EUROPEAN
COMMISSION

Brussels, 22.3.2019
C(2019) 2345 final

IT technical standard

Password

CONTENTS

1. INTRODUCTION

This technical standard sets out requirements for the management of passwords. The aim is to strike a balance between user experience and the security of the Commission's information. Every setting contributes to that balance: failure to comply with one of the requirements would destabilise it and significantly increase the level of risk to which an account is exposed.

This standard provides for two parallel *modi operandi* that can be selected by the system owner:

- traditional password use and handling, allowing for systems to continue their existing password implementation and setup without any impact; and
- user-centric password use and handling, bringing forward a new approach in line with new best practices, standards and technology evolutions.

2. PURPOSE

This standard is a set of rules designed to enhance the security of the Commission's information systems by enhancing the user-friendly approach to authentication.

3. SCOPE

This document sets out minimum requirements applying to all applications and IT systems hosted on Commission premises. Some are mandatory and subject to compliance verification. Some are in the form of recommendations (i.e. guidance) based on market best practices, and not subject to compliance verification. These may become mandatory in future versions of this standard, in the light of customer feedback, further best practice and compliance analysis.

The blank field in the tables below means that the relating requirement is totally at the discretion of the system owner to implement it. Therefore this requirement will not be subject to compliance verification.

4. EXCEPTIONS

This standard is mandatory and an integral part of the Commission's information security policy. Exceptions must be handled in accordance with Article 8.3.d.iv of Commission Decision (EU, Euratom) 2017/8841 (Implementing Rules for Commission Decision (EU, Euratom) 2017/46[1]).

5. DEFINITIONS

For the purposes of this standard, in addition to the definitions in Article 2 of Decision (EU, Euratom) 2017/46 and Article 2 of Commission Decision (EU, Euratom) 2017/8841, the following definitions also apply:

TERM	DEFINITION
authenticator or authentication factor	A category of credential used for authenticating. There are three main authentication factors: – the knowledge factor – a category of credentials consisting of information that

[1] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

	the user knows, such as a personal identification number (PIN), a password or the answer to a secret question; – the possession factor – a category of credentials based on items that the user has with him/her, typically a secure hardware device such as a security token or a mobile phone used in conjunction with a software token; and – the inherence factor – a category of credentials consisting of elements that are integral to the individual in question, in the form of biometric data.
communication and information system (CIS)	A CIS is any system enabling the handling of information in electronic form, including all assets required for its operation, as well as infrastructure, organisation, personnel and information resources. This includes business applications, shared IT services, outsourced systems and end-user devices.
Commission's password blacklist	A list of passwords that cannot be used. The list is customised for the Commission and maintained by DIGIT.
IT system	The technical assets of a CIS, i.e. supporting information, hardware, software and/or a network, other digital information handling components or a combination of those, which may relate to one CIS or shared between multiple CISs.
password	A type of authenticator comprised of a character string intended to be memorised or memorable and permitting the user to demonstrate something they know as part of an authentication process.
password hygiene	The principles used to create a password that cannot easily be guessed.
password throttling	A feature that can block the end-user from making further password login attempts or lock the targeted account once the maximum number of invalid attempts has been reached within the set timespan. The feature uses a dynamic, rolling time period for managing the count password login attempts and adds a time delay between successive attempts.
privileged account	An account that holds system administration privileges and includes at least: Windows local and domain administration accounts, operating system and database administration accounts, and administration accounts for all system and network components.
service account	An account used by an automated service, not an individual user.
Single sign-on (SSO)	A session and user authentication service that permits a user to use one set of login credentials to access multiple applications. The service authenticates the end user for all the applications the user has been given rights to (e.g. EU Login).
user account	An account that has a single individual owner: if it has system privileges, it is a privileged account.

6. PASSWORD STANDARD

Password configuration must follow the principles below because:

- For the time being, password is the primary authenticator of a Commission user and must not be easy to guess; and
- if a password is compromised, the measures in place must prevent or severely limit the possibilities for unauthorised individuals to use it to access Commission systems.

