EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

Brussels, 23/06/2011
HR.DS5/GV/ac ARES (2011) 675291
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON ACCESS CONTROL AND AUTHENTICATION

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 23/06/2011

Version 16/06/2011

TABLE OF CONTENTS

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. INTRODUCTION

Access control mechanisms are the hardware, software or firmware features and operating and management procedures in various combinations designed to detect and prevent unauthorised access and to permit authorised access to information systems, ensuring their confidentiality, integrity and availability.

After a first section defining the general rules for the access control management, this document provides a description of the security measures related to the policy objectives of the Implementing Rules of Commission Decision C(2006)3602 related to each step of the complete user access management process.

User access management starts with user registration, which is a clear set of procedures to associate UserIDs with a user, and continues with the management of associated UserIDs within information systems. When a user tries to access an information system, the process continues with the identification and authentication phases.

This document also describes how user access rights and privileges must be managed, from definition, approval and creation to deletion and the responsibilities of all parties involved in all steps of access control management.

In addition, this document describes the security controls for the authentication of users, including the associated management rules and processes.

3. OBJECTIVES

To establish general access control principles and user access control management rules by fixing baselines for registration, identification and authentication of users and management of access rights in order to:

– Ensure that only authorised users gain access to information systems, operating systems and applications, and that individual accountability is assured.

– Ensure that authentication information is processed, transferred and managed in a secure manner.

4. SCOPE

The security measures described in this security standard apply directly to all the Commission information systems storing or processing information.

This includes systems and applications used and accessed by internal users as well as systems and applications that are accessible by externals such as member states, agencies and external contractors.

The standard covers the complete user rights and privileges life cycle management process and the responsibilities of all relevant parties (requesters for access rights, users, system owners, system managers etc.)

This standard does not cover access control at network level, which is covered in the Standard on Network Security, which is in line with the requirements of this standard.

This standard does not cover physical access control.

5. IMPORTANT DEFINITIONS

User –a general term for any person who has authorised access to and uses the Commission information systems[1]; it is used for the following categories of individuals: an official or other servant of the Communities, a person under contract with the Commission, a subcontractor, a person from another EU body, a self-registered person, a representative of a Member State administration, or another person with close relationship with the Commission not covered by other categories (e.g. partners of staff members).

Account – a record about a specific user, token or computer known by the information system; it contains information about the subject important for the information system.

[1] As a general rule, anybody who is identified to the system (i.e. registers or logs in) is counted as a User for the purposes of this standard. Anonymous users, such as citizens viewing web pages on Commission web sites without logging in, are not included since they do not authenticate and do not have individual access rights.

UserID – user identifier, a character string used as a unique name for an account; it represents the account to the user and identifies the user or token to the system.

Registration – process through which a user applies to obtain an account from a Credential Service Provider; a Registration Authority validates the identity of that user on behalf of the Credential Service Provider.

De-registration – process through which a user is removed from information system registrant status.

Identification – process through which the identity of a user is recognised by an information system. The identification process requires the user to enter a unique user identifier (UserID).

Authentication – the process of verifying the claimed identity of a user; authentication systems are often categorised by the number of factors that they incorporate for the verification; the three factors usually considered in the authentication process are:

- What a user knows (a secret), such as a password, a Personal Identification Number (PIN), or an item of personal information.
- What a user possesses, such as a token. Examples of tokens include swipe cards, smart cards, mechanical and electronic keys.
- What a user is (a biometric), such as a fingerprint, a retina pattern, a voice pattern or a behaviour pattern.

Authorisation –phase during access when it is verified that the requested access to the information system resources is allowed for the requester (requesting user).

Biometrics – personal attributes that can be used to either identify or authenticate a person; they include facial pictures, fingerprints, DNA, iris and retina scans, voiceprints etc.

Token –something the user possesses and controls that may be used to authenticate the user's identity.

Password – a secret that is associated to a user and that this user can use to authenticate his or her identity; passwords are typically character strings.

