



**Item: 6**

**Asset Management Sub-committee: 28 January 2025**

**Information Technology and Cybersecurity Strategy.**

**Report by Corporate Director for Neighbourhood Services and Infrastructure.**

---

## **1. Overview**

- 1.1. Since the publication of the previous Information Technology (IT) Strategy, covering 2021 to 2024, the Council's IT environment continued to undergo significant levels of transformation and renewal, delivering improvements in capacity, capability, connectivity, and resilience.
- 1.2. That period has also witnessed further concern regarding the security of organisations world-wide from cyberattacks, including incidents affecting Councils, Agencies and Health Boards in the Scottish Public Sector.
- 1.3. The IT Strategy has been updated and covers both IT Service provision and cybersecurity as core tenets of the draft IT and Cybersecurity Strategy 2025-2029, attached as Appendix 1 to this report.
- 1.4. Cybersecurity is not the sole responsibility of technical support staff but requires shared ownership of responsibility across the organisation. Therefore, the Cybersecurity aspect sets out the organisational roles and responsibilities to ensure clarity of responsibility.
- 1.5. Aligned to the draft strategy is the draft delivery plan. As the previous delivery plan had been largely completed, a reset has been done, placing greater and more detailed objectives as a continuous improvement process.
- 1.6. The main focus in this strategy compared with previous strategies will be:
  - Shift in focus to greater Cybersecurity.
  - Emerging technologies.
  - Artificial intelligence.
  - Mobile working.
  - Trend towards Cloud Hosting systems.
  - Increased Cybersecurity threat levels.

## 2. Recommendations

2.1. It is recommended that members of the Sub-committee:

- i. Approve the Information Technology and Cybersecurity Strategy 2025-2029, together with Delivery Plan, attached as Appendix 1 to this report.

### For Further Information please contact:

Thomas Aldred, Service Manager (IT), extension 2152, Email [Thomas.aldred@orkney.gov.uk](mailto:Thomas.aldred@orkney.gov.uk).

### Implications of Report

1. **Financial** – The report does not attempt to quantify the financial implications arising from the Strategy. Any costs arising from works associated with the delivery plan will require to be funded from within existing revenue or capital budget allocations, with any request for additional funding required to come forward as a separate report for consideration.
2. **Legal** – No implications.
3. **Corporate Governance** – No implications.
4. **Human Resources** – No implications.
5. **Equalities** – An Equality Impact Assessment has been undertaken and is attached as Appendix 2.
6. **Island Communities Impact** – No implications. IT delivery solutions will be evaluated and planned with relation to need, risk, changes in legislation, corporate priorities and budget restraints independent of location.
7. **Links to Council Plan** – The proposals in this report support and contribute to improved outcomes for communities as outlined in the following Council Plan strategic priorities:
  - Growing our economy.
  - Strengthening our Communities.
  - Developing our Infrastructure.
  - Transforming our Council.
8. **Links to Local Outcomes Improvement Plan** – None directly related to the recommendations in this report.
9. **Environmental and Climate Risk** – None directly related to the recommendations in this report.
10. **Risk** – None directly related to the recommendations in this report.
11. **Procurement** – None directly related to the recommendations in this report.
12. **Health and Safety** – None directly related to the recommendations in this report.
13. **Property and Assets** – None directly related to the recommendations in this report.

- 14. Information Technology** – Yes, Strategy to deliver IT services for the period 2025-2029.
- 15. Cost of Living** – None directly related to the recommendations in this report.

#### **List of Background Papers**

None.

#### **Appendix**

Appendix 1: IT and Cybersecurity Strategy and Delivery Plan.

Appendix 2: Equality Impact Assessment.



# Contents

Section 1 – Executive Summary.....	4
1.1 Introduction.....	4
1.2 Strategic Overview .....	4
Section 2 – Objectives .....	6
2.1 Objectives of the IT and Cyber Security Strategy .....	6
Section 3 – Cyber Security .....	7
3.1 Types of threat: .....	10
3.2 Vulnerabilities .....	10
3.3 Risk Management .....	11
3.4 Cyber Security Strategic Targets .....	12
Chief Executive .....	13
Senior Information Risk Owner (SIRO).....	13
Corporate Leadership Team.....	14
Corporate Director for Neighbourhood Service and Infrastructure .....	14
Head of Property, Asset Management and Facilities.....	14
Service Manager (IT).....	14
Service Manager (Safety and Resilience) .....	14
System owners.....	14
System administrators .....	14
Data Protection Officer .....	15
Freedom of Information Officer.....	15
Information Governance Officer .....	15
Information Security and Assurance Officer .....	15
Section 4 – Governance .....	17
4.1 Structures .....	17
Section 5 – Infrastructure.....	18
Strategic Targets .....	18
Section 6 – Internal and External Customer Communications.....	19
Strategic Targets .....	19
Section 7 – Digital.....	20
Strategic Targets .....	20
Section 8 - Customer Focus .....	21
Strategic Targets .....	21
Delivery of the Strategy .....	22
Appendix 1 - IT and Cyber Security Strategy Delivery Plan 2025-2029 .....	23
1.1. ....	23

- 2. Introduction..... 23
  - 2.1. ....23
  - 2.2. ....23
  - 2.3. ....23
  - 2.4. ....23
- 3. Actions to Support IT Strategy Objectives ..... 24
  - 3.1. Cyber Security Objectives .....24
  - 3.2. Governance Objectives .....29
  - 3.3. Infrastructure .....31
  - 3.4. Internal and External Customer Communication .....36
  - 3.5. Digital Objectives.....38
  - 3.6. Customer Focus Objectives .....40



# Section 1 – Executive Summary

## 1.1 Introduction

Since the publication of the previous IT Strategy, covering 2021 to 2024, the Council's IT environment continued to undergo significant levels of transformation and renewal, delivering improvements in capacity, capability, connectivity, and resilience.

Of greatest significance has been the ongoing establishment of the Microsoft 365 solution which has enabled the adoption of hybrid staff working solutions including capabilities in remote working.

These developments have opened up improvements in how the organisation works, how it meets, how documents are stored and shared and brought real flexibility to the user experience.

However, these changes in how the organisation works have increased demands to maintain service availability for a diverse workforce while keeping the integrity of the data we hold, safely and securely.

The main focus in this strategy compared with previous strategies will be:

- Shift in focus to greater Cybersecurity
- Emerging technologies
- Artificial intelligence
- Mobile working
- Trend towards Cloud Hosting systems
- Increased Cybersecurity threat levels

## 1.2 Strategic Overview

While a digital strategy sets up goals and objectives for how specific functions and services of the Council can be delivered digitally (e.g. processing payments, managing assets, scheduling transport), this strategy details the Council's IT infrastructure and technology foundation that underpins Council operations.

The delivery undertaken by the IT Service year on year shows that expectation to engage with the Council via digital channels continues to increase. However, limitations in consumer connectivity in Orkney remain a constraining factor in progress and maintains a complementary demand for the traditional means of face to face and telephone.

This means that service delivery must continue to match these demands, whilst recognising that for our community, traditional methods must continue to work well and be maintained.

Providing cost effective secure IT services for our Services and Community is something the IT Service takes pride in. IT, done well, reduces workloads, simplifies processing, supports better systems integration, and provides efficiencies.

Simplifying IT sits at the heart of the successful adoption of digital solutions, ensuring good practice is well understood and ensuring secure practice. If it is hard to understand it is hard

to support and hard to secure. IT needs to stay simple as far as practical. Therefore, we will adopt a common approach to technology as much as is practical, so that solutions are repeatable, equipment is standardised, and economies of scale can occur by doing many things the same way as best we can. IT should not be a “pick and mix” solution and what works in one area should be broadly repeatable.

Distributing this offering across the organisation and across the complex geography of Orkney is a growing demand and meeting this need by providing an IT solution that is common, simple and everywhere underpins this strategy, along with the need to ensure and assure from a standpoint of privacy, security and governance.