6.1. General requirements

6.1.1. Password validation

(M=mandatory, R=recommended)

SN	Requirement	Traditional	User Centric
1.	Passwords **shall** be validated against a blacklist of unauthorised passwords based on the Commission's password blacklist. Validation **shall** be based on one of the following methods:	R	M
1.a.	– the blacklist check **shall** be performed as part of the immediate password validity control, i.e. whenever a password is created or modified; or, where this is not the case,	R	M
1.b.	– the blacklist check **shall** be performed offline (by comparing hashes) at least monthly. Where a password is not valid, users **shall** immediately be informed that it does not comply with policy requirements and **shall** be asked to update it immediately. The system **shall** force users with an invalid password to change their passwords at the next login request.	R	M
2.	The password blacklist **should** consist at least of:	R	R
2.a.	– every word in every official EU language (dictionary check);	R	R
2.b.	– typical first and last names in use in a Member State and in English;	R	R
2.c.	– passwords found in publicly available lists of breached passwords;	R	R
2.d.	– the username or the name of the IT system.	R	R
3.	DIGIT **shall** maintain the password blacklist and review it at least monthly. The check **shall** always be based on the latest version of the blacklist.	M	M
4.	DIGIT **shall** make the blacklist available to DGs that provide authentication services.	M	M
5.	When the blacklist cannot be applied, password validity control **shall** be enforced, ensuring that the system does not accept a new password if it is a single-word password and it is:	M	
5.a.	– composed of repetitive or sequential characters (e.g. 'aaaaaaaaaaa' or '1234567890');	M	
5.b.	– any common keyboard sequence — (e.g. qwerty);	M	
5.c.	– vulnerable to dictionary attacks (word included in dictionaries);	M	
5.d.	– identical to one of the last eight passwords used.	M	
6.	Where it is not technically possible to validate the password against the blacklist, the system **shall** ensure that passwords feature at least lower case, upper case and special characters, and at least one digit.	M	

6.1.2. Password length

(M=mandatory, R=recommended)

SN	Requirement	Traditional	User Centric
7.	The maximum password length **should** be 64 characters; passphrases are considered good practice.	R	R

8.	The minimum length **should** be reduced to eight characters if two-factor authentication and lock-out/throttling requirements are met.		R
9.	Where no second authenticator is required, passwords **shall** have at least 10 characters.	M	M
10.	For privileged accounts, where no second authenticator is required, passwords **shall** have at least 14 characters. Where password lengths for privileged and user accounts cannot be differentiated, the most stringent requirement **shall** take precedence for all accounts.	M	M

6.1.3. Failed login attempts

(M=mandatory, R=recommended)

SN	Requirement	Traditional	User Centric
11.	Password throttling **shall** apply at least to:		M
11.a.	– clients (e.g. Windows authentication for workstations)		M
11.b.	– web-facing systems.		M
12.	The password throttling mechanism **should** be configured so that a user is unable to enter a new password or to log in for three seconds after a first failed login attempt. This period should be doubled for each subsequent failed attempt.		R
13.	Password throttling **shall** enforce account lock-out after a maximum of 100 failed login attempts (consecutive or not) over 30 days.		M
14.	Where password throttling is not technically possible:	M	
14.a.	– the residual risk **shall** be documented in a risk acceptance form and fully approved;	M	
14.b.	– the system **shall** ensure that, after five failed log-in attempts, users cannot log in to the system for at least 20 minutes;	M	
14.c.	– where such lock-out mechanism is implemented, secure password self-reset functionality is recommended.	R	

6.1.4. Other configuration settings

(M=mandatory, R=recommended)

SN	Requirement	Traditional	User Centric
15.	Default passwords **shall** be modified on any system or device before it is connected to production networks. The new passwords **shall** comply with the requirements in this document.	M	M
16.	Password expiration in user accounts **should** be omitted if all other requirements (two-factor authentication, password throttling, and password blacklist validation) are properly implemented, unless there is evidence of compromise of the password.		R

7. PASSWORD LIFECYCLE MANAGEMENT

Password lifecycle management must follow the principles below because:

- users should be able to manage their password securely at any time if other individuals have, or may have, found out what it is.

7.1. General requirements

(M=mandatory, R=recommended)

SN	Requirement	Traditional	User Centric
17.	Users **shall** be able to set or update their password autonomously at any time, assuming that password history and password throttling are enforced.		M
18.	Initial passwords:	M	M
18.a.	– **shall** be pre-expired: on first log-in, the user **shall** be forced to define a new password;	M	M
18.b.	– **shall** be communicated in a secure way;	M	M
18.c.	– **shall** have limited time validity, e.g. expire after five business days.	M	M
19.	Users should be able to reset their passwords autonomously. This **shall** be the case at least for Windows workstation and single sign-on authentication.		M
20.	Knowledge-based authentication or password hints **shall not** be used.		M
21.	The autonomous password reset processes **shall** verify the identity of the user prior to initiating the password reset request.		M
22.	Privileged accounts: passwords **shall** be modified after each use or a maximum of 90 days. Where passwords are not automatically rotated after each use, detailed auditing **shall** be implemented; the logs **shall** be reviewed every 90 days or more frequently, depending on the level of risk evaluated by the system owner.	M	M

