Far North District Council
Te Kaunihera o Tai Tokerau ki te Raki

HE ARA TĀMATA
CREATING GREAT PLACES
Supporting our people

ARF010 Data Governance Risk

Risk Status Progress Report June 2022

Prepared: 27/05/2022

Description of risk and impact

Because of	There is a chance that…	leading to…
Lack of formal data governance	Data quality may be negatively impacted Data may be inappropriately used Data breach may negatively impact Council reputation We are non-compliant with relevant legislation	Slow, ineffective decision making Lack of confidence in data and decisions made on the data Increased organisational risk Mistakes/errors Ineffective and poor processes Inefficient customer service Legal liability and sanction Reputational damage to Council and Councillors

Data governance is the overarching framework that outlines the creation, maintenance, disposal and protection of data. The objectives of data governance are:

- Assure data security and data quality
- Maximise the benefit generation of information
- Designate accountability for data quality
- Enable evidence-based policy development
- Increase consistency and confidence in decision making
- Consistent reporting
- Enable evidence-based business cases and strategies.

Existing Treatments

Three active programmes of work will also result in improved data governance. These are:

1. The Enterprise data warehouse programme.
2. Program Darwin: this is now recognized as a strategic organisational risk on the top risk dashboard as ARF014 Programme Darwin
3. The Business Intelligence strategy.

High level treatment plan and progress up-date:

High level treatment plan:	Progress update:
Data governance policies	Underway: **Data Governance Policies:** Draft Data Governance Policy requires revision and signoff DATA GOVERNANCE POLICY (A2685114) Draft Data Protection Policy requires revision and signoff Data Protection Policy (A2685122)

High level treatment plan:	Progress update:
	Draft Data and Information Management Policy requires minor revision and signoff Data and Information Management Policy DRAFT (A3111956) Draft multimedia Policy requires minor revision and signoff Multimedia Policy (A3100700) Data Quality Project has not progressed 210122_Project Charter_Data Quality_v1.0 (A3067389) **ICT Policy System:** ICT Operations and Delivery team have implemented an online IT Policy System in collaboration with Kaon Security Ltd to move to a more effective ICT policy environment, and to provide better governance around ICT use and security. The policies have been reviewed and updated by the ICT Operations and Delivery team, as well as other subject matter experts from around the business (Democracy Services, Information Management, Business Continuity Planning, Legal Services). They are now waiting to be reviewed and approved by the CEO and SLT. This ICT Policy System is an enhanced cloud-based solution that has been developed to assist organisations create, deliver, and maintain a comprehensive suite of ICT policies. This system streamlines the engagement between the users and the content, whilst providing a rich source of guidance on how they should interact with organisational IT systems and data. With security attacks against organisations like ours increasing we must ensure our systems are protected against these threats. One of the foundational steps in achieving this is to document the rules and guidelines around system management, operation, and use. By complying with these rules and guidelines we are protecting our systems. Information security is all about keeping corporate information safe. The policies address the need to protect confidential and sensitive information from disclosure, unauthorised access, loss, corruption, and interference, and are relevant to information in both electronic and physical formats. Information security can be defined in three areas: • **Confidentiality** - Information must not be made available or disclosed to unauthorised individuals, entities, or processes • **Integrity** - Data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes • **Availability** - Information must be accessible and useable on demand by authorised entities. The ICT policy system will be updated with any relevant changes to legislation, standards, and guidelines on a regular ongoing basis.
ALGIM (Association of Local Government Information Management) Local Government ICT Security Framework – SAM for Compliance.	In place and ongoing: In 2020 the ICT Operations and Delivery team implemented an ICT Security Framework (SAM for Compliance). This framework contains a series of policies, procedures and processes that lower risk and vulnerability, and increase confidence in an ever-connected world. Safe, secure, and functional

High level treatment plan:	Progress update:

	information technology systems are vital for the successful operation of our Council.
	
	ICT Operations and Delivery team have implemented or are currently working on a variety of ICT security improvements:
	
	• Multi Factor Authentication (MFA)
	• Single Sign On (SSO) for systems, e.g. CiAnywhere HRP, Freshservice, Mariner 7, Objective IQ, PeopleSafe, Percipio, Promapp, Smartway2
	• Device storage encryption and BIOS password set up on new devices
	• Firewall health check
	• Anti-virus software health check
	• Penetration testing
	• Network user account and contractor user account reviews
	• Computer Security Incident Management system
	• External email warning message
	• National Cyber Security Centre - Microsoft Exchange Server Scan
	• National Cyber Security Centre - Data Breach Service
	• Secure E-waste disposal - Digital Wings
	• Annual upgrade programme - Objective, Pathway, ePathway, TechOne
	• Microsoft 365 security improvements (external review underway May 2022)
	• ICT audit undertaken by Audit NZ
	• Upskilling of ICT staff via ongoing training and webinars
	• Cybersecurity Awareness Programme for all staff and elected members - Phriendly Phishing
	• Microsoft Intune rollout
	• InPhySec - Managed Security Service pilot underway
	• Crowdstrike - Endpoint threat protection pilot underway
	  ○ IT hygiene
	  ○ Anti-virus
	  ○ Endpoint detection and response
	  ○ Threat hunting
	  ○ Vulnerability management
	  ○ USB device monitoring
	• Offsite and off network backups proposal
	• Automated server patch management – WSUS
	• Self-service password reset
	• Wi-Fi replacement project.
	
	The Assurance, Risk and Finance Committee are provided with a Technology Update Report with a focus on cybersecurity every six weeks.

FNDC needs to implement the requirements of the internal policy “PC033 Privacy Policy”, adopted August 2019, such as agree designated Privacy Officers.	Implemented. The Privacy Officers are appointed by role. These roles are the Manager – Legal Services and the Legal Services Officer.

Where are the gaps? / what more could we be doing?

Inherent Risk:	**Trend**	**Residual Risk:**	**Accountable:**	CEO	**Date raised:**	29/11/18	**Report frequency:**
	Increase		**Responsible:**	Chief Digital Officer	**Date accepted:**	30/05/19	Six monthly