Well established, effective IT governance, and an open communications approach, is supported by regularly reporting progress to leadership, colleagues and members. We have established an IT culture of proactively asking for and listening to feedback on our services and have adopted a continuous improvement approach based on identified requirements.



## Section 2 – Objectives

### 2.1 Objectives of the IT and Cyber Security Strategy

Effective and efficient use of IT by Orkney Islands Council is vital in ensuring the delivery of many of the Council's key objectives. There are significant challenges in sustaining a comprehensive and secure IT environment with Information Security being at the very core of what IT do ensuring data confidentiality and integrity is maintained, but at the same time ensuring the correct level of availability to those that require it.



*Fig1: Ensuring data information security - CIA Triad*

To ensure that this new 5-year strategy covers the objectives this IT and Cyber Security Strategy will cover the following areas.

- Cyber Security
- IT Governance
- Infrastructure and Systems
- Internal and External Customer Communications
- Digital
- Customer Focus

This document outlines our direction, highlights our priorities and compliments our Digital Strategy. It reflects feedback from our consultations and aims at providing a strategy that will support a flexible modern agile approach to providing IT services.

## Section 3 – Cyber Security

The Cyber Security Strategy has been incorporated into the Council Information Technology Strategy and has been introduced in response to the increasing threat from cyber criminals and several successful and high-profile cyber-attacks on public and private organisations. The purpose of this strategy is to give assurance to stakeholders of the Council's commitment in delivering robust information security measures to protect citizen and stakeholder data from misuse and cyber threats, and to safeguard their privacy through increasingly secure and modern information governance and data sharing arrangements both internally and with partners.

Across the globe, cyber-attacks are growing in frequency and becoming more sophisticated. Amidst the increased use of information technology since the 2020 Covid-19 pandemic, cyber criminals have become more active, and our exposure has increased. When cyber-attacks succeed the damage can be significant; with personal, economic and social consequences.

Cyber-attacks will continue to evolve, which is why we will continue to work at pace to stay ahead of all threats. The Information Technology Strategy which continues to ensure we will place stakeholders at the heart of everything we do in a changing technological landscape. The measures outlined in this strategy will deliver assurance and compliance in the way we operate and deliver our services, supporting the Council to remain at the forefront of cyber resilience. To ensure this strategy continues to deliver robust Cyber security high level scrutiny will be achieved by the Corporate Risk Register and twice-yearly review by the Policy and Resources Committee.

In technology terms, the legacy of the 2020 Covid-19 pandemic is a transformation in how organisations, including the Council, deliver and utilise technology with more remote working combined with office-based activity.

While these changes have delivered significant benefits to the workplace, they have also presented new and lucrative opportunity routes for cyber-criminal activity. Cyber security has become, and will remain, a key responsibility for all of us collectively and as individuals.

The prevalence of digital services and the dependence on their confidentiality, integrity, and availability means that a robust and comprehensive cyber security strategy and framework are vital to ensure that appropriate measures are in place.

Systems and data must conform to secure access arrangements and information storage must be protected, carefully curated and still available for use by those authorised to do so.

Vendors must comply with effective and recognised standards of security, robustness and service, both in the organisation that they are and the product that they produce, supply and support.

Information systems must have clearly defined internal owners within our organisation, responsible for the functionality, controls and development roadmaps of systems we use.

Finally, staff training is also an important factor in combating cyber threats and reducing risk in a constantly changing online environment. Ongoing programmes seek to raise awareness of cyber security and to strengthen the human element of cyber defence. This strategy is our cyber security commitment, both to the people we represent and the national interest; and supports delivery of the Information Technology Strategy and in line with Council Plan priorities by providing a framework for the Council to securely harness the benefits of digital technology for the benefit of all.

Orkney Islands Council is increasingly dependent on the use of digital technologies to provide services and to communicate with its citizens. With the increase in the use of publicly visible technology, e.g. websites, payment portals, and other publicly available internet-based services, there is an associated increased risk of exposure to threats from criminal and other malicious parties. There has been a significant rise in the incidence of cyber-crime in recent years with no signs of this trend abating. The Council must rise to the challenge of meeting this increased risk through implementation of strong security controls and raising staff awareness while at the same time enabling the use of innovative and progressive technological solutions where possible.

Through delivery of this strategy, we will comply with and embed the principles of good cyber security practice based on the controls of ISO 27001:2022, an internationally recognised standard for information security. We will also follow the “10 Steps to Cyber Security” framework published by the National Cyber Security Centre.

The scope of this strategy includes all of the Council’s information systems, the data held on them, and the services they help provide. It aims to increase cyber security for the benefit of all citizens, businesses, partners, and stakeholders.

The world today is dependent on connectivity to function effectively, and this dependence leads to risks from malicious actors looking to disrupt services for political or financial gain. The risks posed by cyber threats are widespread and pervasive across all sectors. Well managed cyber risk is an enabler for organisations to function and protect their critical assets as well as maintain functional integrity and maintain confidence with partner agencies and stakeholders.

Failure to manage cyber risk can result in severe impacts including:

**Financial impacts.** Direct costs for remediation and recovery of systems, forensic investigations, costs of additional equipment to assist in recovery of systems and services, potential regulatory penalties.

**Data impacts.** Loss of access to data, data theft.

**Operational impacts.** Loss of access to systems for a prolonged period, staff demotivation stress and burnout.

**Reputational impacts.** Erosion of trust and confidence from our citizens, reduced levels of trust from partner agencies, negative publicity in media.

**Regulatory impacts.** Imposition of penalties and improvement notices, ongoing monitoring and auditing from regulators.

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs and data from attack, damage, or unauthorised access. Cyber security is the practice of ensuring the confidentiality, integrity and availability (CIA) of information held on digital systems.

- **Attacks on Confidentiality:** This is where a threat actor steals or copies personal information for criminal or malicious purposes.
- **Attacks on Integrity:** This is where a threat actor seeks to corrupt, damage or destroy information held on systems.
- **Attacks on Availability:** This is where a threat actor attempts to prevent legitimate access to systems to cause reputational damage. Denial of service attacks are a typical route for this.

In order to deliver services, the Council collects, processes, transmits and stores large amounts of personal and sensitive data and transmits sensitive data across networks to other devices.

A successful cyber-attack would interrupt the Council's ability to deliver services, many of which serve our most vulnerable residents, for an extended period as well as incurring large recovery costs and significant damage to our reputation.

A successful cyber security approach enables us to protect information, the systems that are used to process or store it, ensures our services are kept up and running, and is vital in ensuring the public trusts the Council to protect their information and store it securely.

The Council continues to use an increasing range of technology, from apps and the cloud to locally hosted devices. Much of our business is done online, e.g. corresponding with residents and local businesses, carrying out case work, and reviewing reports for Council meetings.

This direction of travel is expected to continue and accelerate, making effective cyber security ever more crucial in protecting against new types of threats, risks and vulnerabilities.

## **Threats**

A threat left unchecked could disrupt the day-to-day operations of the Council and the delivery of local public services, and ultimately has the potential to compromise the security of other organisations.

## 3.1 Types of threat:

### Cyber criminals and cyber crime

Cyber criminals are generally working for financial gain, most commonly, for the purposes of fraud: either selling illegally gained information to a third party, using it directly for criminal means, or denying legitimate access to information in order to hold it to ransom.