8. SELECTING AND STORING PASSWORDS

The selection and storage of passwords must follow the principles below because:

- users are encouraged to set a separate, secure password for every IT system in order to limit the impact of password loss; preferably, they should be offered secure authentication mechanisms common to several IT systems; and
- users should not be expected to remember every password and should be provided with tools that enable them to manage authentication in a user-friendly way (e.g. password vault tool).

8.1. General requirements

(M=mandatory, R=recommended)

SN	Requirement	Traditional	User Centric
23.	DIGIT **shall** maintain and offer to all users a Commission-supported password vault tool enabling the secure storage of passwords and the generation of		M

	strong passwords.		
24.	For IT systems that do not use single sign-on as a means of user authentication, users **shall** not re-use an identical password on different production and non-production environments and IT systems, whether internal or external. Instead, they **shall** create individual passwords for each system and environment.	M	M
25.	For their convenience, users **should** store passwords in the Commission-supported password vault, with the exception of their Windows account password.		R
26.	Only password vaults that meet the following requirements **shall** be used:		M
26.a.	– data **shall** be encrypted and encryption mechanisms **shall** meet the Commission's requirements;		M
26.b.	– the security of the password vault **shall** be tested or assurance on its security obtained from a trusted and reputable source;		M
26.c.	– they **shall** not be the web browser's integrated password vault.		M
27.	DIGIT **shall** maintain and offer a privileged access management tool that supports:		M
27.a.	– password vaulting, i.e. secure centralised storage of credentials;		M
27.b.	– scheduled and automated password rotation;		M
27.c.	– features to limit access on the basis of other parameters (e.g. on/off working hours);		M
27.d.	– detailed auditing, covering at least which individual users accessed which privileged or shared accounts, when and for what purpose.		M
28.	Privileged account passwords **should** be managed in a privileged access management tool; account holders should never have to remember or read the account password.		R
29.	DIGIT **shall** regularly conduct activities to raise users' awareness of the importance of password hygiene and the principles set out in this document.	M	M
30.	For IT systems that do not use single sign-on as a means of user authentication, system owners **shall** include, in the system user guidance and documentation, recommendations to use a password vault to store passwords securely.	M	M

SUMMARY OF DIFFERENCES BETWEEN ACCOUNT TYPES

The following table summarises the different requirements of normal and privileged accounts:

Section, Topic	User account	Privileged account
1. Password configuration *Password length where no second authenticator is required*	Passwords **shall** have at least 10 characters.	Passwords **shall** have at least 14 characters. Where password lengths for privileged and normal user accounts cannot be differentiated, the most stringent requirement **shall** take precedence for all accounts.
2. Password lifecycle management *Password expiry*	Password expiration in user accounts **should** be omitted if all other requirements (two-factor authentication, password throttling, and password blacklist validation) are properly implemented, unless there is evidence of compromise of the password.	Passwords **shall** be modified after each use or a maximum of 90 days. Where passwords are not automatically rotated after each use, detailed auditing **shall** be implemented; the logs **shall** be reviewed every 90 days or more frequently, depending on the level of risk evaluated by the system owner.
3. Password definition and storage *Password vaulting*	For their convenience, users should store passwords (other than their Windows password) in the Commission-supported password vault.	Passwords **should** be managed in a password vault; account holders should never have to remember or read the account password.

REFERENCES

NIST 800-63 draft
https://pages.nist.gov/800-63-3/

SANS password guidelines, 2014
https://www.sans.org/reading-room/whitepapers/bestprac/password-management-applications-practices-36755

SANS password policy, 2014
https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

OWASP authentication cheat sheet
https://www.owasp.org/index.php/Authentication_Cheat_Sheet

OWASP session management cheat sheet
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

OWASP application security recommendations
https://www.owasp.org/index.php/OWASP_Application_Security_FAQ#Browser_Cache

OWASP password storage cheat sheet
https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

CIS 20 critical security controls
https://www.cisecurity.org/controls/

Tel. +32 22 991 111 Office: B-28 03/09 — Tel. direct line +32 229-56 867

ken.ducatel@ec.europa.eu