Information Security Policy

Title: Information Security Policy	**Approved**:	**Effective from**: 01/09/2016	**Next review**: 12/12/2024
Version: 2.04	**Author**: Cliff Dean		**Last review**: 22/12/2022

Version History

Revision Date	Reviser	Previous Version	Description of Revision
July 2016	Cliff Dean	1.0	Updated to reflect password changes
October 2017	Cliff Dean	1.1	Updated Policy reference
February 2018	Cliff Dean	2.0	Updated role-based access
May 2018	Cliff Dean	2.01	Updated NDA, NCA and access control
July 2019	Cliff Dean	2.02	Updated PCI DSS notes
May 2020	Cliff Dean	2.03	Updated words and context on PCI logs and network creation process
December 2022	Andrew Herbert	2.04	Updated MFA, Passwords, ADR rules

Document Approvals

This document requires the following approvals:

Sponsor Approval
North Kesteven - Executive Board

West Lindsey - Corporate Policy and Resources Committee

Document Distribution

This document will be distributed to:

Name	Method
All staff	Intranet

Notes: All roles listed above receive copies, or are notified, of updated versions of the document.

The Method of Issue includes provision of paper or electronic copy of authorised document, or notification by e-mail to those with access to the authorised version on the Intranet.

1. Aim

a. To provide structure for the information security policy including information assets, protecting the data that we collect and store securely.
b. Key roles within the council maintain the privacy of individuals and deliver Information Assurance (IA)
    I. Senior Information Risk Owner (SIRO),
    II. System Owner (SO),
    III. Chief Information Owner (CIO IT),
    IV. Data Protection Officer (DPO),
    V. Information Asset Owner (IAO).
c. All colleagues understand that the information we hold is valuable. We are committed to preserving the confidentiality, integrity, and availability of our information assets:
d. for sound decision-making;
e. to deliver quality services to our citizens and customers;
f. to comply with the law;
g. to meet the expectations of our customers and citizens; and
h. to protect our reputation as a professional and trustworthy organisation.
i. Problems with any information we hold can cause issues for our staff, business, customers, citizens, and third parties. Information security is everyone's responsibility.

2. Scope

The Council has a strong information assurance structure which ensures that access to data is controlled and only provided to those that need it for the required duration. System Owners and Information Asset Owners are senior individuals that manage the risk associated with the use of data.

3. Definitions

Information Asset Owners role is to understand what information is held for their own business area, how that information is used, who has access to it and why. As a result, they can understand and address risks to the information, ensure that information is used appropriately, and provide input to the SIRO on the security and use of their information asset whether in paper or electronic format.

4. Principles

It is important that citizens can trust the council to act appropriately when obtaining and holding information and when using the authority's facilities. It is also important that information owned by other organisations which is made available to the Council under secondary disclosure agreements is treated appropriately.

5. Access Control and Asset Management

i. To control the access to information, stringent access controls are applied to any area or system where sensitive or protectively marked data is stored. Asset and configuration management controls are also in place and access to IT equipment and systems is strictly controlled.

ii. Removable media, such as laptops have encryption added which has been approved by National Cyber Security Centre (NCSC). USB memory devices are disallowed as standard and access to secure devices is only provided through a request, record and approve process.

iii. Access control for contractors is only provided for the minimum level of access that is required and is controlled by the Service Desk.

iv. The Service Desk takes care during the life cycle of an information asset. Members of IT are subject to a disclosure and barring service review. Controls are in place when the data is stored (e.g. secure server rooms), when data is in transit (e.g. use of encryption) and when disposal is required (following the guidance provided by NCSC).

v. Multi-factor authentication (MFA) to mitigate against password guessing and theft, including brute force attacks is available for all colleagues and is a recommended security enhancement.