Key tools and methods used by cyber criminals include:

- **Malware:** Malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals.
- **Ransomware:** A type of malware that encrypts data to prevent legitimate access. This type of criminal action is usually followed by a ransom demand for a means of decryption to regain access or to prevent stolen data being published on criminal websites.
- **Phishing:** Emails purporting to come from a trusted source and intended to extract sensitive or personal information from the recipient.
- **Hactivism:** Hacktivists will usually attempt to take over public websites or social media accounts to raise the profile of a particular cause. When targeted against local government websites and networks these attacks can cause reputational damage. If online services are regularly disrupted by cyber-attacks, this can lead to the erosion of public confidence in those services. Hacktivist groups have also successfully used distributed denial of service attacks to disrupt the websites of a number of councils (Distributed Denial of Service or DDoS attacks send overwhelming quantities of network traffic to the target with the intention of preventing access to the services it provides).
- **Insiders:** Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but often is due to simple human error or a lack of awareness about the particular risks involved.
- **Zero-day threat:** A zero-day exploit is a cyber-attack that occurs as soon as a weakness is discovered in software and before the supplier is either aware of it or can provide an update to mitigate it. It is an attack that exploits a previously unknown security vulnerability. This poses a risk to any computer or system that has not had the relevant update applied.
- **Physical threats:** The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other incident, natural or otherwise, that impact upon IT systems.

## 3.2 Vulnerabilities

Vulnerabilities are weaknesses or other conditions in an organisation that a threat actor; such as a hacker, nation state, disgruntled employee, or other attacker, can exploit to adversely affect system security. Cyber vulnerabilities typically include a subset of those weaknesses and focus on issues in the IT software, hardware, and systems an organisation uses.

## Types of vulnerability

- **Failure to System Maintenance:** Software vulnerabilities are constantly discovered by software suppliers and independent security professionals, and patches or updates are made available by the suppliers as quickly as possible to reduce the risk of a malicious actor exploiting them. The vulnerabilities are assessed and scored using an internationally recognised system to allow prioritisation according to severity of likelihood and impact. It is necessary to apply these patches and updates in a timely fashion to avoid the risk of malicious exploitation. Defence against exploitation employs the use of both automated tools and manual intervention to patch and update systems in a timely manner. If systems are not patched or updated in a timely fashion, then an attack on a system has a much better chance of success. It is also vital that system owners budget for future upgrades and set a timely schedule for the work to be undertaken,
- **Legacy Software:** Software that is in use but out of support, or unsupported, cannot be patched. Therefore, the likelihood of it being successfully compromised grows over time and cannot be addressed.
- **People:** 'Social engineering' seeks to trick people into allowing access to systems or handing over their credentials. Training and support are the main methods of dealing with this challenge, and these can be backed up with well thought out procedures and guidelines as well as good controls on user systems plus system monitoring for unusual events.

## 3.3 Risk Management

Cyber Risk Management is a fundamental part of broader risk management to ensure cyber security challenges are fully identified across the Council and appropriate action is carried out to mitigate the risk. The management of cyber security is, in large part, the management of risk, and falls within the Council's overall risk management policy. The Council has robust processes in place to manage risk at various levels within the organisation. To mitigate the multiple threats we face and safeguard our interests in cyberspace, we need a strategic approach that underpins our collective and individual actions in the digital domain.

This will include:

- A cyber security risk management framework to help build a risk aware culture within the Council.
- Cyber Awareness training to help mitigate insider threats, understand supply chain risks and ensure all staff understand the issues and their responsibilities.
- Applying ISO 27001:2002 controls and conforming to appropriate standards and frameworks to ensure that the Council will be able to identify, mitigate and protect against information security risks in a timely manner.
- Accrediting to the Public Sector Network (PSN) and any successor standards set by the Cabinet Office or Scottish Government.
- Undertaking an annual security health check using an independent specialist.
- Undertaking ad hoc security health checks for major system changes and externally hosted systems where necessary.

## 3.4 Cyber Security Strategic Targets

### Deter and Detect

The Council shall present a difficult target for all forms of attack and exploitation online. To achieve this will involve detecting, understanding, investigating and disrupting hostile action against us.

- Support enhanced governance through the application of government's cyber security guidance, e.g. 10 Steps to Cyber Security, NCSC cloud security guidelines, etc.
- Support network security through:
  - The use of multi-factor authentication, where technically possible.
  - Application of password protocols with high entropy. This means reliance on password length rather than complexity as per NCSC guidelines. Passwords which would on their own grant extensive system access, will have higher entropy levels.
- Raise defences through malware prevention.
- Review and enforce removable media/device controls.
- Maintain secure configuration.
- Deliver agreed plans and guidance.
- Training and educating users to help detect, deter and defend against the Cyber threats.

### Defend and Develop

The Council will continually develop its cyber security strategy to address the risks faced by the public sector. This includes developing a coordinated and tailored approach to risks and threats that we may encounter and mitigation of potential vulnerabilities.

- Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud.
- Ensure that major cyber security risks are present on the corporate risk register and hence managed by the Corporate Leadership Team.
- Implement processes, procedures and controls to manage changes in cyber threat level and vulnerabilities.
- Manage vulnerabilities that may allow an attacker to gain access to critical systems.
- Operate the Council's penetration testing programme and cyber-incident response.
- Develop training for staff and elected members.
- Develop an incident response and management plan, with clearly defined actions, roles and responsibilities.
- Develop a communication plan in the event of an incident which includes notifying (for example) the Corporate Leadership Team, the Communications Service, the National Cyber Security Centre (NCSC), Scottish Government Cyber Co-ordination Centre (SC3), Government Security Group (Cabinet Office), Police Scotland, and Information Commissioner's Office (ICO).



In continuing to provide assurance, the Council will:

- Maintain and continuously develop appropriate cyber security governance processes and a security framework with policies/procedures reviewed on a regular basis.
- Maintain, rehearse and regularly review an incident response and management plan, with clearly defined actions, roles and responsibilities. A copy of all incidents shall be recorded regardless of the need to report them.
- Set practice exercises on a regular basis; to ensure effective reaction to incidents when they occur.
- Maintain and regularly test and review business continuity plans for each service.
- Review vendor management – process of assessments of third parties.
- Explore Active Cyber Defence tools and new technologies to ensure the Council has best solutions to match with threats.
- Apply the government's cyber security guidance – 10 Steps to Cyber Security.
- Provide relevant cyber security training for staff and elected members.
- Comply with the applicable standards (PSN, PCI-DSS, etc).
- Protect enterprise technology by working with the Council's supply chain to develop model architecture and review audit logs to reduce chances of threats.
- Engage with external intelligence providers (Scottish Local Authority Information Security Group, Scottish Cyber Coordination Centre (SC3), Government Cyber Coordination Centre (GC3) OLECG and the OLECG cyber security subgroup, Cyber Scotland, North of Scotland Regional Resilience Partnership).

Effective cyber security governance in the Council is delivered through the following roles and functions:

## Chief Executive

The Chief Executive plays a critical role in cyber security. The Chief Executive is ultimately responsible for the Council's strategic direction, governance, and preparedness in managing cyber risks, including:

- **Providing strategic leadership** by ensuring cyber security is a strategic priority for the Council, and recognising its importance to service delivery and public trust,
- **Fostering a culture of security** by promoting a security-conscious culture across the organisation, and ensuring that as the Council adopts digital solutions, it balances innovation with robust security practices.
- **Supporting Incident Response and Resilience** by ensuring the Council has robust incident response plans that include clear roles and responsibilities for mitigating cyber-attacks and co-ordinating with external bodies, such as the National Cyber Security Centre (NCSC), local resilience forums, and law enforcement during incidents.

## Senior Information Risk Owner (SIRO)

The Council's nominated Senior Information Risk Owner (SIRO) is the Corporate Director for Neighbourhood Services and Infrastructure. The SIRO is responsible for the governance of cyber security and information risk within the Council. This includes ensuring that

information governance risk is managed in accordance with the General Data Protection Regulation (GDPR). However, whilst the SIRO is the nominated officer, responsibility for safeguarding information and information systems is shared across the organisation with all staff having a role to play.

## **Corporate Leadership Team**

Corporate Leadership Team (CLT) sponsor the Cyber Security Strategy and oversee the strategic framework through which the Council governs its information resources.

## **Corporate Director for Neighbourhood Service and Infrastructure**

The Corporate Director for Neighbourhood Services and Infrastructure has responsibility for the oversight of cyber security management through the Head of Property, Asset Management and Facilities, and provides a link into the promotion of cyber security at board level.

