Meeting of:	**GOVERNANCE AND AUDIT COMMITTEE**
Date of Meeting:	**18 APRIL 2024**
Report Title:	**ICT DEPARTMENT PROCESSES AND PROCEDURES**
Report Owner / Corporate Director:	**CHIEF OFFICER - FINANCE, HOUSING & CHANGE**
Responsible Officer:	**MARTIN MORGANS** **HEAD OF PARTNERSHIPS AND HOUSING**
Policy Framework and Procedure Rules:	**There is no effect upon the Policy Framework and Procedure Rules**
Executive Summary:	Outlining how the ICT processes and procedures are maintained to ensure an efficient operating model that minimises disruptions. Highlighting the key aims of protecting the networks, data and services that the Council delivers. This covers all aspects inclusive of cyber security, from the secure design of systems and services through to access management and the handling of incidents.

1. Purpose of Report

1.1 The purpose of the report is to inform Governance and Audit Committee of how ICT Department's processes and procedures are maintained to ensure an efficient operating model that minimises disruption to the Council. The report highlights the key aims of protecting the networks, data, and services that the Council delivers. This covers all aspects of cyber security, from the secure design of systems and services through to access management and the handling of incidents.

2. Background

2.1 The Council is very dependent on Information and Communication Technology (ICT) with regard to its day-to-day operations and has an excellent record of ICT reliability. Council dependency on ICT has increased with the introduction of hybrid working, as staff and members access systems remotely and many meetings now take place on a hybrid basis with attendees joining the meeting either in person or remotely.

2.2 The current ICT disaster recovery infrastructure is co-located within a neighbouring Local Authority. All Council ICT systems data is directly replicated to this

infrastructure in real time, so an exact copy of the Council's data is always available at this remote site. All data is also backed up to a secure offsite location overnight. The ICT Business Continuity Plan lists the key systems that will be made available in priority order within 8 hours following the invocation of the ICT Business Continuity Plan. Non key systems would be made available within 5 working days.

2.3 Instances of major ICT outages affecting the core network are very low in Bridgend Council with only three having been experienced in recent years as summarised below, none of which involved any cyber related activity:

- 2013 Core network hardware failure, 4 hours downtime.
- 2020 External civil contractor cut fibre cable, 8 hours downtime.
- 2023 Infrastructure hardware failure, 12 hours downtime.

3. Current situation

3.1 The Council subscribes to the National Cyber Security Centre (NCSC) "Early Warning" system, which is a free service designed to inform organisations of potential cyber-attacks on their network, as soon as possible. The Early Warning system uses a variety of information feeds from the NCSC, trusted public, commercial and closed sources, which includes several privileged feeds which are not available elsewhere.

3.1.1 "Early Warning" filters millions of events that the NCSC receives every day and, using the Internet Protocol (IP) and domain names provided by an organisation, correlates those which are relevant to that organisation, so that the Council receives relevant daily notifications to the Council's nominated contacts via the Early Warning portal.

The following outlines the high-level types of alerts available via "Early Warning":

- **Incident Notifications** – This is activity that could suggests an active compromise of the Council's system e.g., Malware.
- **Network Abuse Events** – This may be an indicator that the Council's assets such as computer hardware have been associated with malicious or undesirable activity.
- **Vulnerability and Open Port Alerts** – These are indications of vulnerable services running on the Council's network, or potentially undesired applications being exposed to the internet.

3.2 The Council's Firewalls are the perimeter defence which block on average 2500 external attacks every day. The email security gateway blocks on average 450 phishing emails per day. Phishing is currently regarded as the highest risk of a successful cyber-attack, which could lead to a ransomware infection. The Intrusion Prevention System (IPS) is a security feature integrated into the Council's firewalls to provide advanced threat protection capabilities. IPS works alongside traditional firewall functionalities to actively monitor and protect the network from various cyber

threats, including intrusions, malware, and exploits. Steps 1 – 7 below outline how the Firewall IPS typically functions:

1. Detection
2. Signature-Based Detection
3. Anomaly-Based Detection
4. Prevention and Mitigation
5. Integration with Threat Intelligence
6. Tuning and Customization
7. Reporting and Analysis

3.3 PSN Code of Connection Certification

3.3.1 The PSN (Public Services Network) is a network operated by several suppliers for the government that provides a trusted, reliable, cost-effective solution to departments, agencies, local authorities, and other bodies that work in the public sector, which need to share information between themselves. The Code of Connection (CoCo) provides a minimum set of security standards that organisations must adhere to when joining the Public Services Network. Certification shows that organisations have successfully achieved PSN compliance by demonstrating that their infrastructure is sufficiently secure and would not present an unacceptable risk to the security of the network. Organisations must submit the following material as part of the certification process on an annual basis:

- As a local authority, the chief executive must sign the CoCo.
- Provision of an up-to-date network diagram.
- The Remediation Action Plan (RAP) from their most recent PSN compliance assessment, if applicable, and evidence that the remedial work was carried out as planned.
- A recent (within the last 12 months) IT Health Check (ITHC) report, plus a new RAP to address any issues found.