6. Applying the Policy - Passwords

a. Choosing Passwords

i. Anyone needing access to IT systems is issued with a Microsoft network password and individual system passwords if they are not configured for single sign on. Single sign on is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some of our 3rd party systems seamlessly sign on at each system.
ii. Physical passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.
iii. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

b. Weak and strong passwords
   i. A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.
   ii. A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

c. Everyone must use strong passwords with a minimum standard of:
   i. At least 12 characters.
   ii. More complex than a single word (such passwords are easier for hackers to crack).
   iii. Using the three random words technique to help you create less predictable passwords.
   iv. By using a password that's made up of three random words, you're creating a password that will be 'strong enough' to keep the criminals out, but easy enough for you to remember.
   v. Login attempts should use a second step of Multi-Factor Authentication.
   vi. Conditional access risk assessments are made on user's login requests.
   vii. All cloud-based systems should have Multi-Factor Authentication enabled.

7. Protecting Passwords

a. It is of utmost importance that the password always remains protected. The following guidelines must always be adhered to:
   i. Never reveal your passwords to anyone.
   ii. Never use the 'remember password' function.

iii. Never write your passwords down or store them where they are open to theft.
iv. Never store your passwords in a computer system without encryption.
v. Do not use any part of your username within the password.
vi. Do not use the same password to access different Council Systems.
vii. Do not use the same password for systems inside and outside of work.

b. How are passwords discovered?
   i. Attackers use a variety of techniques to discover passwords. Many of these techniques are freely available and documented on the Internet, and use powerful, automated tools.
   ii. Approaches to discovering passwords include:
   iii. social engineering e.g. phishing; coercion
   iv. manual password guessing, perhaps using personal information 'cribs' such as name, date of birth, or pet names
   v. intercepting a password as it is transmitted over a network
   vi. 'shoulder surfing', observing someone typing in their password at their desk
   vii. installing a key logger to intercept passwords when they are entered a device
   viii. searching an enterprise's IT infrastructure for electronically stored password information
   ix. brute-force attacks; the automated guessing of large numbers of passwords until the correct one is found
   x. finding passwords which have been stored insecurely, such as handwritten on paper and hidden close to a device
   xi. compromising databases containing large numbers of user passwords, then using this information to attack other systems where users have re-used these passwords

c. Changing Passwords
   i. We will only ask users to change their passwords on indication or suspicion of compromise, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to the IT ServiceDesk.
   ii. Users must not reuse the same password within 6 password changes, one golden rule is users should never use the same password for both home and work.

8. Make sure the systems you deploy do not store passwords as plain text, even if the information on the protected system is relatively unimportant. Periodically search systems for password information that is stored in plain text.

9. All passwords should be stored in a hashed format, using multiple iterations of the hash function. Hashing is a one-way cryptographic function which converts a plain

text password into a 'hash', an unreadable string of characters designed to be impossible to convert back. However, attackers can still use brute-force attacks and rainbow tables (pre-computed tables for reversing cryptographic hash functions) to retrieve passwords from stolen hashes. For this reason, applications should add a 'salt' to a password before hashing. The hash function should follow public standards (such as PBKDF2), for example SHA-256.

10. An attacker who has accessed a password hash file will not know the actual passwords. But if the passwords have been hashed poorly, or the attacker has enough computing power, it may be possible for them to recover some of the passwords. For this reason it is important to protect access to the user database. As well as being a target for attackers looking to compromise your system, these are a target in their own right, even if the information is out of date.

11. **System Administration Standards**
    a. The following applies to administrative accounts
    b. The password administration process for individual Council systems is well-documented and available to designated individuals.
    c. All Council IT systems will be configured to enforce the following:
        i. Accounts must be provisioned with privileges appropriate for the user need. Administrator (or other high privilege) accounts should only be provisioned to users who need those privileges. Administrators must not conduct 'normal' day-to-day business from their high privilege account. Privileges should be periodically reviewed and removed where no longer required.
        ii. Users must identify and authenticate to devices and services. For passwords, you must:
        iii. ensure that ALL passwords are changed from defaults.
        iv. not allow password/account sharing.
        v. ensure that high-privilege users (i.e. administrators) use different passwords for their high-privilege and low-privilege user accounts.
        vi. combine passwords with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication.
        vii. ensure that passwords are never stored as plain text but are (as a minimum) hashed using a cryptographic function capable of multiple iterations and/or a variable work factor. It is advisable to add a salt before hashing passwords.
        viii. allow users several logins attempts before locking out accounts.
        ix. authentication of individual users, not groups of users - i.e. no generic accounts.
        x. protection with regards to the retrieval of passwords and security details.
        xi. system access monitoring and logging - at a user level.
        xii. role management so that functions can be performed without sharing passwords.