## **Head of Property, Asset Management and Facilities**

The Head of Property, Asset Management and Facilities has responsibility for the oversight of this plan and the IT implementation plan this feeds into as well as responsibility for oversight of cyber security generally.

## **Service Manager (IT)**

The Service Manager (IT) has responsibility for implementation of cybersecurity controls by the IT Support team.

## **Service Manager (Safety and Resilience)**

The Safety and Resilience team have responsibility for both the major incident plan and the overall business continuity process that would be necessary if an incident such as a cyberattack were to occur.

## **System owners**

System owners are responsible for ensuring that the procurement of new systems is overseen by a project board that includes the Information Security and Assurance Officer and the Information Governance Officer and that systems meet the required standards for cyber security and data protection standards, and the Digital Strategy.

System owners are also responsible for ensuring that upgrades are budgeted and undertaken in a timely fashion, that access is permitted for maintenance and patching, and that adequate provision is made for user acceptance testing when required.

## **System administrators**

System administrators are responsible for installing, supporting, and maintaining data and application servers, and other IT (Information Technology) infrastructure. The persons with this function will normally be nominated by the Service Manager (IT), or where the system is directly managed by a service, the Head of Service for that area. The system

administrator must not be the same person as the Data Controller for the data contained on the system.

System administrators are also responsible for:

- Ensuring that access privileges are granted at the appropriate level for staff requiring access to the system and revoking privileges in a timely manner when staff no longer need access.
- Ensuring that access is permitted for maintenance and patching.
- Developing and monitoring procedures for the system, satisfying the requirements of the relevant Data Controller, satisfying corporate security standards based on cyber security policies and procedures.

### **Data Protection Officer**

The Data Protection Officer is responsible for ensuring that data protection responses do not compromise the cyber security of the Council's data, IT infrastructure, or services.

### **Freedom of Information Officer**

The Freedom of Information Officer is responsible for ensuring that freedom of information responses do not compromise the cyber security of the Council's data, IT infrastructure, or services.

### **Information Governance Officer**

The Information Governance Officer is responsible for ensuring that, in conjunction with the Head of Property, Asset Management and Facilities and the Information Security and Assurance Officer, Information Governance policies support the principles of this strategy document.

### **Information Security and Assurance Officer**

The Information Security and Assurance Officer is responsible for developing and maintaining this strategy document to reflect changes in cyber security standards, and national public sector policies and frameworks.

The Information Security and Assurance Officer is also responsible for developing and maintaining Council and operational policies, cyber security standards and controls, reporting mechanisms and checklists, and risk management for cyber security.

It is the responsibility of all Staff to comply with the standards set out in this Information Technology and Cyber Security Strategy.

Currently the Council must comply with the following standards:

- Bankers' Automated Clearing Services (BACS).
- Payment Card Industry Data Security Standard (PCI DSS).
- Public Services Network (PSN).

In addition, the Council should follow all relevant National Cyber Security Centre (NCSC) guidance.

To ensure as robust a cyber security stance is taken IT will work with and assist our partners including Orkney Health and Social Care Partnership, Orkney Ferries Ltd, UHI Orkney and others.

## Section 4 – Governance

Good governance helps to ensure that investment in IT delivers benefits to the wider community as well as addressing corporate and service objectives. Our Strategy will take account of national and local initiatives and developments. We continue to work closely with colleagues in the NHS, UHI and the SG Digital Office as well as seeking opportunities to work with other Orkney based partners. These partnerships provide a firm platform for deriving benefits from joint working, shared systems, and procurement.

Good governance requires us to be open and accountable. Feedback from stakeholders tells us that we need to explain our services and the value of changes to the business.

### 4.1 Structures

- Asset Management Sub-committee considers reports from IT on a regular basis, including on delivery of this Strategy, the IT Capital Programme and the IT Asset Management Plan.
- The Corporate Leadership Team reviews IT performance, considers significant change requests, agrees the IT Capital Programme and ensure strategic fit working with the Council's Asset Management Strategy.
- IT will work closely with Internal and External Auditors to ensure good governance is acted upon.
- To ensure that any changes to key IT infrastructure and systems are correctly scrutinised IT will follow best IT Infrastructure (ITIL) practice with changes being discussed within a Change Advisory Board (CAB).
- IT will work with the Procurement team to ensure best practice is conducted with regard to infrastructure and systems procurement.
- IT will meet regularly with colleagues within the Improvement and Performance section to ensure the IT Strategy aligns with the Council's Digital Strategy.

## Section 5 – Infrastructure

The Council's IT assets, both physical and data, need constant maintenance and investment to ensure they remain fit for purpose and can fully support the Council's business objectives. These systems must be resilient, secure, available and enable improved public services whilst supporting innovation and change.

When ensuring resilience, consideration must also be given to responsible and careful arrangements around the supply and consumption of energy. Making use of such technologies as Cloud services, server virtualisation and remote collaboration and conferencing will assist in achieving a 'power light' collaborative green digital strategy.

One of the key themes of the recent digital transformation is the move "out" of the buildings and beyond the normal perimeters of the Council's local area network. Therefore, there is a challenge to be met in the continuing establishment of a Council network without walls that provides access to IT systems widely, flexibly, securely and responsively.

Continuing partnerships and collaboration with other councils has provided further opportunities to understand, enhance and improve our digital approach and overall network capabilities. Such partnerships as the Society of Council IT Managers (SOCITM), Scottish Wide Area Network (SWAN2) along with our own locally implemented improvements have provided an understanding that we can apply to expanding and linking our digital network to our users throughout our islands, premises, and schools.

### Strategic Targets

- We will continue our existing activities to 'harden' our local core infrastructure to provide an accessible, secure, and stable IT platform for existing and future systems requirements.
- Fully implement the next iteration of the Scottish Wide Area Network (SWAN2) while lowering costs.
- Ensure that our network fully enables access to electronic resources such as the Scottish Educational Digital Network (GLOW) and supports Council employees working in more flexible and mobile ways, including widening access to the Intranet.
- Continue to develop the use of Cloud technologies to enhance our IT offerings to customers and staff on an enhanced expanded local to cloud based network infrastructure.
- Continue to develop the use of cloud based remote working technologies.
- Work with staff and partners in meeting their expectations and needs through identifying what systems and equipment are required; improve efficiencies by identifying and removing redundant systems on our infrastructure.
- Ensure our IT Infrastructure represents 'value for money' and supports the Council's business objectives.
- Continue to improve our resilience and disaster recovery infrastructure.
- Ensure that our data holdings are secure, accurate and available to services to derive maximum value from the data we hold.

## Section 6 – Internal and External Customer Communications

Effective communications between our customers, partners and staff are an essential ingredient to provide high quality Council services. Balancing security and data protection obligations, while providing good ways to collaborate with partner organisations in the public sector and Orkney economy will be a theme for our enhancements in our digital offerings.

Documentation and access to documentation forms an essential part of effective technology based interactive services. It provides information to customers and staff required to deliver services. We will continue to support the ongoing development of Records Management solutions and governance standards being applied across the Council's data holdings both on-premise and in the Cloud, which will help us produce a robust documentation infrastructure, while meeting our green targets.

### Strategic Targets

- Continuously improve the Council's digital communications infrastructure and encourage its use, through providing facilities to support Council employees and customers to work and interact in a more flexible and mobile way, supporting sustainable communities.
- Introduce and promote digital document and record management to support effective, secure document creation and storage.
- Ensure easy access for staff and customers to information and meet our legislative data management requirements.
- Continuously improve our use of technology and work towards using systems that are used by others.
- Work proactively with partner organisations and other councils to achieve the best fit technologies for our customers – do not re-invent the wheel.
- Assist Customer Services to improve the way we work and communicate with our customers. Continuously review the way we collect staff and customer feedback through surveys and providing information on our activities and plans to our customers and staff.
- Continue to develop our Information Technology Infrastructure Library (ITIL) processes around IT support in incident management, service management, problem management, change management and asset management, including the creation of staff 'self-help'.



