Information Security

Password Management Policy for Web Users

Document Classification:	Public
Document Ref.:	ECMWF-InfoSec-A05-04-PO
Issue:	1.0
Date:	26/02/2020
Document Author:	InfoSec Team
Document Owner:	Information Security Officer
Document Status:	Final

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

Approval

Name	Position	Date
Martin Palkovic	Director of Computing	

Distribution

Name	Department
Public	N/A

Relevant Documentation

Document Reference	Document Title	Issue
ECMWF-InfoSec-PO-A05-01	ECMWF Information Security Policy	2.0

Contents

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 document 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.

3 Scope

This policy applies to external users and third parties that have a user account used for access to any web services provided by ECMWF or in any cloud services accessed for the purposes of ECMWF's business.

4 Password Management Policy

4.1 Password Creation

- All web access passwords must conform to the Annex A - Password Construction Guideline defined in Annex A - Password Construction Guideline.
- Always use different passwords for ECMWF web accounts from other non-ECMWF accounts (e.g. personal ISP account, personal email accounts etc.).

4.2 Password Change

- Web access passwords must be
  - changed every six months.
  - different from all the previous ten 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 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.
- Passwords must not be stored on-line or in a file on a computer system or mobile devices (phone, tablet) without adequate encryption.
- "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.
- If an account compromise is suspected, the incident must be reported as soon as possible to ECMWF's Servicedesk.
- The use of a password management tool is strongly recommended.

5 Compliance

5.1 Enforcement

Password cracking or guessing may be performed during security assessment activities 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 user will be informed to change the password to be compliant with the Password Construction Guideline defined in Annex A.

6 Policy Review

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

7 Annex A - Password Construction Guideline

All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:

- Contain at least 8 alphanumeric characters.
- Contain at least 1 character of each of the four following classes:
    - 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 8 characters.
- Can be found in a dictionary, including foreign language, 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 version of “Welcome123” “Password123” “Changeme123”