3.3.2 The Cyber Security Audit**,** carried out by the Regional Internal Audit Service recommended the need to review the opportunity for structured reporting to CMB. The PSN application will be formally submitted on annual basis to CMB, which will form the initial point in time position. ICT will explore increasing the frequency utilising available tools and metrics working towards a quarterly position.

3.4 Change Process – Information Technology Infrastructure Library (ITIL) Change Management

3.4.1 ICT have implemented a robust Change Management process based on the ITIL, which is a set of detailed practices for IT Service Management (ITSM). The main aim of change management is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes to minimise the impact of change related problems upon the service quality of the organisation.

To ensure the efficient supply of IT services, it is essential that changes are managed and controlled systematically, thus minimising any undue disruption to services delivered to the customer. This management and control encompass the way changes are initiated, assessed, planned, scheduled, and implemented.

3.5 Patch management – Servers, Desktops & Laptops

3.5.1 Effective patch management is paramount for mitigating security risks, ensuring system reliability, and maintaining compliance with regulatory requirements. Through the utilisation of a number of tools, the Council has established an effective patch management framework in-line with the Change Management process outlined in 3.4 above. This facilitates the timely and efficient deployment of updates across the server and client environments. Through the conduct of diligent testing and proactive monitoring, ICT aim to uphold the integrity and security of the Council's IT infrastructure while minimising disruptions to business operations.

3.5.2 The Council is a Windows ecosystem. Therefore, there is tight integration with the Microsoft Patch Deployment Schedule. The stages leading to patch deployments are outlined below:

- Microsoft Patch Tuesday: Updates released by Microsoft on the second Tuesday of each month are promptly evaluated and prepared for deployment.
- Testing Phase: Before widespread deployment, patches undergo testing within a designated test group to assess compatibility and ensure no disruptions occur. This testing phase typically spans one week.
- Widespread Deployment: Following successful testing, patches are rolled out to the entire estate with a two-week deadline for installation. This timeline provides ample opportunity for endpoints to receive and apply the necessary updates.
- Monitoring and Compliance: Post-deployment, patching activities are closely monitored to verify successful installation and compliance with patching policies. Any discrepancies or failures are promptly addressed to maintain a secure and resilient IT infrastructure.

3.6 Data Centre

3.6.1 The data centre is a building, or dedicated space within a building, which is used to house computer systems and associated components, such as telecommunications and storage systems for the Council. Due to the age of the current data centre infrastructure, £1,260,000 was included in the Capital Programme for 2023-24 to procure and implement the data centre refresh project. ICT completed a procurement exercise in June 2023. The new data centre infrastructure is due to go live at the end of April 2024. The new infrastructure chosen is inherently more robust and includes fewer single points of failure than our current infrastructure.

3.6.2 Welsh Government has requested that local government organisations look at a 'Cloud First' strategy for ICT provision. "On premise" refers to a set of services delivered from an infrastructure that is installed into a physical datacentre local to

the organisation. The two options that were available to the Council are outlined below; the Council selected the “Private Cloud” option as the preferred choice:

- “Public Cloud” refers to a set of services delivered from infrastructure that is remote to the Council, is implemented on a scaled-up basis, is publicly available, and shared across many customers - yet still secure, accredited, and managed by Council. In this model the funding mechanism is a revenue charge in relation to the actual usage and requires less capital investment.

- “Private cloud” refers to a set of services that are delivered from infrastructure dedicated to the customer only, but from a location remote to the Council, such as a managed data centre. In this model the infrastructure is typically funded through capital replacement plans and the purchased infrastructure is in place for five to seven years and then needs replacing. The primary benefit of this option is the removal of the requirement of the Council to build and maintain a local data centre.

3.6.3 The benefits of partnering and working with a managed data centre provider within the context of a “private cloud” offer advantages in terms of security and resilience which is outlined below:

3.6.4 Power

The data center site provides N+N topology for redundancy which means there is a duplicate component for every component i.e., the data center maintains two of everything. A unique dedicated 400kV substation on-site connects, directly and privately, to the U.K. Super Grid. All power into the site is 100% renewable energy and available at highly competitive rates.