## Section 7 – Digital

Technology offers a tangible benefit to customers. IT therefore needs to embrace emerging technology and deliver a service that meets our customer expectations. This also means supporting our workforce to develop their own digital skills and implementing hardware that supports a more digital position.

Many staff work using a hybrid working arrangement. We will continue to not only support but enhance technologies to develop an ever-increasing mobile workforce in a secure and robust manner.

### Strategic Targets

- Support the introduction of new streamlined electronic processes and collaborative communications using available interactive technologies, such as Office 365, Electronic Document and Records Management System (EDRMS), Customer Service Platform and many other available IT solutions.
- Demonstrate leadership behaviour that supports and fuels a digital culture among staff and customers.
- Listen to and support staff on how to ‘get the best’, from these systems through providing pro-active knowledge bases.
- Advise on appropriate training using available browser based interactive platforms such as provided by partners, iLearn, IT Helpdesk and all other available resources.
- Enhance technologies to support modern working practices.
- Improve and develop our staff’s digital competency.
- Actively support areas of change in automated systems including Artificial Intelligence where appropriate.

Furthermore, our partnerships in the public sector, especially across Orkney, and our relationship with the technology economy across the isles, will be of importance. While we cannot merge infrastructure and systems across discrete organisations, we will seek to enhance our partnership and digital collaboration.

## Section 8 - Customer Focus

What we do as a Council touches the lives of most people in Orkney. Much of the time it won't be noticed, which is how it should be. Our services are provided in the background, efficiently and are there when they are needed. Our staff need IT to support them in delivering these services. At the same time our customers have an increasing expectation to be able to use technology to interact with our services at a time and in a way that suits them.

As a Council our customer base covers a wide variety of stakeholders. This includes Council staff in the various Council Offices, school staff and pupils, Marine Services, Airfields, and local Community Councils, as well as the wider Orkney community. Technology can be difficult to understand and use. IT will use their expertise to work with Services to introduce IT that has a stronger 'Customer Focus'. Any new system needs to meet the needs of our external and internal customers, with the design stage taking both into account as early as possible.

### Strategic Targets

- IT will use their expertise to work with Services to introduce IT that has a stronger 'Customer Focus'.
- Any new system requires to meet the needs of our external and internal customers, with the design stage taking both into account as early as possible.
- IT will use feedback from customers and staff to deliver continuous improvements to our business processes.
- We will review our Service Charter and introduce new targets as appropriate to support our changing business needs.
- We will encourage our stakeholders to work with us to discuss their issues and any planned IT developments.
- Where available and appropriate we will use technology and user workshops to train and inform staff on our service technologies.
- We will concentrate on developing and updating user guidance with the aim to make our staff more technically independent on the systems they use.

## Delivery of the Strategy

Each key aspect of this Strategy will be allocated to a lead officer within the IT Management Team and they will be responsible for preparing a Delivery Plan to demonstrate how each of the Strategic Targets will be delivered.

The Delivery Plan will set out the operational targets, resources required and performance indicators to demonstrate improvement.

Scrutiny of this Delivery Plan will be through regular reports to the Asset Management Sub-committee, usually biannually.

# Appendix 1 - IT and Cyber Security Strategy Delivery Plan 2025-2029

## Purpose

### 1.1.

This Delivery Plan provides information on delivering each of the objectives of the Information Technology (IT) Strategy.

## 2. Introduction

### 2.1.

The IT and Cyber Security Strategy Delivery Plan is a technical plan which underpins and supports the IT and Cyber Security Strategy and aims to improve and maintain the Council's IT infrastructure and systems.

### 2.2.

The table below set out the detail of how the IT and Cyber Security Strategy is being delivered. The IT and Cyber Security Strategy has a number of strategic targets, grouped into 6 themes. Objectives have been abstracted from the strategic targets in the strategy, and the table in sub-section of section 3 below, corresponds to a group of actions (one per row) contributing to that objective.

### 2.3.

Each action is owned by a specific member of staff, who is accountable for the correct and thorough completion of the task, and each is led by a specific member of staff who is responsible to the owner for the planning, execution and implementation of each necessary piece of work.

### 2.4.

For each action, progress will be reported, and an indication is given of the next steps planned. Where appropriate, an indication is given about where to find more information about the project or workstream.

### 3. Actions to Support IT Strategy Objectives

#### 3.1. Cyber Security Objectives

We will maintain a secure physical and virtual environment, with a high degree of resilience and confidence, based on national standards to present a difficult target for all forms of attack and exploitation online. To achieve this will involve detecting, understanding, investigating and disrupting hostile action against us.

**Objective 3.1.1:** We will implement suitable security controls to present a difficult target for all forms of attack and exploitation online.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.1.1.1. Public Services Network (PSN) accreditation.	Kenny MacPherson	Tony Whenman	Current accreditation until May 2025. Preparations for the next PSN accreditation due May 2025 have started. A full IT Health Check has been completed and a remediation plan has been drawn up.	Remediation Plan actions.
3.1.1.2. Build and Maintain IT Network defences following recognised (NCSC) security protocols.	Tony Whenman	Thomas Aldred	Network design is based on National Cyber Security Centre (NCSC) guidelines and security protocols. A review of network design to ensure it meets guidelines has found that some IT systems, while in a secure design do not meet current best practice.	Review systems by end 2025. Develop best practice designs 2025-2026. Establish financial cost implications 2025-2026. Migrate to best practice 2026-2029 where resources permit.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.1.1.3. Undertake an annual ITHC using an independent specialist	Kenny MacPherson /Tony Whenman	Thomas Aldred	A health check is conducted annually by an external accredited cyber security specialist. Any issues identified are programmed into an Action Plan that is worked through by IT and stakeholder services. Weekly internal checks are performed by the Information Security and Assurance Officer.	Review Health Check Report. Finalised Action Plan. Apply remediation steps as per plan by May 2025. Continuous review of internal checks.
3.1.1.4. Support Systems Security	Tony Whenman	System Owners	Systems security is supported using multi-factor authentication, where technically possible, and use of password protocols with high entropy. This means reliance on password length rather than complexity as per NCSC guidelines.	Work with System Owners to introduce Muli-factor authentication on an ongoing basis.
3.1.1.5. Train and educate users to defend against cyber threats	Tony Whenman	OD/ Communications /IT Support	Regular notification of new threats by bulletin email and SharePoint distribution. iLearn courses.	Continue to develop ways of enhancing user participation.

**Objective 3.1.2:** We will develop a coordinated and tailored approach to risks and threats that we may encounter and mitigation of potential vulnerabilities.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.1.2.1. Develop and maintain Cyber risk management framework.	Kenny MacPherson	Tony Whenman	Internal controls and governance for the prevention and detection of irregularities and fraud are in place.	Review and adjust controls, due end 2025.
3.1.2.2. Ensure that major cyber security risks are present on the corporate risk register.	Kenny MacPherson	Tony Whenman	Cyber security is currently recorded as a risk on the Corporate Risk Register.	Ensure the cyber security risk register is reviewed and updated regularly. Ongoing
3.1.2.3. Implement processes, procedures and controls to manage changes.	Kenny MacPherson	Tony Whenman /Thomas Aldred /System admins	Change Advisory Board (CAB) is in place.	Generate assurance that changes are presented to the CAB. Review 2025, with implementation 2026 onwards.
3.1.2.4. Review Process for Change management.	Kenny MacPherson	Tony Whenman /Thomas Aldred /System admins	It is important that all significant System changes are documented and agreed. It is known that some system administrators commit unrecorded changes.	Work with system owners to ensure changes are recorded and agreed before changes are made. Ongoing.



