PASSWORD MANAGEMENT POLICY

Approval
Date: **03/11/2021**
ASI Manager: **Dr Francesca Pruneti**
Digitally signed pursuant to Legislative Decree No. 82/2005

About the document		
Edited by: *O.U. IT Security*	**Target audience:** *Anyone who has to use credentials or implement authentication systems for the University's services of Parma*	**Document deposit:***www.unipr.it/regolamento- security-EN*

Automatically translated by DeepL

Summary

1. Purpose of the document

The purpose of this document is to define a policy for understanding the criteria and precautions needed to create and manage passwords that cannot be easily obtained by a third party or programmes designed to force credentials.

2. Scope of application

This policy applies both to users who must use the credentials assigned to them to access tools and services that process University of Parma data, and to those who must implement and manage authentication systems (federated or not) in the University,

3. Password composition and management rules

Type of rule	Content rule
Mandatory	The password must contain at least 8 characters. The password must contain the following types of characters: • Lower case letters a to z; • Capital letters from A to Z; • Numbers 0 to 9; • Special characters (e.g. !, $, #, ^, %,*,etc.). The password must contain at least one number, one capital letter and one special character. The password must be changed within 90 days. The password must be different from the passwords used in the last year. The password must not be traceable to the identity of the account holder. The password must not contain more than two consecutive characters of the user name.
Mandatory	Passwords must not be shared with anyone, not even with administrative assistants, secretaries, colleagues and family members.
Mandatory	Passwords must not be included in e-mail messages or other forms of electronic communication together with the user's name or any other information relating to the service (e.g. access site).
Mandatory	Passwords must not be written down and stored anywhere within of the workplace.
Mandatory	Passwords must not be stored in a file a computer system or mobile devices (e.g. phone, tablet) without encryption.
Mandatory	The 'remember password' function of applications (e.g. web browsers) should not be used except with advanced management programmes that use strong encryption systems

Mandatory	Accounts with administrator privileges must have a different password standard accounts and must provide at least two-factor authentication.
Recommended	It is recommended **not to use the same password** as the federated University user (IDEM**) for other** non-federated or external **accounts.**
Recommended	It is recommended not to use passwords containing **personal information**, as they are easy to guess or discover (e.g. user's phone number, name, children's birthdays, anniversaries, etc.).
Recommended	It is recommended not to use words in common use, or contained in a dictionary, because they can be easily guessed.
Recommended	If it is suspected that a password is no longer secure or reliable, it must be changed immediately.
Recommended	Passwords must be blocked after 5 wrong attempts within 10 minutes. After 40 false entries within 24 hours, credentials can only be unlocked by contacting the operator (e.g. IT Help Desk).

Document Revisions

Ver.	Description of changes	Author	Date modification
1.0	*Initial version*	*O.U. IT Security*	*16/06/2021*