PIN (Personal Identification Number) – a password consisting only of decimal digits.

Registration Authority – a trusted entity that establishes and vouches for the identity of a user or subscriber to a Credentials Service Provider.

Credentials Service Provider – a trusted entity that issues or registers subscriber or user tokens and issues electronic credentials to subscribers and users.

Credentials – data that are used as part of the authentication process to establish the claimed identity of a user or entity; they are attributes (permanent or temporary) that are associated to an existing account and used for identification and authentication;

typically a UserID and a Password, in the simplest form of a single factor authentication scheme.

Role – a job type defined as a set of responsibilities.

Role-based – when mapped to job function, assumes that a person will take on different roles, over time, within an organisation and different responsibilities in relation to information systems.

Requester – an individual or organisation that requests to be granted access to Commission information systems.

Right – a permission set in the system allowing its holder a certain usage of internal resources of the information system, e.g. to access a part of a file system or a function in the system or to perform a specific action.

Privilege – any supervisor or administrator right which allows setting, changing or deleting (important) parameters of an information system and/or access rights.

Abuse of user rights – deliberately exploiting rightfully-obtained rights in order to harm a system or its users.

Abuse of privileges – deliberately misusing rightfully-acquired privileges to harm the system or its users.

Usurpation of rights – illicitly obtaining user rights or privileges on an information system.

Accountability – property that ensures that the actions of an individual or entity can be traced uniquely to the individual or entity.

Profiles – the organisation of the logical access control is built on the following assumptions:

- Each individual can be uniquely identified by means of a personal and individual UserID (mapping 1 to 1).
- Each individual may have access to one or more information systems and within each information system an individual is uniquely identified by means of a UserID (mapping 1 to n).
- Each information system is composed of a number of rights or access authorisations which are grouped together into standard profiles (mapping 1 to k) which can correspond to roles.

Standard profile – a standard profile is composed of a predefined set of access authorisations of an information system. Before an information system becomes operational, the System Owner is accountable for reviewing the rights available and groups them into standard profiles. Standard profiles are defined because they facilitate the administrative work during the approval of authorisation requests. Standard profiles are further categorised as "normal" (or "non-privileged") and "privileged".

6. GENERAL REQUIREMENTS ON ACCESS CONTROL

The rules in this section constitute general rules in the area of access control. Compliance with them is mandatory and their specification for different areas of access control is repeated and/or detailed in the following sections that have the same structure as section 6 of Annex 1 of the Implementing Rules.

General principles:

(1) To ensure the confidentiality, integrity and availability of the European Commission data, all System Owners are accountable for the development and implementation of user access management procedures and processes for their own information system(s).

(2) Access authorisations must be implemented on the basis of the "need-to-know" principle: users must only be provided with minimum access and functionality needed to perform their tasks.

(3) Privileges may only be given to users when really justified.

(4) Access authorisations must only be given to individuals. In exceptional situations access authorisation may be given to group or functional UserIDs; in these situations a business justification is filed together with the access request, and accountability will remain with an individual.

(5) No single person must be allowed to approve access requests for himself (except in the context of systems permitting self-registration; see section 7 below).

Organisational principles:

(6) The organisational functions responsible for the approval of the access requests and the implementation of these requests must be segregated (these functions may not be performed by the same persons).

(7) Segregation of duties must be implemented between user profiles at application, operating system and network device levels, and between "system administration" and "application administration" profiles.

Process principles:

(8) Access authorisations must only be implemented on the basis of formal access request.

(9) Every change in the access control administration must be logged (auditability).

(10) Users' rights and privileges must be revoked immediately after they are not authorised or needed any more.

(11) In case of job transfer the implemented access authorisations must be adjusted accordingly.

(12) Logging of access attempts is mandatory to guarantee the auditability of the access control system and allow for proper follow up in case of (un)intended system misuse. The logging will at a minimum comprise:

- Invalid login attempts.
- Access (attempted) to sensitive data and systems.
- Access to data and systems by privileged users (users with privileged profiles).
- Access rights modifications.

