Information Security

Password Management Policy

Document Classification:	Internal
Document Ref.:	ECMWF-InfoSec-A05-03-PO
Issue:	2.3
Date:	22/05/2023
Document Author:	InfoSec Team
Document Owner:	Information Security Officer
Document Status:	Final

Revision History

Issue	Date	Revision Author	Summary of Changes
1.1	23/03/2016	Ahmed Benallegue	Change to the frequency of change
2.0	28/09/2017	Michele Di Mascolo Ahmed Benallegue	• User-level and system-level password management policy merged • New InfoSec template • Clarification of Password lifecycle • Application Development Section added • Password Construction Guideline added as Annex
2.1	26/01/2023	Giacomo Rollo	Updates to chapter 5 and Annex A
2.2	20/02/2023	Ahmed Benallegue	Document review
2.3	22/05/2023	Ahmed Benallegue	Minor update to Annex A

Approval

Name	Position	Date
Martin Palkovic	Director of Computing	22/05/2023

Distribution

Name	Department
ECMWF InfoSec Representatives	All
ECMWF InfoSec Champions	All
ECMWF staff, external users & third parties	N/A

Relevant Documentation

Document Reference	Document Title	Issue
ECMWF-InfoSec-PO-A05-01	ECMWF Information Security Policy	1.0
ECMWF-InfoSec-A05-04-PO	Password Management Policy for Web Users	1.4

Contents

1 Introduction

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

2 Purpose

The purpose of this document is to establish the standard to be applied at ECMWF for the creation of user-level and system-level passwords, the protection of those passwords, their frequency of change and other relevant security precautions.

3 Scope

This policy applies to ECMWF staff, external users and third parties that have a user account provided by ECMWF or is responsible for an account or any form of access that supports or requires a password on any system that resides in ECMWF premises or in any cloud computing services accessed for the purposes of ECMWF's business.

4 Definitions

User-level password: passwords used for user accounts, e.g.: desktop computer, email, web.

System-level passwords: passwords used for service accounts such as root, Windows Administrator accounts, system administration accounts, application administration accounts, non-interactive authentication between servers and applications, password used to access ECMWF's wireless network, etc.

5 Password Management Policy

5.1 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.
- Always use different passwords for ECMWF accounts from other non-ECMWF accounts (e.g. personal ISP account, personal email accounts etc.).

5.2 Password Change

- System-level passwords must be
  - changed every 4 months.
  - different from any previous passwords.
  - changed if a user who has access to them leaves ECMWF.
- User-level passwords must be
  - changed every 12 months.
  - different from 10 previous passwords.

5.3 Password Protection

- All passwords are to be treated as sensitive confidential ECMWF information.
- Passwords must not be shared with ECMWF staff, external users and third parties except for operational or administrative needs. Shared passwords must be properly manged.
- “first time” passwords or passwords auto generated through forgot/reset features must be changed by the user after the first/next access. The initial or “first-time” passwords will automatically expire after a month. First-time password can be communicated by email messages, instant messaging or other form of electronic or non-electronic communication.
- 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 security forms.
- Passwords must not be written down and stored anywhere in the office or at any other location used for teleworking, including home.
- All system-level passwords are to be kept in sealed envelopes in a safe in the Console area under the supervision of the Shift team. It is the Section Heads’ responsibility to ensure that the system-level passwords relevant to their sections are up-to-date and properly destroyed when no longer needed.
- Passwords must not be stored on-line or in a file on a computer system or mobile devices (phone, tablet) in clear text. Use of password management tool is highly recommended.
- Do not hint at the format of a password (e.g. "my family name").
- Systems or applications often have default accounts. When possible, they should be disabled completely. If the account cannot be disabled, the default passwords should be changed immediately upon installation and configuration.
- If an account compromise is suspected, the incident must be reported as soon as possible to ECMWF’s Servicedesk. All passwords related to the affected account must be changed.

5.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

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

6 Compliance

6.1 Enforcement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, business tool reports, internal and external audits and feedback to the policy owner.

Password cracking or guessing may be performed on a periodic or random basis by the Information Security Team or its delegates. If a password is guessed or cracked during one of these scans, the responsible entity will be required to change it to be in compliance with the Password Construction Guideline defined in Annex A.

6.2 Exceptions

Any exception to the policy must be approved by ECMWF’s Information Security Governance Board. The exceptions are temporary and will be reviewed regularly to grant the compliance to the policy. All the approved exceptions, with the relative expiration time, will be listed in a separated document.

6.3 Non-Compliance

Non-compliance with ECMWF's security standards may be considered as misconduct in line with Articles 37 and 38 of the Staff Regulations.

7 Policy Review

This policy and the relative exceptions will be reviewed annually at the beginning of each calendar year or when significant changes are required.

8 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 character such as @#$%^&*()_+|~-=\`{}[]:";'<>/

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 building names, system commands, sites, companies, 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 version of "Welcome123" "Password123" "Changeme123"

A good method for password selection is to pick a known phrase that can be remembered, then choose the first or last letter of the first twelve words to be the password. For example, Ih8W@Es2A1mh for "I have been working at ECMWF since 2002 and I am happy".

Password managers have built-in password generators that create randomised, unique and strong passwords. It is recommended to use them when possible.