WEST DUNBARTONSHIRE COUNCIL

Report by Chief Officer – People & Technology

Corporate Services Committee: 19 May 2021

Subject: Universal Serial Bus **(**USB) Data Drive Policy

1. Purpose

1.1 The purpose of this report is to secure approval of the new USB Data Drive Policy. This policy will form part of the existing Information Security Policy framework which was approved by this Committee on 25th August 2019.

2. Recommendations

2.1 The Committee is asked to:

2.1.1 Note that there have been several recent high profile cyber incidents with the most common means of attack being email and the direct introduction of malware via USB storage;

2.1.2 Note that the USB Data Drive Policy will become the seventh element of the Information & Communication Technology (ICT) Information Security Policy framework as follows:

- West Dunbartonshire Council Information Security Policy;
- West Dunbartonshire Council Acceptable Use Policy (AUP);
- Acquisition and Disposal of ICT;
- Privacy and Monitoring;
- Information Security - DPA forum charter;
- Reporting of Information Security concerns; and
- USB Data Drive Policy.

2.1.3 Note that the Data Breach procedures document is also referenced in the USB data drive policy; and

2.1.4 Approve the Council USB Data Drive Policy as an addition to the Information Security Policy framework.

3. Background

3.1 The existing Council Information Security Policy Framework - Acceptable Use Policy already makes reference to the use/misuse of USB drives.

3.2 The requirement to include a more detailed USB data drive component was captured as part of an Internal Cyber Security Audit and is included in action IAAP/082 2-Use of removable media devices.

3.3 The USB Data Drive Policy marks the start of a process to gradually phase out the use of USB drives in order to reduce the Council's Cyber threat footprint.

3.4 There are alternatives to using USB data drives and employees will be directed to these where appropriate, such as:

- Access files and resources via thin client technology;
- Access files and resources via the Council Ourcloud platform;
- Ask suppliers to email course and seminar presentations rather than issue on USB drives;
- Email documents/files via the council secure email facility which is automatically virus checked; and
- Explore potential to use the Microsoft 365 platform to securely share files in the cloud.

4. Main Issues

4.1 Due to the increased threat landscape and sophistication of techniques used by threat actors, the Council must take steps to mitigate risks as much as possible. The policy will make it easier for everyone affected to understand and carry out their roles in relation to the proper governance and use of the Council's ICT Resources.

4.2 The gradual move away from USB data drives will affect some service areas more than others. the Council's ICT team will endeavour to support use of alternatives before the removal of USB completely such as agreeing exceptions; investigating technologies to permit/restrict usage based on USB category. At this time there is no defined date for removal as ICT are currently assessing how widespread the use of USB drives is and the time required to identify alternate solutions.

4.3 The USB Data Drive Policy will initially be reviewed at least annually in line with technological changes and as business requirements become clearer. It is expected that the review period would then change to reflect the declining use of USB drives.

4.4 This Policy will be supported by existing corporate procedures and guidance which will set out how employees, elected members, 3rd party suppliers / consultants / trainers and other relevant groups are expected to carry out their roles in relation to the use of technology.

4.5 The Information Security Policy Framework was communicated to employees via Email, Intranet, awareness sessions, and via a mandatory online

Information Security I-Learn course and this addition to the framework will be communicated in the same way.

4.6 The Policy (USB Data Drive Policy) and Framework is and will continue to be promoted and available via the Council's intranet.

4.7 The policy allows for an amnesty on all existing USB drives which can be passed to ICT for safe recovery of data where required and/or disposal of both the data and USB drives.

5. People Implications

5.1 The addition of the USB Data Drive Policy to the Information Security Policy Framework forms part of the Council's mitigation against the risk that our employees, elected members and other bodies (partners, suppliers etc.) may encounter when using council ICT resources.

5.2 This policy provides the information needed for employees, elected members and other groups to understand their obligations in the proper use and governance of council and citizen information and data.

6. Financial and Procurement Implications

6.1 There are no direct financial or procurement implications associated with this report or policy. There may be a cost associated with providing suitable alternative solutions.

7. Risk Analysis

7.1 Without an up to date Information Security Policy Framework including specific guidance on the use of USB data drives to mitigate against emerging threats and new technologies, there is an increased likelihood of reputational and financial risks for example financial penalties due to data breaches, and/or the potential for disruption caused by ransomware attack.

7.2 This policy is part of a suite of controls introduced to address Strategic risks SR004 (Information Technology) and SR008 (Threat of Cyber attack) included in the Council strategic risk register.

8. Equalities Impact Assessment (EIA)

8.1 An equalities impact assessment was carried out and there are no adverse equalities issues identified.

9. Environmental Sustainability

9.1 Not applicable.

10. Consultation

10.1 Legal, CPU, Education and the Section 95 Officer have been consulted on the content of this paper. The Trades Union have been consulted and comments received.

11. Strategic Assessment

11.1 High quality ICT resources and services contribute to the Council's strategic priority of delivering fit for purpose (secure) estate and facilities.

Name: Victoria Rogers
Designation: Chief Officer - People and Technology
Date: 30 April 2021

Person to Contact: Brian Miller, ICT Section Head Infrastructure
07876397925
brian.miller@west-dunbarton.gov.uk

Appendix: USB Data Drive Policy

Background papers: Information Security Policy framework

Wards Affected: All