<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.1.2.5. Manage IT Infrastructure vulnerabilities that may allow an attacker to gain access to critical systems.	Tony Whenman	Thomas Aldred	Internal network is scanned on a weekly basis to capture the threat level and vulnerability position. Remediation is in place to correct vulnerability position.	Continue to enhance remediation actions and reporting. Ongoing
3.1.2.6. Manage third party system vulnerabilities that may allow an attacker to gain access to critical systems.	Tony Whenman	System Owners	Internal systems are scanned on a weekly basis to capture the threat level and vulnerability position. Remediation is only partly in place to correct vulnerability position as is reliance on supplying vendor to provide security updates.	Continue to work with System Owners, System Administrators and supplying vendors to enhance patching regime and to ensure only fully supported systems are procured. Ongoing
3.1.2.7. Operate a Council network penetration testing programme.	Tony Whenman	Thomas Aldred	Penetration testing is completed yearly on all systems. However, due to ever increasing criminal cyber incidents, penetration testing should be increased to match the threat.	Develop a more robust testing regime. Continuous review and improvement.
3.1.2.8. Upgrade all end user devices to latest operating system.	Thomas Aldred	Ray Groundwater	IT are working through an upgrade cycle of moving End-Of-Life (EOL) Windows operating systems. Approximately 50% of EOL devices have been upgraded.	Continue to upgrade with deadline of 14 October 2025 for EOL of Windows 10.

**Objective 3.1.3:** We will increase defences to mitigate cyber risks as far as possible.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.1.3.1. Develop a new web proxy system to ensure devices are always secured.	Tony Whenman	Thomas Aldred	Internal web proxy in place, but due for replacement June 2025. Remote working has brought a new threat where devices not on the Council network are not protected by a Web Proxy.	Purchase new Web Proxy which will also cover devices not on the Council network, this includes school devices. In progress replacement due summer 2025.
3.1.3.2. Purchase, set up and run a security information and event management (SIEM) solution.	Tony Whenman	Thomas Aldred	No SIEM in place – relying on SolarWinds reporting. SIEM is a standard component in cybersecurity which reviews logs across multiple systems automatically generating a clear overview for IT security management purposes.	Investigate most suitable SIEM solution and implement by end 2025. Likely to be delivered by 3.1.3.1

**Objective 3.1.4:** We will develop a culture of security by raising awareness of personnel to vulnerabilities, risks and threats from cyberspace and the need to protect information systems.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025.</b>	<b>Next Steps.</b>
3.1.4.1. Identify and implement measures to develop a culture of security.	Kenny MacPherson	Tony Whenman.	Information Governance Group owns and maintains standards. Use of regular all staff bulletins and email alerts to educate and inform. Information Security Officer developed content for mandatory online training courses for all staff, now delivered through iLearn.	Ongoing work to ensure high levels of security awareness remains.

Action.	Owner.	Lead.	Current position, January 2025.	Next Steps.
			Close co-operation between Information Security Officer and Information Governance Officer, within Information Governance Group and operationally.	

### 3.2. Governance Objectives

We will report on progress and make sure that decision makers have the information they need to make sound decisions.

**Objective 3.2.1:** Regular reporting to Council Asset Management Sub-committee on the delivery of Digital & IT Strategy, IT Asset Management Plan and IT Capital Programme.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.2.1.1. Establish regular Asset Management Sub-committee reporting.	Kenny MacPherson	Thomas Aldred	Reports to Asset Management Sub-committee are being submitted at least twice a year, either as stand-alone reports or included in broader financial reports.	Continue to submit reports.

**Objective 3.2.2:** The Corporate Leadership Team reviews IT Performance, considers significant change requests, agrees the IT Capital Programme and ensure strategic fit working with the Council's Asset Management Strategy.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.2.2.1. Significant changes are reported to Corporate	Kenny MacPherson	Thomas Aldred	Reports to CLT are submitted in the form of briefings.	Ensure significant changes are reported to CLT on an ongoing basis.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
Leadership Team (CLT).				
3.2.3.1. Ensure IT Capital Programme is strategically aligned to the Council's Asset Management Strategy.	Kenny MacPherson	Thomas Aldred/ Tony Whenman	IT Capital Replacement Programme is approved by Asset Management Sub-committee, following oversight by CLT.	Ensure reports are completed.

**Objective 3.2.3:** Establish and operate effective IT infrastructure and systems to support delivery of the outcomes in the Digital Strategy.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.2.3.1. Ensure full cooperation between IT and the Improvement and Performance team.	Kenny MacPherson	Thomas Aldred/ Tony Whenman	IT and the Improvement and Performance team meet on a monthly basis to review status and cooperation between the Council's IT Strategy and Digital Strategy.	Continue to enhance cooperation and systems to the benefit of the Council to ensure the IT and Cyber Security Strategy aligns with the Digital Strategy.

### 3.3. Infrastructure

We will invest in and maintain the Council's IT assets, both physical and data, to ensure they remain fit for purpose, and we will ensure they are resilient, secure and available, as well as improving services, while supporting innovation and change.

**Objective 3.3.1:** We will ensure that the IT asset base is available, resilient and effective.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.3.1.1. Embed processes for annual review of the IT asset base.	Kenny MacPherson	Thomas Aldred	The annual IT Capital Replacement Programme supports this objective by ensuring timely replacement of priority core infrastructure.  The IT Capital Replacement Programme for 2024/25 was approved by Asset Management Sub-committee in March 2024.	Deliver 2024/25 IT Capital Programme by 31 March 2025.
3.3.1.2. Upgrade of infrastructure.	Thomas Aldred	Ross Sutherland	The Council webserver infrastructure is not fit for purpose. There is little resilience in the current system and the network design no longer meets the NCSC's recommendations.	Implementation of new webserver infrastructure expected to be completed by September 2025.
3.3.1.3 Replace Analogue Phone systems and lines.	Thomas Aldred	Ray Groundwater	Due to the analogue switch off announced to occur in December 2025, IT has been migrating individual phone systems to the Council's Avaya phone system with resilience built in by adopting a local survivable BT line. At present, 22 Council establishments have been migrated with a further 53 to be completed. Of those 53 Council sites 12 at present cannot be migrated due to the absence of a BT digital line.	Continue to migrate phone systems/lines as they become available through BT.

**Objective 3.3.2:** We will ensure resilience is considered as part of project definition.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.3.2.1. When new systems are put in place resilience is considered.	Kenny MacPherson	Thomas Aldred	When new systems are being considered resilience of the system is taken as a key priority.	Consider resilience for main Internet feeds, which is dependent on the full implementation of SWAN II and webserver infrastructure.

**Objective 3.3.3.** We will seek to provide protection via good Disaster Recovery capability to support business continuity.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.3.3.1. Disaster recovery project.	Thomas Aldred	Pamela Money	A new data centre has been implemented at the Harbour Master's building at Scapa and is operational. This synchronises IT systems between Kirkwall and Scapa.	Continue to increase resilience via disaster recovery including investigation of additional Internet feed.
3.3.3.2. Immutable backups	Thomas Aldred	Ross Sutherland	Installation of an enhanced backup solution designed with measures to protect against ransomware cyberattacks is underway at both the main Council datacentre and the disaster recovery data centre at the Harbour Master's building at Scapa. This adds an additional layer of protection to systems and data if an attack was orchestrated against the Council.	Continue to ensure system is updated and appropriate for needs.

### 3.3.4.

Objective 3.3.4: We will support the innovation opportunities provided by developing a foundation for Business Intelligence and Data Warehousing to be explored and leveraged.

Work towards this objective will be done under Customer Focus Objective 3.3.

### 3.3.5.

Objective 3.3.5: We will continue to harden our local core infrastructure to provide an accessible, secure and stable IT platform for existing and future system requirements.

Work towards this objective will be done under Cyber Security Objectives 3.1 and Infrastructure and Systems Objective 3.5.

