Information Security

Password Management Policy for Web Users

Document Classification:	Public
Document Ref.:	ECMWF-InfoSec-A05-04-PO
Issue:	1.5
Date:	22/04/2024
Document Author:	Information Security Team
Document Owner:	Information Security Officer
Document Status:	Issued

Revision History

Issue	Date	Revision Author	Summary of Changes
1.0	13/11/2019	Michele Di Mascolo	First Draft
1.0	27/02/2020	Ahmed Benallegue	Finalisation of the first document
1.1	26/01/2023	Giacomo Rollo	Review of Chapter 4 and Annex A
1.2	21/02/2023	Giacomo Rollo	General review
1.3	27/03/2023	Ahmed Benalleue	Document review
1.4	22/05/2023	Ahmed Benallegue	Minor update to Annex A
1.5	22/04/2024	Giacomo Rollo/Ahmed Benallegue	Document review

Approval

Name	Position	Date
Florence Rabier	Director General	05/09/2024

Distribution

Name	Department
Public	All

Relevant Documentation

Document Reference	Document Title	Issue
ECMWF-InfoSec-PO-A05-01	ECMWF Information Security Policy	2.2
ECMWF-InfoSec-A05-03-PO	Password Management Policy	2.4

Contents

Definitions

Definitions used in this document are listed here:

System Administrator	IT professional responsible for managing and maintaining the operation, configuration, and security of computer systems, servers, networks, and associated software and hardware within ECMWF. Their duties typically include installing, configuring, and updating operating systems and software, monitoring system performance, troubleshooting technical issues, implementing security measures, and ensuring data integrity and availability.
End-user	ECMWF staff, external users, contractors, and third-party providers, accessing systems managed or provided by ECMWF.

1 Introduction

Passwords are an important aspect of Information Security. All users with web access to ECMWF systems are responsible for taking appropriate steps, outlined below, to select and secure their passwords.

2 Purpose

The purpose of this Policy is to establish the standard to be applied for the creation of web access passwords, the protection of those passwords, their frequency of change and other relevant security precautions in relation to passwords.

3 Scope

This Policy applies to all End-users.

4 Password Management Policy

4.1 Password Creation

- Passwords must be unique for each account provided by ECMWF.
- Passwords must conform to the guidelines defined in Annex A - Password Construction Guideline.
- Endusers must use passwords for ECMWF accounts that are different from any other of their account (e.g. personal ISP account, personal email accounts etc.).

4.2 Password Change

- "First time" passwords, or passwords auto generated through forgot/reset features must be valid for 30 days (maximum) and must be changed by the user after the first/next access.
- Passwords must be:
    - Changed every 12 months
    - Different from 10 previously chosen passwords

4.3 Password Protection

All passwords are to be treated as sensitive information:

- Passwords must not be shared with ECMWF staff, other users and third parties.
- Passwords must not be inserted, in clear text, into email messages, instant messaging or other forms of electronic communication.
- Passwords must not be revealed over the phone, on questionnaires or on security forms.
- Passwords must not be written down and stored anywhere in the office or at home.
- Passwords must not be stored on-line or in a file on a computer system or mobile devices (phone, tablet) in clear text.

Additional protection measures:

- Use of password management tools is highly recommended.
- Systems or applications default password accounts must be disabled.
- If an account compromise is suspected:
  - Any incident must be reported as soon as possible to ECMWF's ServiceDesk.
  - All passwords related to the affected account must be changed.

4.4 Use of Multi Factor Authentication (MFA)

The use of MFA is mandatory to access sensitive information, including but not limited to:

- Corporate emails.
- Personnel information.
- Critical systems such as the ERP.

When available, adoption of Multi Factor Authentication (MFA) solutions is strongly recommended.

5 Roles and responsibilities

The System Administrators are responsible for:

- Configuring the managed systems in compliance with Section 4 of this Policy.

The End-users are responsible for:

- Complying with this Policy, specifically with Section 4 of this Policy.
- Reporting if they become aware of a breach or a potential breach of this Policy. Reports can be made to ECMWF's ServiceDesk

6 Policy Review

This Policy will be reviewed annually at the beginning of each calendar year or when significant changes are required.

Reading, September 2024

The Director-General

7 Annex A - Password Construction Guideline

All passwords should meet or exceed the following guidelines.

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain characters from at least 3 of the following 4 categories:
    - Lower case characters (e.g. a-z)
    - Upper case characters (e.g. A-Z)
    - Numeric characters (e.g. 0-9)
    - Special characters (e.g. @#$%^&*()+|~-=\`{}[]:";'<>/).

Poor, or weak, passwords have the following characteristics:

- Contain less than 12 characters.
- Contain the user's account name or part of the user's full name that exceed two consecutive characters.
- Can be found in a dictionary, including foreign languages, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fictional characters.
- Contain work-related information such as companies' names, building names, system commands, sites, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward or preceded or followed by a number (for example: terces, secret1 or 1secret).
- Are some versions of "Welcome123" "Password123" "Changeme123"

It is recommended to use password managers when possible.

Password managers have built-in password generators that create randomised, unique, and strong passwords.