

****

**East Renfrewshire Council**

**Multi-Factor Authentication Policy for Council Systems**

|  |  |
| --- | --- |
| Name of Record | ERC MFA Policy  |
| Author | HR Manager & Head of Digital & Community Safety |
| Owner | Head of Digital & Community Safety |
| Status | Approved by CMT |
| Approved by | CMT  |
| Date of Publication | 08/03/2023 |
| Review Date | 08/03/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Notes | Author | Date |
| 1.0 | Creation of a new policy  | HR Manager & Head of Digital & Community Safety | Mar 23 |

**

**PURPOSE**

The purpose of this policy is to define how and when the additional security provided by multi-factor authentication will be used to access systems within the Council, including the responsibilities of employees.

**SCOPE**

This policy applies to all East Renfrewshire Council and East Renfrewshire Culture and Leisure Trust employees, as well as any other type of worker accessing our systems where MFA is applied. For the purposes of this policy, the word Council will be used to also cover East Renfrewshire Culture and Leisure Trust.

This policy applies whether the systems are accessed through Council or personal devices, at work locations or at other locations such as a person’s home.

This policy applies to any system where access is being provided across the public internet and/or where a system contains confidential or restricted data (OFFICIAL-SENSITIVE) or that requires an additional layer of protection as determined by the System Provider, System Product Owner, Data Protection Officer or Information Security Officer.

The requirement to implement MFA derives from:

* the adopted mandatory standard (reference Standard DAB0001) as defined by the Scottish Local Government Digital (SLGDO) Office Digital Assurance Board (DAB) which implements the National Institute of Standards and Technology NIST SP 1800-17b/c standard;
* the technical requirement under Principle (f) of the Data Protection Act to ensure secured access to hosted systems;
* NCSC guidance[[1]](#footnote-1);
* Scottish Government Public Sector Cyber Resilience Framework which mandates MFA for cloud hosted systems.

**DEFINITIONS**

Multi-Factor Authentication (MFA)

MFA provides an extra layer of security for accessing Council systems designed to ensure that the person requesting access is actually who they claim to be and that this cannot be refuted.

Passwords are very hard for users to generate and store securely but very easy for hackers to steal or guess. MFA provides additional authentication checks to ensure that one or more of the other authentication methods (usually a password) have not been compromised

It is an authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are **something you know**, **something you have**, and **something you are**.

Examples of these factors include:

|  |  |  |
| --- | --- | --- |
| **Something you know:** | **Something you have:** | **Something you are:** |
| Password | Authenticator app on portable device with One Time Passwords (OTPs) | Fingerprint |
| PIN | Text Message/Phone call  | Retinal Scan |
| Memorable date/place/other info | Physical token (such as ID card or USB dongle) | Face ID |
|  | Certificates securely stored on devices | Location Analysis (specific trusted IP address) |
|  |  | Behaviour Analysis (what time do you normally log-on, how long do you log on for) |

System User

Any person accessing, logging into, or attempting to access or log into, a Council hardware or software system; or connecting to, or attempting to connect to or navigate a Council network, whether by hardware or software or both, from any location.

The term "System User" includes employees on permanent or fixed term contracts (temporary), workers such as casuals, agency workers (employed through 3rd party organisations), contractors who are self-employed and engaged on a project through the Council, and any System Providers who require access to the system for the purposes of supporting the Council.

System Provider

A contracted supplier of the Council who are the primary provider and support the organisation for technology solutions.

System Product Owner

A defined responsible person with a service or department who has been formally assigned the responsibility of Product Owner of a particular system. This may be an individual's named role or a part responsibility of a role and may also be referred to as the Information Asset Owner (operational business manager with responsibility for the information assets).

**POLICY**

**When**

All System Users who have access to systems being provided across the public internet and/or where a system contains confidential or restricted data or that requires an additional layer of protection must use MFA. This is determined by Council parties such as the Information Security Officer, System Product Owner and/or the Data Protection Officer in collaboration with the System Provider who can assist with options available.

**How**

Where MFA is delivered through the use of a trusted IP address (something you are) there will be no need for individual user action to achieve MFA other than the use of username & password (something you know).

Where MFA is delivered through the use of a 2nd factor based on a physical device (something you have) then the System User will be required to do the following:

* One-time password (OTP) – the System Users will be required to set up a device to serve as the second authentication method. This device can be a council provided or personal mobile phone with a free authenticator app installed (such as Microsoft Authenticator or Google Authenticator).
* Text Message/Phone Call – the System Users will be required to identify a device to serve as the second authentication method. This second device can be a council provided or personal mobile phone (or Council desk phone where a phone call is the method).
* Physical token – the System User will be provided with the relevant token either by the System Owner or ICT.
* Local Certificate – the System Users laptop or desktop will be configured with the relevant certificate by ICT.

Where staff do not have access to any device to undertake MFA they should make their line manager aware so that a review can be undertaken to identify if any alternative arrangements can be made.

**What**

Every system that implements MFA will deliver this in different ways, often supporting a different range of factors. A partner document to this policy, MFA System Schedule, defines the specific details and factors for each MFA enabled system within the Council. This schedule will be updated regularly by ICT, but no later than the review date of this policy.

**EXCEPTIONS**

For systems that are MFA enabled, there will be no exceptions to the use of MFA to access those systems.

**PERIODIC REVIEW OF THIS POLICY**

Due to the rapid change in technology, this policy will be reviewed in line with system changes and the increased usage of MFA across Council systems and processes.

**POLICY COMPLIANCE**

The purpose of MFA is to enhance the Council’s data security so that only the System User is accessing their account. Where a System User is found to be in violation of this policy, access to Council systems may be revoked and, where they are an employee of the Council, a disciplinary process will be followed.

1. National Cyber Security Centre is a UK Government organisation responsible for providing guidance and support for cyber threats. [↑](#footnote-ref-1)