### 3.3.6.

Objective 3.3.6: We will ensure that our network fully enables access to electronic resources such as the Scottish Educational Digital Network (GLOW), which supports employees working in more flexible and mobile ways.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.3.6.1. Upgrade network capacity for access to cloud systems.	Thomas Aldred	Pamela Money	Network capacity has been upgraded to meet increased demands for access to cloud-based systems.	Implement SWAN2 which will increase bandwidth and improve network capacity. Ongoing as required.
3.3.6.2. Upgrade core networking infrastructure to ensure bandwidth capacity across network.	Thomas Aldred	Pamela Money	Core network infrastructure is currently within bandwidth requirements for Council services. However, a number of core infrastructure devices are nearing End-Of-Life (EOL) within the next 12 months.	Upgrade infrastructure before EOL. Ongoing as required.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.3.6.3. Make use of R100 infrastructure to enhance rural Wide Area Network (WAN) connections.	Kenny MacPherson	Thomas Aldred	Make use of the Scottish Government R100 infrastructure as and when it becomes available to enhance rural Wide Area Network (WAN) connections where suitable.	Continue to review and make use of connections as required.

**Objective 3.3.7:** We will develop co-operative connectivity with public sector and third sector bodies.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025.</b>	<b>Next Steps.</b>
3.3.7.1. Implement SWAN2 services.	Thomas Aldred	Vince Buchan	<p>The Scottish Wide Area Network (SWAN) used by many councils and public sector organisations delivers connectivity to the Council headquarters and other Council sites (mainly outside Kirkwall and Stromness).</p> <p>The national contract for SWAN has ended and the procurement process for a successor (SWAN2) has now completed, with transitions to new BT circuits to be completed by March 2026. At present Burray Primary School has been migrated with remaining sites to be completed by August 2025. BT infrastructure and resourcing are the limiting factor.</p>	Work with BT to migrate further sites.



Action.	Owner.	Lead.	Current position, January 2025.	Next Steps.
3.3.7.2. Implement joint systems with NHS Orkney.	Vince Buchan	Ray Groundwater	The Scottish Government Digital Office Microsoft 365 collaboration project has been set up to create a Digital Partnership between Orkney Islands Council and NHS Orkney to recognise the transformational potential of using M365 as a collaboration platform between the two organisations to provide concrete deliverables.	Waiting for Scottish Government Digital Office Phase 2 collaboration project.

**Objective 3.3.8:** We will introduce and promote the use of cloud technologies to enhance our IT offerings to customers and staff on an enhanced expanded local to cloud-based network infrastructure.

Future work towards this objective will be done as part of Governance Objective 3.2 and Objective 3.3.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.3.8.1. Develop appropriate cloud technologies.	Thomas Aldred	Ray Groundwater	Microsoft Azure Virtual Desktop in place as is MS Teams.	Continue to develop new technology as it becomes available.

**Objective 3.3.9:** We will work with staff and partners in meeting their expectations and needs through identifying what systems and equipment are required, and we will improve efficiencies by identifying and removing redundant systems on our infrastructure.

Work towards this objective will be done as part of Governance Objectives (technology standards) and Customer Focus Objectives (account management), as well as within projects under the Digital Strategy Delivery Plan.

**Objective 3.3.10:** We will ensure our IT infrastructure represents value for money and supports the Council's business objectives, including the objectives in the Digital Strategy.

Work towards this objective will be done as part of Governance Objective 3.2 above.

**Objective 3.3.11:** We will improve our publicising of our forward schedule of change to keep staff and customers informed.

<b>Action.</b>	<b>Owner.</b>	<b>Lead.</b>	<b>Current position, January 2025</b>	<b>Next Steps.</b>
3.3.11.1. Establish a process for keeping colleagues informed.	Thomas Aldred	Ray Groundwater	Alerts via email and SharePoint portal are in place.	Develop a robust process. This is a continuous process when new systems become available.
3.3.11.2. Implement a change management system for core corporate, and other sensitive and major systems.	Tony Whenman	System Owners	IT are working closely with stakeholders to ensure major/ sensitive systems are upgraded in a controlled manner using recognised change and project management methodologies. At present systems are upgraded without change management in place.	Cement robust processes with stakeholders. Review during 2025 and implement changes from 2026 onwards.

**Objective 3.3.12:** We will ensure that our data holdings are secure, accurate and available to services to derive maximum value from the data we hold.

Work towards this objective will be done as part of Customer Focus Objective 3.6 and above.

### **3.4. Internal and External Customer Communication**

We will communicate effectively with our customers, partners and staff, and where appropriate with citizens of Orkney and visitors; we will find way continuously to improve our services, especially when resources are limited to the benefit of the Orkney Community.

**Objective 3.4.1:** We will continuously improve the Council’s digital communications infrastructure and encourage its use, through providing facilities to support Council employees and customers to work and interact in a more flexible and mobile way, supporting sustainable communities.

Work towards this objective will be done as part of other objectives above, especially Governance Objective 3.2 and Customer Focus Objectives 3.6.

**Objective 3.4.2:** We will actively participate in national initiatives for sharing intelligence.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.4.2.1. Identify and implement measures to participate in national intelligence sharing initiatives.	Kenny MacPherson	Tony Whenman.	The Information Security Officer is a member of the UK-wide CiSP (Cyber-security Information Sharing Partnership), ensuring that the Council shares and receives intelligence on current cyber threats.  SciNET (Scottish Cyber Information Network) is a sub-group for Scotland of CiSp. The Scottish Local Authority Information Security Group is a sub-group of SciNET.	While action complete IT will continue to work with our partners and develop more as we develop our Cyber robustness.

**Objective 3.4.2:** We will introduce and promote digital document and record management to support secure document creation and storage.

Work towards this objective will be done as part of Digital Objective 3.5.

**Objective 3.4.3:** We will ensure easy access for staff and customers to information and meet our legislative data management requirements.

Work towards this objective will be done as part of Cyber Security Objectives and Customer Focus Objectives.

**Objective 3.4.4:** We will roll out enhanced desktop communications tools in keeping with our Microsoft 365 digital and governance strategies, as and when available, e.g., video, email, instant messaging, telecommunications, document and records management.

Work towards this objective will be done as part of Customer Focus Objective 3.6.

**Objective 3.4.5:** We will review our use of technology and work towards using systems that are used by others, where possible

Work towards this objective will be done as part of Governance Objective 3.2 above.

**Objective 3.4.6:** We will work proactively with partner organisations and other councils to achieve the best fit technologies for our customers, and so that we do not re-invent the wheel; this will include support for the 'Empowering Communities' programme.

Work towards this objective will be done as part of other objectives above, especially Governance Objective 3.2.

**Objective 3.4.7:** We will improve fault reporting, IT status information and staff communications through the IT Helpdesk, Customer Services announcements, and creation of staff self-help. Work towards this objective will be done as part of Customer Focus Objective 3.6.

### 3.5. Digital Objectives

We will embrace emerging technology and deliver a service that meets our customer expectations, also supporting our workforce to develop their own digital skills and implementing hardware that supports a more digital approach.

**Objective 3.5.1:** We will support the introduction of new streamlined electronic processes and collaborative communications through the use of available interactive technologies.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.5.1.1. Provide IT support to the Electronic Document and Records Management (EDRMS) project.	Vince Buchan	Ray Groundwater	Technical input to the EDRMS project continues to be provided.	Work to be completed as required in the EDRMS Project Plan.
3.5.1.2. Upgrade of systems.	Thomas Aldred	Ross Sutherland	Some systems procured and used by Services have been identified in the latest IT Health Check as requiring immediate upgrade.	IT will work with System Owners to identify new replacement systems that meet NCSC security guidelines. Once replacement systems have been identified by System Owners on an ongoing basis.

**Objective 3.5.2:** We will demonstrate leadership behaviour that supports and fuels a digital culture among staff and customers.

Work towards this objective is being done as part of the Digital Strategy Delivery Plan objectives, under the theme of Digital.

**Objective 3.5.3:** We will listen to and support staff on how to get the best from digital systems.

Work towards this objective is being done as part of Customer Focus Objectives, at Objective 3.6, and within implementation projects described elsewhere in this plan, and in the Digital Strategy Delivery Plan.

**Objective 3.5.4:** We will improve and develop our staff’s digital competency.

Work towards this objective is being done as part of the Digital Strategy Delivery Plan objectives, under the theme of Digital.