xiii. password admin processes must be properly controlled, secure and auditable.

12. Applying the Policy – Employee Access

a. User Access Management
   i. Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by the Council. Each user must be allocated access rights and permissions to computer systems and data that:
   ii. Are commensurate with the tasks they are expected to perform.
   iii. Have a unique login that is not shared with or disclosed to any other user.
   iv. Have an associated unique password that is requested at each new login.
   v. Allow users a number of login attempts before locking out accounts.
   vi. User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.
   vii. Employees have the right to use the equipment for work purposes only, personal usage of corporate devices is not allowed.

13. Information Security Requirements for Cloud Hosted applications

The Council uses the 14 Cloud Security Principles defined by the National Cyber Security Centre(NCSC) and colleagues should always adhere to these. This will help you build confidence in the cloud service, the company that runs it, the way that it's operated, and whether it gives you an effective set of security features. We recommend this approach when you are hosting 'Council' data in the cloud (such as personally identifiable, commercially sensitive and government OFFICIAL data). The Council also thinks that the cloud provider has a responsibility for services to be 'secure by design and by default'.

a. User Registration
b. A request for access to the Council's computer systems must first be submitted to the Service Desk using the Intranet new starters form. Applications for access must only be submitted by immediate Line Managers.
c. When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of your Line Manager to request the suspension of the access rights via the Intranet Leavers Form.

User Responsibilities

d. It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:
e. Following the Password Policy Statements outlined above in Section 7.
f. Ensuring that any device they are using that is left unattended is locked or logged out.
g. Leaving nothing on display that may contain access information such as login names and passwords.
h. Ensuring that they keep their password safe.
i. Ensuring that their Line Manger informs the Service Desk of any changes to their role and access requirements.
j. Change ALL default passwords.
k. Remove the bitlocker usb stick following the logon process.

14. Network Access Control

The use of modems on non-Council owned PCsconnected to the Council's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from the Service Desk before connecting any equipment to the Council's network.

15. User Authentication for External Connections

Where remote access to the Council's network is required, an application must be made via the IT Service Desk. Remote access to the network must be approved by a request to the Service Desk.

16. Supplier's Remote Access to the Council Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from the appropriate Team Manager and the ServiceDesk. Any changes to supplier's connections must be immediately sent to the IT ServiceDesk so that access can be updated or ceased. All permissions and access methods must be controlled by the appropriate Team Manager (application systems) and the IT ServiceDesk (network access).

Partners or 3rd party suppliers must contact the IT ServiceDesk before connecting to the Council network, and a log of activity must be maintained. Remote access software must be disabled when not in use.

All suppliers must complete both a non-disclosure and network connection agreement or if not completed a Head of Service or Strategic Lead shall evidence the exception.

17. Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the Access Control and Asset Management (section 6) and the Password section (section 7) above must be applied. The login procedure must also be protected by:

a. Not displaying any previous login information e.g. username.

b. Limiting the number of unsuccessful attempts and locking the account if exceeded.
c. The password characters being hidden by symbols.
d. Displaying a general warning notice that only authorised users are allowed.
e. All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).
f. System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

18. Application and Information Access

a. Access within software applications must be restricted using the security features built into the individual product. The local systems administrator of the software application is responsible for granting access to the information within the system. The access must:
b. Be compliant with the User Access Management section (section 6) and the Password section (section 7) above.
c. Be separated into clearly defined roles.
d. Give the appropriate level of access required for the role of the user.
e. Be unable to be overridden (with the admin settings removed or hidden from the user).
f. Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
g. Be logged and auditable.