- Most powerful data center site in Europe
- Direct, private 400kV Super Grid connection, supported by regularly tested, highly resilient generators and Uninterrupted Power Supply (UPS) systems
- All systems concurrently maintainable
- 100% renewable energy
-

3.6.5 Security

Stringent security and safety measures are hallmarks of the site, ensuring the security of digital assets. Sited in a low crime rate area, the data center site is set back from the perimeter, which has military-grade fencing, digital tripwires and multiple CCTV towers with diverse power and connectivity feeds. Ten-ton, anti-ram raid blocks are installed between paved areas and entries for added protection. Traffic management systems are in place at the entrance and the exit, supported by double airlock gates. Layered access is controlled using zoned card swipe and CCTV monitoring throughout and can be supplemented with custom fitments for multi-factor authentication, secure trunking, airlocks, and additional surveillance.

- On-site security operations centre with patrols 24x7x365
- Meets or exceeds the standards required by global enterprises
- Meets the U.K. government/military security specifications

3.6.6 Connectivity

Rich in connectivity, the data center has fiber delivered by many Tier 1 service providers and offers low latency between Wales and London of less than 1.5 milliseconds. The site offers Cloud Gateway, which facilitates direct access into leading public cloud providers such as Microsoft ExpressRoute. In addition, the site is a new hosting facility for LINX Wales, which provides peering services and public policy representation to network operators. In summary, the data centre offers:

- Carrier-neutral site
- 10GE, nx10GE, 40GE and 100GE point-to-point connectivity
- Low latency: Less than 1.5 milliseconds, Wales to London providing instantaneous data exchange
- Pre-installed links to virtual meet-me-rooms in London
- Direct access into leading public cloud providers
- Independent fiber route available
- 12+ international carriers

3.7 Chief Information Security Officer (CISO)

3.7.1 The Cyber Security Audit**,** carried out by the Regional Internal Audit Service recommended, that the Council introduces a Chief Information Security Officer (CISO), or equivalent, reporting directly to Corporate Management Board. The competitiveness of the market for a candidate with this skill set, is not achievable within the pay scales of the Council. Therefore, in the absence of a CISO the risks are being mitigated by distributing the functions across key members of staff within ICT, including the Group Manager ICT, Data and Network Services Manager, and Network Analyst.

3.8 Enhanced E-Learning

3.8.1 The Cyber Security Audit**,** carried out by the Regional Internal Audit Service recommended that current e-learning needed to be enhanced to include cyber security. Training is to be refreshed from time-to-time so that officers Council wide can continue to maintain their knowledge and understanding of cyber-attack methods and how to spot them. ICT are currently carrying out an exercise to assess the market and enable a decision with regards procurement.

4. Equality implications (including Socio-economic Duty and Welsh Language)

4.1 The protected characteristics identified within the Equality Act, Socio-economic Duty and the impact on the use of the Welsh Language have been considered in the preparation of this report. As a public body in Wales the Council must consider the impact of strategic decisions, such as the development or the review of policies, strategies, services and functions. This is an information report, therefore it is not necessary to carry out an Equality Impact assessment in the production of this report. It is considered that there will be no significant or unacceptable equality impacts because of this report.

5. Well-being of Future Generations implications and connection to Corporate Well-being Objectives

5.1 A prosperous Wales - Improving ICT infrastructure and enablement to support Councils drive for a prosperous Wales.

A resilient Wales – Supporting the changes to working practices providing flexibility to Council officers.

A healthier Wales – Timely access to information to ensure support can be provided promptly preventing further deterioration, supported by real time information.

A more equal Wales – Flexible services, responsive to the needs of the most vulnerable.

A globally responsive Wales – Digital services reduces the need for journeys and resources such as fuel and paper, reducing Co2 emissions and use of resources.

6. Climate Change Implications

6.1 The consolidation of compute, storage, and networking has reduced the physical data centre space requirement. It has also lowered energy consumption, helping the Council with reducing power needs and tackling climate change.

7. Safeguarding and Corporate Parent Implications

7.1 There are no safeguarding and corporate parent implications arising from this report.

8. Financial Implications

8.1 £1,260,000 was included in the Capital Programme for 2023-24 to procure and implement the data centre refresh project, which is anticipated to be fully spent.

9. Recommendation(s)

9.1 Committee to note the report.

Background documents
None