Decision Report - Executive Decision
Forward Plan Reference: n/a non key
Decision Date – 19/4/2023
Non Key Decision

Somerset Council IT Policies from April 2023

Executive Member(s): Cllr Mike Rigby - Lead Member for Transport and Digital
Local Member(s) and Division:
Lead Officer: Dave Littlewood, Strategic Manager Enterprise Architecture & Governance
Author: Rob Rooks, Service Manager-Enterprise Architecture General
Contact Details: rob.rooks@somerset.gov.uk

Summary / Background

1. Updated and amended set of Information Security policies for Somerset Council to apply to members, officers and contracted third parties.

2. Standard templates (ISO27001) have been used as a start point and are representative of existing policies used separately by SCC and the four districts. SME representatives from the five councils updated and reviewed the templates into working policies. They have since been reviewed by LGR HR and Union representatives and approved by JNF.

Recommendations

3. The Executive member agrees the adoption of these updated and unified policies by Somerset Council.

Approval relates specifically to the policies that apply to all users of Somerset Councils systems and/or data – *See Appendix A*:

- ICT 02 Access Control Policy
- ICT 02A Password Policy
- ICT 03 Asset Management Policy
- ICT 07 Acceptable Use Policy
- ICT 08 Clean Desk and Clear Screen Policy
- ICT 09 Mobile Device Policy
- ICT 18 Information Transfer Policy

The rest of the policy set supports these policies and/or are targeted at ICT as follows:

- ICT 01 Information Security Policy (Overview)
- ICT 04 Risk Management Policy
- ICT 05 Information Classification and Handling Policy

- ICT 06 Information Security Awareness and Training Policy
- ICT 10 Business Continuity Policy
- ICT 11 Backup Policy
- ICT 12 Malware and Antivirus Policy
- ICT 13 Change Management Policy
- ICT 14 Acceptable Usage Policy (Supplier specific)
- ICT 14A Memorandum of Understanding (Supplier specific)
- ICT 15 Continual Improvement Policy
- ICT 16 Logging and Monitoring Policy
- ICT 17 Network Security Management Policy
- ICT 19 Secure Development Policy
- ICT 20 Physical and Environmental Security Policy
- ICT 22 Cryptographic Control and Encryption Policy
- ICT 23 Document and Record Policy
- ICT 24 Significant Incident Policy and Collection of Evidence
- ICT 25 Patch Management Policy

Reasons for recommendations

4. These policies are what we will do to ensure acceptable use of Somerset Council services, data and assets, principally related to ICT and Information Security. They will be used and referred to in parallel to HR policies and Information Governance policies (i.e. GDPR).

5. There is no exempt information.

6. Urgency provisions are not being sought.

Other options considered

7. Policies based on ISO27001 or equivalent are the accepted approach and therefore no other options have been considered.

Links to Council Vision, Business Plan and Medium-Term Financial Strategy

8. The adoption of policies has no links to the County Vision, Business Plan or Medium-Term Financial Plan.

9. Approval of updated policies for the whole of Somerset Council guides appropriate and secure use of council systems and data to the benefit of all.

Financial and Risk Implications

10. There are no financial implications foreseen.

11. There are no risk implications foreseen

Legal Implications

12. There are no legal implications

HR Implications

13. The policies non-compliance may be used by ICT and HR to apply remediation up to and including termination of employment or third party contracts. This is a standard approach and HR and Union representatives have reviewed and contributed to the policies and the Equalities Impact Assessment being presented for approval.

Other Implications:

Equalities Implications

14. Whilst these policies themselves present no disproportionate impacts from an equality implication their implementation may. This will be addressed through a proportionate and understanding response to particular need by managers.

Community Safety Implications

15. No implications

Climate Change and Sustainability Implications

16. No implications

Health and Safety Implications

17. No implications

Health and Wellbeing Implications

18. No implications

Social Value

19. Not applicable

Scrutiny comments / recommendations:

20. The proposed decision has not been considered by a Scrutiny Committee, but has been provided to the Chair of the Joint Scrutiny for Local Government Reorganisation Committee for information and the Opposition Spokesperson.

All necessary internal consultations have been made with subject matter experts for all councils and internal auditors and extended to HR and Union representatives.

Background

21. Standard templates (ISO27001) were identified as a start point and are representative of existing policies used separately by the county council and the four district councils. Whilst there is no intention at the moment of seeking ISO27001, they are industry standard and meet compliance standards we do have to qualify for.

    As Information Security policies they detail what we will do, but not how we will do it. They complement policies produced by HR and Information Governance.

    SME representatives from the five councils updated and reviewed the templates into working policies. The LGR Technology Gateway Panel representing each of the councils then reviewed, provided feedback and approved individual groups of policies over the last year. The complete TGP approved policy set has since been reviewed by LGR HR and Union representatives and JNF. Approval has been sought and gained for the seven highlighted to the Executive Member.

    The policy set will be reviewed and updated by a similar process at agreed regular intervals.

Background Papers

Appendices

- Appendix A – 7 IT User Policies