	Derelict buildings	H	M	New Regulations set late 2015 Investigate relief policies	Look at rates remission policy in line with other councils. Implement Plan for buildings not compliant in time frame	TBC	GM P & E	
	Martinborough Town Hall (Waihinga Centre)	Earthquake, Cost over run, timeline over run	M	M	Critical funding points. Monitor project costs and forecast monthly		2017/18 to 2018/19	CEO	
	Maintenance /Failure to future proof assets and amenities to cater for growth	Failure to manage assets , drop in customer service, dissatisfaction of ratepayers, reputation	L	H	Complete scheduled cyclical maintenance as planned Update and implement Asset management plans. External reviews e.g. Wellington water, ID growth forecasts	Consider Amenities asset management plan, Spatial plan	On-going	GM Infrastructure/ Amenities manager	
	Bonny Glen Resource Consent	Consent not reissued	H	M	Alternate sites	Monitor situation	2019	GM Infrastructure	
	Waste Water (FTN High priority)	Failure to meet consent obligations, legal costs, timing and budget not met	H	M	Understanding the impact of consent conditions - mainly about the term, the shorter the term the higher the initial rates impact. Monitoring actual spend vs budget monthly. Pursuing cost savings from suppliers	Continue to work through consent application process	FTN Consent in progress	CEO/GM Infrastructure/ Asset & Operations Manager	
	Flooding incidents/Claims from ratepayers	Incorrect LIMs issued, incorrect information provided to developers	M	M	Improving recording systems and looking at possible disclaimers on LIMs, identify appropriate building platforms for new sections and follow through at Building consent stage.	Continue to ensure record keeping is up to date and comprehensive and flood risk is a key party of subdivision review and sign off	On-going	GM P&E	
	Water Availability/Use	Health	L	H	On-going management and education Continue discussion with Regional Council /Minimise infrastructure leaks	More education/promotion of water conservation - Comms manager. Use website, facebook etc	On-going	GM Infrastructure	Await govt recommendations on 3 waters
Information Technology	NCS Access (User control)	Loss of data	L	H	Limited access to user control		On-going	Tech Solutions	
	Personal Internet Usage	Time, cost	H	L			On-going	All Managers	
	Technology Changes (IT/Broadband/Cell Phone)	Loss of data/reputation/security	H	L	Managed by contractor	New disaster recovery regime	On-going	CEO	
	Cyber Bullying	Staff wellbeing	L	H	Firewalls in place		On-going	All Managers/Tech Solutions	
	People gaining entry - Visitors not signing in	Theft, reputation	M	M	Sign in book and entrance control updated with key pad		On-going	Receptionists	
	Confidential/Sensitive Information not passworded or encrypted	Reputation	M	H	Password or encrypt all mobile storage devices	Updated IT policy to reflect this	On-going	All Staff & Elected members	
	Confidential/Personal Information left in public areas	Reputation	M	H	Keep conversations quiet. Go to meeting room if necessary		On-going	All Staff	
	Database Information theft/Cyber bug corrupting system	Loss of data & Reputation	M	H	Managed by contractor, firewalls in place	Disaster recovery upgrade	On-going	Tech Solutions	

High | Medium | Low | Priority | Project

STRATEGIC RISK MANAGEMENT as at August 2018

Risk Identification		Risk			Risk Management				
	Risk Category	Risk	Likelihood H/M/L	Impact H/M/L	What are we already doing about it? (mitigating factors)	What more can we do about it?	Timescale	Person Responsible	Reviewed Level of Risk
General	Communication	Failure to gain stakeholder engagement, lack of transparency, statutory consultation not met	M	H	Regular Staff meetings, Rates newsletter, engagement through Facebook & website, professional/proactive approach, customer follow up, Comms Manager	Regular Team Meetings Regular leadership meetings Website & Facebook current	On-going	CEO	
	Leadership	Mayor or CEO transition, High turnover of Councillors or Senior Managers	L	L	Lead by example, honesty, positive delegation. Good induction processes, pre-election briefings for potential candidates	Training, organised approach, induction, excellent communication	On-going	CEO & Group Managers	
Demographics	Aging Community	Rates arrears, infrastructure failure	L	L	Monitor demographics and facilities	Monitor	On-going	Council	
	Schools not performing	Decreasing house sales, failure to attract families resulting in aged community	L	L	No ability to manage	Monitor	On-going	N/A	
Economy	Economic Downturn/recession	Increase in rates arrears	M	M	Increased rates debtors but we have the power to sell so ultimately this won't impact SWDC		On-going	GMCS	
	Low employment/Lack of employees	Increase in rates arrears, businesses including Council can't find staff	M	M	Wairarapa Economic development strategy		On-going	CEO	
	Lack of availability of affordable residential property		M	M	Researching new development options, Spatial plan	Not our job, we can only create the environment	On-going	GM P & E	
	Commercial Buildings not available to drive growth		L	L	Combined district plan review, Spatial plan	Not our job, we can only create the environment	On-going	CEO	
Environmental	Coastal Erosion	Decreased rating base	H	H	Work with NZTA on mitigation Work with land owners		On-going	GM Infra	
	Weather event	Infrastructure, business continuity	H	H	Have CDEM plan through WREMO Community Civil defence Centres Train staff and community to be prepared		On-going	GM Infra	
	Pests/bugs/disease	Agriculture and horticulture down turn	H	H	Biosecurity Act		On-going	GM P & E	
	Climate Change	Erosion of rateable land	H	H	Assess potential impact	Monitor	On-going	Council	
Governance	Treaty Settlement		H	M	Treaty settlement in progress, keep communications open with treaty settlement parties	Liaising with recipients Understanding our obligations	Next 10 years	Council	
Transport	Remutaka Hill Road	Cut off major city	M	M	Lobby to ensure good as can be and contribute to the regional land transport plan		On-going	Council	
	Public Transport	Reduce accessibility and ease of movement in region	M	M	Advocating for Public transport to meet the communities needs, Govt funding approval for rail improvements 31 Aug-18 - will take several years to implement		On-going	Council	

High | Medium | Low | Priority