Digital Security – Network Access and Availability

Contents:

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Digital Security

Background

Protecting the council's digital information assets is key to delivering the council's digital strategy. A failure of confidentiality, integrity or availability could have a significant effect on the ability of the council to deliver its services via digital platforms. This policy sets out the minimum requirements for access to the council's digital resources.

Key Messages

Access to the council's digital resources is only permitted from authorised devices by authorised personnel.

Access to digital resources will be controlled and monitored.

User accounts must be protected by a password.

User devices are not backed up by ICT, users must take care to ensure that important data is held in locations that are backed up: No important data should solely be stored on a user device.

Where the principles in this policy cannot be met, the risk must be recorded in the ICT Risk Management and Accreditation Database (RMAD) and authorised by the appropriate SIRO.

Policy Detail – Network Access

User Access

Access to the network will be controlled and monitored. Individuals will be given a unique account with which they will be able to access resources on the network.

The principles of role based access will be applied so that users have an appropriate level of access according to their function.

All accounts that are able to logon to the network must be traceable to an authorised and accountable individual.

Where a business unit has SIRO & ICT approval to use a generic network account, the business unit manager will be responsible for maintaining a record of use to maintain this accountability. This use of Generic accounts should be recorded in the RMAD and controls reviewed periodically to ensure they are effective.

All changes to user accounts and user rights must be authorised and logged.

User accounts will be disabled when no longer required.

User access and activity logs will be reviewed for unauthorised use.

Device Access

Access to the council's digital resources will only be permitted from devices owned and managed by the councils. The device must be authenticated.

Remote Access

The councils operate several technologies for remote access;

- Terminal Services via SSL VPN (Citrix and Juniper)
- Email to smart devices (ActiveSync)

Access to these services is only permitted from council owned and managed devices.

User access to Terminal Services platforms (Citrix and Juniper) will be protected by second factor authentication.

The Device and the User must be authenticated to the service.

Democratic Services Committee Application (Mod Gov)

Access to the Modern Government App and Website is not restricted to council owned and managed devices. Access is permitted from approved devices by authenticated users.

Data Backup

The council's' digital resources, stored on servers managed by ICT, will be regularly backed up.

Backups and incremental and will be held for 120 days/increments.

Backup data will not be solely stored on the same site from which the backup was obtained.

A random sample of test restores will be undertaken each month to verify the integrity of backed up data.

User devices are not backed up by ICT, users must take care to ensure that important data is held in locations that are backed up: No important data should solely be stored on a user device.

Personal Cloud storage

Personal Cloud Storage accounts (from any vendor) should never be used to store council data or conduct council business.

Apple iCloud is inappropriate for holding council data and should not be used even where the apple ID is provided by the council.

Other Cloud storage, where provided or managed by ICT, may be used where the Information Asset Owner permits that usage for that data.

Note:

Staff are reminded that smart devices should never be used as the primary means of storing council data. Data on smart devices is not automatically backed up, so any unique data should be moved to network storage (personal and shared drives) at the first opportunity - sending the information to yourself in an email is the easiest way to do this, then transfer any attachments to the appropriate Folder on the network, then remove the original from your smart device storage.

Email that is received on a smart device comes from the network - draft messages created on the smart device are stored on the device until they are successfully sent.

Staff should take a similar approach to any personal data they may be storing on a smart device i.e. photos, ensuring they have a copy of their personal data at all times. Network storage must not be used for personal data.

Variation from policy

The councils accept that occasionally, for operational reasons, it is not always possible to adhere closely to this policy. Requests for exemption will be considered by affected SIROs and granted on the merits of an individual case. Exemptions (and associated mitigations) will be recorded in the ICT RMADS and reviewed by the CIGG.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Incident Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
03/08/2016	Will Causton	1.0	Initial Version
23/09/2016	Will Causton/CIGG	1.1	Amended following CIGG Consultation
05/10/2016	Hannah Lynch	1.2	Final Formatting

Appendix 1 Supplier Remote Access and Desktop Sharing

In many cases, suppliers require remote access to provide contracted services.

The requirement for the councils to own and manage devices used to connect is relaxed for this purpose, however the supplier must demonstrate management of their staff and equipment to a comparable standard as set out in the device management standards and user access controls set out in part 2 of this policy.

Note: If suppliers request details of our device management standards, please refer them to this Government document and ask them to provide written assurance that they operate systems that meet these principles.

https://www.gov.uk/government/publications/end-user-devices-security-principles/end-user-devices-security-principles

EKS ICT will maintain an operational process for managing Supplier Remote Access. The process will ensure that whoever facilitates access (where this is not EKS ICT) will ensure that:

- The information asset owner or system administrator has authorised the access.
- The identity of the individual who was granted access is recorded.
- The services accessed are recorded.
- The session is authorised for no more than 24 hours.

Access for periods greater than 24 hours may be permitted to facilitate extensive upgrades or commissioned installation works. Extended access should be authorised for a set period by the EKS Technical Systems Manager (or their delegate) and noted in the ICT Risk Management and Accreditation Document Set (RMADS).

Remote access must take place from a country with adequate data protection legislation. (See Appendix 2)

Desktop Sharing with external Third Parties

For desktop sharing; where a user engages directly with a third party via direct remote assistance products (like GoTomeeting or Teamviewer), that allow remote viewing or control of a console (Desktop). The user is responsible for ensuring that:

- The remote access session is authorised by the information asset owner.
- Supervised.
- The supplier meets the minimum standards for device management.
- The access is logged via the ICT self-service portal so that a record is maintained.

Appendix 2: Access from overseas.

Guidance from the Cabinet office and the ICO indicate that not all countries have adequate data protection measures. Additionally, staff should recognise that in some foreign countries they should expect to undergo electronic surveillance. With that in mind remote access for any purpose should only be provided from safe locations.

The Data Protection Act says that:

Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The EEA countries are currently the EU countries plus Iceland, Liechtenstein and Norway:

Austria	Germany	Malta
Belgium	Greece	Netherlands
Bulgaria	Hungary	Norway
Croatia	Iceland	Poland
Cyprus	Ireland	Portugal
Czech Republic	Italy	Romania
Denmark	Latvia	Slovakia
Estonia	Liechtenstein	Slovenia
Finland	Lithuania	Spain
France	Luxembourg	Sweden
		United Kingdom

Certain countries have been deemed to offer an adequate level of protection for personal data. Currently, the following countries are considered as having adequate protection.

Andorra	Guernsey	New Zealand
Argentina	Isle of Man	Switzerland
Canada	Israel	Uruguay
Faroe Islands	Jersey	United States of America