Information Security Policy

April 2018

districtnk
100 flourishing communities
North Kesteven District Council

Alternative Formats

This document can be made available in large print, Braille, audio tape, electronic formats such as CD, or in a different language. Our website is ReadSpeaker enabled. For a copy please contact the Corporate Information Team at the Council using the following options:

Phone: 01529 414155 (main switchboard)

Fax: 01529 413956

Web: www.n-kesteven.gov.uk

Email: equality@n-kesteven.gov.uk

Corporate Information Manager
North Kesteven District Council
Kesteven Street
Sleaford
Lincolnshire
NG34 7EF

Introduction

The purpose of this policy is to provide structure for information security and covers information assets, protecting the data that we collect and ensuring it is stored securely.

The key roles within the Council maintain the privacy of individuals and deliver Information Assurance (IA) are :

- Senior Information Risk Owners (SIRO),
- System Owner (SO),
- Chief Information Owner (CIO),
- Data Protection Officer (DPO),
- Information Asset Owners (IAOs).

It is vital that all colleagues understand that the information we hold is valuable. We are committed to preserving the confidentiality, integrity, and availability of our information assets:

- for sound decision-making;
- to deliver quality services to our citizens and customers;
- to comply with the law;
- to meet the expectations of our customers and citizens; and
- to protect our reputation as a professional and trustworthy organisation.

Information security is everyone's responsibility. Problems with any information we hold can cause issues for colleagues, business, customers, and third parties. This policy links with the Council's Records Management and Retention Policy and Confidential Waste Policy.

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 manage the risk associated with the use of data.

Definitions

The Information Asset Owner's 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 are able to understand and address risks to the information, ensure that information is used appropriately, and provide input to the SIRO on its security (whether in paper or electronic format).

Principles

It is important that customers are able to 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.

Access Control and Asset Management

To control the access to information, stringent access controls are applied to any area or system where official-sensitive or protectively marked data is stored (please also see the Protective Marking Policy). Asset and configuration management controls are also in place and access to IT equipment and systems is strictly controlled.

Removable media, such as laptops, have encryption added which has been approved by the 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.

The IT Team takes particular care during the life cycle of an information asset. Information assets are documents or records in several different formats, for example, emails, reports, various

software applications, and so on. Controls are in place when the data is stored (for example, secure server rooms), when data is in transit (for example, use of encryption) and when disposal is required (following the guidance provided by the NCSC). Members of IT are subject to a disclosure and baring service review to ensure high levels of integrity within the service.

Apply the Policy – Passwords

Choosing Passwords
Anyone needing access to North Kesteven District Council IT systems is issued with a one-time only password device called a Cryptocard. This device will also provide access to the parts of the building that individuals are permitted to use during the authorised hours. In addition, colleagues have a Microsoft network password and individual system passwords (if they are not configured for single sign on). Single sign on provides access control for multiple related, yet independent, software systems. With this, 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 some of our third party systems) seamlessly.

Physical passwords are the first line of defence for the Council's IT systems and together with the user ID help to establish that individuals are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of the Council's computers and systems. The Cryptocard device is personally configured and cannot be used on any other user account. If lost, an individual may be charged for a replacement at their Line Manger's discretion.

Weak and Strong Passwords
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.

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. All users must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain at least three out of the following four character types of alpha upper and lower case, numeric, and special characters, such as $
- More complex than a single word (such passwords are easier for hackers to crack).

For example: Tk5£5Z0cDd!

Protecting Passwords
It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal passwords to anyone.
- Never use the 'remember password' function.
- Never write passwords down or store them where they are open to theft.
- Never store passwords in a computer system without encryption.
- Do not use any part of a user's username within the password.
- Do not use the same password to access different North Kesteven District Council Systems.
- Do not use the same password for systems inside and outside of work.