**Objective 3.5.5:** We will continue to identify Account Managers for digital technologies, to encourage our stakeholders to work with these Account Managers to discuss their issues and any planned IT developments; we will ensure that account managers are visible, knowledgeable, proactive in communicating with stakeholders, and effective in receiving and acting on feedback.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.5.5.1. Identify IT technology specialism teams.	Thomas Aldred	Ray Groundwater	IT specialism team leader roles are clearly visible within IT however work to defined specialisms within other departments is ongoing to enable proactive communication with stakeholders enabling effective action being taken on feedback received.	Create a stronger working relationship with System Owner specialists. On an ongoing basis.

**Objective 3.5.6:** We will use technology (where available and appropriate) and user workshops to train and inform staff on our service technologies.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.5.6.1. Creation of video files within MS Teams for training purposes	Thomas Aldred	Ray Groundwater	Work is underway to trial the recording of Teams sessions as a resource to be used in specific application areas.	Will continue to develop further training videos as required.

**Objective 3.5.7:** We will concentrate on developing and updating user guidance with the aim to make our staff more technically skilled and independent with the systems they use.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.5.7.1. Develop and update user guidance.	Thomas Aldred	Ray Groundwater	Guidance is issued to staff as and when needed, generally when a project moves into the delivery phase.	SharePoint site to house all guidance in a user-friendly way. This is a moving and ongoing project.

### 3.6. Customer Focus Objectives

We will use our experience to work with all Council services to introduce IT systems with a stronger citizen/customer focus: any new system will meet the needs of users within the Council, and also those outside the Council who use it in any way; system design will take the needs of all these users into account at as early a stage as possible.

**Objective 3.6.1:** We will continue to implement collaborative technologies.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.6.1.1. Enhance the use of Microsoft technologies.	Thomas Aldred	Ray Groundwater	IT has continued to develop further the adoption and use of Microsoft 365. However, a roadmap should be defined to ensure the Council is making best use of its investment in Microsoft technologies. This along with Artificial Intelligence (AI) should include licensing options, partnership access, Schools, and field workers.	Create a Microsoft roadmap and include new Microsoft releases as they become available.
3.6.1.3. Enhance technology use between corporate	Tony Whenman /Paul Kesterton	Schools	Many school staff now have access to corporate email and Microsoft teams. There is however a need to increase its use to ensure sensitive data is not held in GLOW systems.	Continue to develop, support and promote use of M365 in schools.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
and School staff				

**Objective 3.6.2:** We will review our Service Charter and introduce new targets as appropriate to support our changing business needs.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.6.2.1. Review IT Service Charter.	Kenny MacPherson	Thomas Aldred	The IT Service Charter was last reviewed in June 2019. Individual Service Charter highlighting Service Level Agreement for the Orkney and Shetland Valuation Joint Board has been developed and shared.	Review IT Service Charter during 2025.

**Objective 3.6.3:** We will work to improve internal fault reporting and service delivery through the use of various software tools to ensure that important information is communicated effectively and clearly.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.6.3.1. Power BI for clear reporting.	Thomas Aldred	Ray Groundwater	Microsoft Power BI software enables reporting business intelligence (BI) data to be visualised. Reporting utilisation needs enhancement.	Enhance processes on an ongoing basis.
3.6.3.2. We will encourage our stakeholders to work with us to discuss their issues	Kenny MacPherson	Thomas Aldred	IT meet with key stakeholders find way for recording portfolio.	Enhance meeting schedules on an ongoing basis.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
and any planned IT development.				

**Objective 3.6.4:** We will use opportunities within the IT team to train staff to cover across more than one system, thus moving away from the risk inherent in specialised, singleton posts.

Action.	Owner.	Lead.	Current position, January 2025	Next Steps.
3.6.4.1. Ensure more than one member of IT staff is trained and allocated to provide support for each supported system.	Thomas Aldred	Ray Groundwater	Work is underway to ensure that sufficient staff have the skills and experience to cover the support of all main systems and infrastructure. Training courses, including by external providers, have been delivered to IT staff, with more planned.	Continue to review training needs for IT staff. Also include system owners.





## Equality Impact Assessment

The purpose of an Equality Impact Assessment (EqIA) is to improve the work of Orkney Islands Council by making sure it promotes equality and does not discriminate. This assessment records the likely impact of any changes to a function, policy or plan by anticipating the consequences, and making sure that any negative impacts are eliminated or minimised and positive impacts are maximised.

<b>1. Identification of Function, Policy or Plan</b>	
Name of function / policy / plan to be assessed.	IT & Cyber Security Strategy 2025 - 2029
Service / service area responsible.	Neighbourhood Services and Infrastructure
Name of person carrying out the assessment and contact details.	Thomas Aldred <a href="mailto:Thomas.aldred@orkney.gov.uk">Thomas.aldred@orkney.gov.uk</a> ext. 2152
Date of assessment.	16/01/2025
Is the function / policy / plan new or existing? (Please indicate also if the service is to be deleted, reduced or changed significantly).	This is a new strategy, but built on the previous one.

<b>2. Initial Screening</b>	
What are the intended outcomes of the function / policy / plan?	A five-year IT strategy for the Council to ensure systems are delivered and security is maintained
Is the function / policy / plan strategically important?	Yes
State who is, or may be affected by this function / policy / plan, and how.	Users of Internal Council systems.
How have stakeholders been involved in the development of this function / policy / plan?	Stakeholders have been interviewed, CLT and Asset Management Sub-committee will scrutinise.
Is there any existing data and /	No

<p>or research relating to equalities issues in this policy area? Please summarise.</p> <p>E.g. consultations, national surveys, performance data, complaints, service user feedback, academic / consultants' reports, benchmarking (see equalities resources on OIC information portal).</p>	
<p>Is there any existing evidence relating to socio-economic disadvantage and inequalities of outcome in this policy area? Please summarise.</p> <p>E.g. For people living in poverty or for people of low income. See <a href="#">The Fairer Scotland Duty Guidance for Public Bodies</a> for further information.</p>	<p>(Please complete this section for proposals relating to strategic decisions).</p> <p>No Not Applicable</p>
<p>Could the function / policy have a differential impact on any of the following equality areas?</p>	<p>(Please provide any evidence – positive impacts / benefits, negative impacts and reasons).</p>
<p>1. Race: this includes ethnic or national groups, colour and nationality.</p>	No
<p>2. Sex: a man or a woman.</p>	No
<p>3. Sexual Orientation: whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes.</p>	No
<p>4. Gender Reassignment: the process of transitioning from one gender to another.</p>	No
<p>5. Pregnancy and maternity.</p>	No
<p>6. Age: people of different ages.</p>	No
<p>7. Religion or beliefs or none (atheists).</p>	No
<p>8. Caring responsibilities.</p>	No
<p>9. Care experienced.</p>	No
<p>10. Marriage and Civil Partnerships.</p>	No

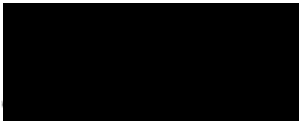
11. Disability: people with disabilities (whether registered or not).	(Includes physical impairment, sensory impairment, cognitive impairment, mental health) No
12. Socio-economic disadvantage.	No

### 3. Impact Assessment

Does the analysis above identify any differential impacts which need to be addressed?	No
How could you minimise or remove any potential negative impacts?	N/A
Do you have enough information to make a judgement? If no, what information do you require?	Yes

### 4. Conclusions and Planned Action

Is further work required?	No.
What action is to be taken?	N/A
Who will undertake it?	N/A
When will it be done?	N/A
How will it be monitored? (e.g. through service plans).	N/A

Signature: 

Date: 16/01/2025

Name: THOMAS ALDRED

(BLOCK CAPITALS).

Please sign and date this form, keep one copy and send a copy to HR and Performance. A Word version should also be emailed to HR and Performance at [hrsupport@orkney.gov.uk](mailto:hrsupport@orkney.gov.uk)