19. PCI – DSS

For colleagues involved in the processing of customer payments the following standards shall apply:

a. Protect stored cardholder data- keep storage to a minimum
b. Card application systems will be restricted so access is provided on business need basis
c. Card payment system checks will be recorded
d. Staff working with cardholder payments will undertake enhance pre – employment checks
e. An IT Health check will be undertaken on an annual basis.
f. An internal scan and the results and actions will be recorded within the IT Service Desk.
g. An external scan and the results and actions will be recorded within the IT Service Desk.
h. For any incident on any device used in connection with payment card transactions full details should be reported to the IT ServiceDesk and the payment card service provider immediately.

i. Payment card data will not be stored within the Council network.
j. The IT Service Desk will be used to capture the review and actions for the logs for the PCI-DSS network.

20. Software

Software should not be downloaded or installed by staff, this includes software shared on mobile device, the internet, and DVDs attached to magazines or distributed both inside and outside the organisation. Staff should not attempt to install any software.

When hardware e.g. laptop is decommissioned, the asset id should be removed from the asset list and the software asset register should be updated so that if possible the software license can be reused.

IT colleagues as part of the desktop refresh programme will arrange for the secure disposal of hardware. IT staff will, for individual hardware failures, remove hard drive then shred using an external company.

The hardware will be removed from the network by IT colleagues. Licensing details to be updated on LanSweeper by IT colleagues.

21. HR Security

All staff employed by the Council are required to undergo pre-employment checks.

After taking up duty, all new staff attend induction training that covers data security principles. Staff also must complete the Data Protection and Information Assurance training package. The council keep records of all training completed.

Staff who use information processing facilities are subject to the conditions of the Corporate IT Access Policy.

Third party access will only be provided after a signed network agreement is verified by the ICT Team.

22. Physical Security

To prevent unauthorised physical access, damage or interference to council premises and information, all council buildings are secured. Access to data storage areas is further secured with an additional alternative solution.

23. Incident Management

To ensure information security events and weaknesses associated with any council assets are captured, the council has a well-established incident management process and uses regular IT Health Checks to enhance security and monitoring. All reports are documented, followed up and reported to Senior Management.

24. Business Continuity

The Council has an excellent and robust approach following the national standard for business continuity. The management of IT assets to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters, the council have defined business continuity plans, procedures, roles and responsibilities.

25. Background Legislation

a. Data Protection Act 2018

Personal information relating to identifiable individuals must be kept accurate and up to date. It must be fairly obtained and securely stored. Personal information may only be disclosed to people who are authorised to use it. Unauthorised disclosure of council or client personal information is prohibited and could constitute a breach of this Act.

b. Computer Misuse Act 1990

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is not allowed and would constitute an offence under this Act for which the penalties are imprisonment and/or a fine.

This Act addresses the following offences:

Unauthorised access to computer material.

Unauthorised access with intent to commit or facilitate commission of further Offences.

Unauthorised modification of computer material.

c. Copyright, Patents and Designs Act 1988

Documentation must be used strictly in accordance with current applicable copyright legislation, and software must be used in accordance with the licence restrictions. Unauthorised copies of documents or software may not be made under any circumstances.

d. Companies Act 1985

Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.

e. PCI DSS

Is the core PCI standard as it applies to any organisation that stores, processes, and/or transmits cardholder data. This includes businesses, processors, acquirers, issuers and service providers. Literally every entity in the payment processing industry.

f. Freedom of Information Act 2000

This Act gives a general right of access to all types of data and information that has been recorded by the council.

The Council is also progressing its compliance activities associated with General Data Protection Regulation.

By signing below, I agree to the following terms:

1. I have received, read and understood a copy of the ICT Security Policy

2. I will strictly abide by the Policy;
3. I accept and agree that my computer usage may be monitored.

Signature: _____

Name: _____

Date: _____