Corporate Information Governance Group CIGG

Information Governance Policy Framework

EKservices

Password Policy

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policy 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.

Password Policy

Background

Passwords are a key method in protecting the data for which we are responsible. Good password choices defend the organisation from loss or theft of data and protect you from impersonation and identity theft. This policy document sets out the minimum standards everyone must adhere to when making decisions about passwords.

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password testing is performed on a periodic basis; breaches of this policy will be reported as an Information Security Incident.

Key Message

Mobile devices, (e.g. phones and tablets) must be protected by a screen lock password. As a minimum, this can be a 4 digit pin or longer if the system supports it. It must be changed every 90 days, or whenever there is a suspicion that the passcode is compromised.

The main network password (also known as the Active Directory Password) must be at least 12 Characters long and contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numbers 0 to 9
- Non-alphabetic characters (for example,!, $, #, %)

The password must be changed at least every 365 days or whenever there is reason to believe the password is compromised. A password generator is available if required which creates passwords that exceed the required standard if you would like some suggestions; this can be found by using the following link Password Generator

Passwords should never be written down or stored on-line without encryption.

Responsibilities

All users will familiarise themselves with this password policy. If you observe a breach of this policy, report it to the ICT Service Desk.

System Administrators will familiarise themselves with the Supplement for Business Systems within this policy.

ICT Staff will familiarise themselves with the Supplement for ICT Systems within this policy.

Policy Detail:

Password Protection Standards:

Always use different passwords from the ones you use in your personal life or for other organisations.

Always use different passwords for the various systems within the organisation.

Do not share your passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information. (Exceptions to this are during ICT Support sessions, where the password must be changed afterwards)

Passwords should never be written down or stored on-line without encryption.

Do not reveal a password in email, chat, or other electronic communication.

Do not reveal a password on questionnaires or security forms.

If an unauthorised person requests a password, or there are other suspicious circumstances, do not provide the password. Report the request immediately to the ICT Service Desk.

If an account or password compromise is suspected, the password must be changed and the incident reported to the ICT Service Desk promptly.

Password Standards

Mobile Devices

Mobile devices, like iPhones and Tablets must be protected by a screen lock password. As a minimum, this must be a 4 digit pin and require only numbers. Where the Mobile Operating system allows the use of a longer PIN (i.e. 6 Numbers) the longer length must be used. It must be changed every 90 days, or whenever there is a suspicion that it is compromised.

The Main Network Password

Some advice that may help you remember a longer password is that you use three consecutive words with some special characters included; these are very strong and can be easier to remember that a random string of letters and numbers.

For example;

OrangeCatch£Price!

The phrase itself is easier to remember as it is so unusual; it is made a strong password by inclusion of upper and lower case letters with special characters placed between the words.

If you have more than one account, it is permitted to re-use up to two thirds of the password as an “aide memoir” as long as each password is substantially different and changed regularly to extend the above example the following are samples of sufficiently different passwords.

PeachCatch£Price!

AppleCatch£Price!

(NOTE: Do not use any of these examples as passwords!)

Explicit Requirements for the Main Network Password

The password must:

Be at least 12 Characters long and contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numbers 0 to 9
- Non-alphabetic characters (for example,!, $, #, %)

The password must not:

- Be a single word, words or Phrase that are in common usage.
- Contain a sequence of known names i.e. family, pets, friends, co-workers, fantasy characters,
- Computer terms and names, commands, sites, companies, hardware, software,
- Birthdays or other personal information such as addresses and phone numbers.
- Car Registration plates
- Contain any of the above spelled backwards.
- Contain any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Contain any word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Contain any variation of the word “Password” (e.g. Passw0rd, P455w0rd)

Internal only Systems

For systems which are already protected by the Main Network Password, i.e. they are only available once you have logged on using the Main Network Password, password restrictions can be relaxed and it is not required that this policy is followed. The Business Administrator for that system, in consultation with the Information Asset Owner may choose to allow lower strength passwords more appropriate to the data contained within that system. In many cases, a password will still be required. But it is for the Information Asset Owner to decide and communicate what is appropriate for that system.

Remote Access

Access to the Organisation Networks via remote access (i.e. Citrix) will be controlled using a 2nd factor authentication. (Tokens)

Password Release Policy

Passwords for accounts and systems may only be released or reset once the identity and authority of the requester has been proven. All Users have the authority to request a password reset for their own account. Line managers can request a password reset for any of their staff that are accountable to them (for when staff are on leave or similar).

All password reset requests must be recorded by ICT. Only one person should know the password beyond what is required to handle a password reset.

Supplement for Business Systems

Within our organisation there are many systems protected by a second password, e.g. Training or Admin Systems. Where these are only available once staff have logged onto the main network using a very strong password, the Information Asset Owner can make a decision to relax the requirements of a strong password if they feel that the information contained within that system does not require that level of protection. In this case, the owner of that Information Asset must communicate their minimum requirements to the users of that service. The IAO should also document the reasons for doing so and conduct regular reviews to establish that it continues to be appropriate.

Supplement for ICT Systems

All system-level passwords with non-expiring passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least every 180 days.

Where possible, accounts with non-expiring passwords should not be created, where this is not practical, knowledge of this password must either reside with a single named individual or the password must be created by two members of staff who confidentially create half the password each.

Non expiring passwords (e.g. for Service Accounts) must be a minimum of 21 Characters long. Care should be taken to establish that the service that requires this should be able to survive the password being reset. Additional steps should be taken to limit the activity of the account in question (eg restricting where it can be used). Contact the Network and Security team for advice.

User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

Where SNMP is configurable, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

Default passwords must not be used on any system and must be changed at the earliest possible opportunity.

Where ICT staff have more than one Account for administrative reasons, different passwords must be used on each account.

Occasionally, for troubleshooting purposes an ICT Technician may temporarily change a user’s password to something both the ICT Technician and the user know in order to assist with support or diagnosis as a short term measure. A Service Desk ticket must be raised to record that this has happened and closed only when the account has had a password set known only to the account holder.

Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Shall support authentication of individual users, not groups.
- Wherever possible, shall not store passwords in clear text or in any easily reversible form shall provide for role management, such that one user can take over the functions of another without having to know the other's password.

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 Office.

Document Control		
Title/Version	-	CIGG Password Policy 1.0
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	

Revision History

Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
22/10/2015	Will Causton	1.0	Initial Version
19/01/2016	Hannah Lynch	1.1	Format Changes
23/09/2016	CIGG	1.2	Final Review