How are Passwords Discovered?
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. Approaches to discovering passwords include:

- social engineering, for example, phishing; coercion
- manual password guessing, perhaps using personal information 'cribs' such as name, date of birth, or pet names
- intercepting a password as it is transmitted over a network
- 'shoulder surfing', observing someone typing in their password at their desk
- installing a key logger to intercept passwords when they are entered into a device
- searching an enterprise's IT infrastructure for electronically stored password information
- brute-force attacks; the automated guessing of large numbers of passwords until the correct one is found
- finding passwords which have been stored insecurely, such as handwritten on paper and hidden close to a device
- compromising databases containing large numbers of user passwords, then using this information to attack other systems where users have re-used these passwords

Changing Passwords
Users will only be asked to change their passwords on indication or suspicion of compromise, or whenever a system prompts a user to change it. Default passwords must also be changed immediately. If a user become aware, or suspects, that their password has become known to someone else, it must be changed immediately and concern are to be reported to the IT Helpdesk Users must not reuse the same password within six password changes; one golden rule is users should never use the same password for both home and work.

System Administration Standards
The password administration process for individual North Kesteven District Council systems is well-documented and available to designated individuals.

All North Kesteven District Council IT systems will be configured to enforce the following:

- 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.

Users must identify and authenticate to access devices and services. For passwords, users must:

- ensure that ALL passwords are changed from defaults
- not allow password/account sharing
- ensure that high-privilege users (i.e. administrators) use different passwords for their high-privilege and low-privilege accounts
- combine passwords with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication
- 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.

The IT Team will allow users a number of login attempts before locking out accounts:

- Authentication of individual users, not groups of users, i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.

- System access monitoring and logging – at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

Applying the Policy – Employee Access

User Access Management
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 North Kesteven District Council. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.
- Allow users a number of login attempts before locking out accounts.

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.

User Registration
A request for access to the Council's computer systems must first be submitted to the IT Team using the Intranet new starters form. Applications for access must only be submitted by immediate Line Managers.

When a colleague leaves the Council, their access to computer systems and data must be suspended at the close of business on their last working day. It is the responsibility of a Line Manager to request the suspension of the access rights via the Intranet Leavers Form.

Roles and Responsibilities

All Employees
It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

- Following the password requirements, as detailed earlier in the Policy
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Ensuring Cryptocard device is kept safe.
- Ensuring Line Manger informs the IT Team of any changes to a user's role and access requirements.
- Change ALL default passwords.

Network Access Control
The use of modems on non-Council owned PC's connected 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 IT Team before connecting any equipment to the Council's network.

User Authentication for External Connections
Where remote access to the North Kesteven District Council network is required, an application must be made via the IT Helpdesk. Remote access to the network must be secured by two factor authentication consisting of a username and a one-time only password obtained from the IT Helpdesk. For further information please refer to the Remote Working Policy.

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

Partners or third party suppliers must contact the IT helpdesk before connecting to the NKDC network, complete the change control log before logging onto a server and a log of activity must be maintained. Remote access software must be disabled when not in use.

Operating System Access Control
Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section and the Password section (detailed earlier in the Policy) must be applied. The login procedure must also be protected by:

- Not displaying any previous login information, for example, username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised users are allowed.

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 (for example, administration rights).

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.

Application and Information Access
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:

- Be compliant with the User Access Management section and the Password section detailed earlier in the Policy.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

Responsibilities
All colleagues are required to undergo pre-employment checks.

After taking up duty, all new colleagues attend induction training that covers data security principles. Colleagues also have to complete the General Data Protection Regulations and Information Assurance training package. The Council retains statistics of all training completed.

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

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.

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.

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. For further information, please see the IT Disaster Recovery Policy.

Background Legislation

Data Protection Act 1998 and EU Directive on Data Protection
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 (please see the Data Protection Policy for further information).

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:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

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.

Companies Act 1985
Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.

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.

Policy Review

This Policy will be formally reviewed every two years to ensure it continues to be relevant and current. In some circumstances it may be necessary to review this Policy more frequently in response to specific events.