See the Standard on Logging and Monitoring for more details.

(13) The use of utilities and systems that require privileges outside the normal profiles must be explicitly logged.

(14) Implemented access authorisations need to be reviewed periodically, whereby:

- The system owner receives and reviews an overview of all implemented access authorisations of the information systems (and functions) under his responsibility.
- The line management receives and reviews an overview of all implemented access authorisations for users under his responsibility.

System owner responsibilities:

(15) The system owner ss accountable for the access authorisations of all information systems for which he has been assigned the system owner.

(16) The system owner is accountable for the explicit authorisations to ensure that the information systems under his control are used for the purpose they were designed and built for. However, he may delegate the actual authorisations to the IT service provider or the system manager.

System manager responsibilities (either directly or indirectly by subcontracting to an IT Service provider with agreed SLAs as described in the Decision (2006) 3602):

(17) Ensures that access authorisations needed by users are adequately approved

(18) Keeps a file of all standard profiles (normal and privileged access rights) for each information system under his administrative responsibility.

(19) Only administers access authorisations, based on approved and authenticated access requests.

(20) Keeps a file of all access requests (auditability).

(21) Ensures that access control procedures are monitored and enforced.

(22) Ensures that monitoring reports are produced, analyses these reports and forwards the results to the responsible system owner.

(23) Is responsible for the correct and timely implementation of the approved and administered authorisation request into the access control function of the information system

(24) Only implements access authorisations, based on approved and authenticated access requests.

(25) Is responsible for timely informing the user when an access request has been implemented (i.e. the functions are now available to the user).

User responsibilities:

(26) Users must not reveal their authentication mechanisms or share them with other persons.

(27) Users are accountable for the use of the personal UserID(s) and the secrecy of the access credentials.

(28) Users must refrain from abuse of user rights, abuse of privileges and usurpation of rights.

7. USER REGISTRATION AND ACCESS MANAGEMENT

Policy objective 6.1.1 – There must be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. Exceptions can be granted for systems and services dedicated to public access.

7.1. Risks

The controls described in this standard will reduce the level of the following threats that are described in the Standard on Risk Management:

Threat identification	Impacted security needs
T23 – Disclosure	C
T26 – Tampering with Software	C, I, A
T33 – Unauthorised use of equipment	C, I, A
T34 – Fraudulent copying of software	C
T36 – Data corruption	C,I
T39 – Abuse of rights	C,I,A

7.2. Requester registration and registration authority.

(29) With the exception of allowed self-registration (bullet point (c) below), all requesters, either individuals or organisations (third-parties), who want to access European Commission information systems or applications must be formally registered with the registration authority that is entitled by the EC to vouch for their identities, as follows:

(a) European Commission staff and personnel must be registered with the HR part of the Directorate-General Human Resources and Security, which is accountable for encoding their user information, including their contractual details between the European Commission and the user.

(b) Third-party users such as Member states, agencies, or Contractor Organisations must be registered with the System Owner of the system they want to access (and subsequently the individuals belonging to them: see next requirement). The latter is responsible for encoding their information[2].

(c) Exceptions to the formal registration to a registration authority may be granted in order to allow users to register themselves to a particular system. In this case, the self-registration facility must be documented and justified in the Security Plan, and the access rights permitted to self-registered users described in detail. The data that

[2] Including the security conventions between them and the European Commission but this the subject of the standard on network security.

may be accessed by self-registered users must be restricted (e.g. to EC information classified as PUBLIC or to data provided by the users themselves).

(30) Organisations (or third-parties) must be registered before the individuals belonging to them.

(31) During the registration process every requester must undergo identity proofing[3]. This verification must be documented.

(32) The registration may only be considered as successful and complete after successful identity verification, allowing then the registration authority to vouch for the identity of the requester during the access authorisation processes (see next section).

7.3. Access request and credentials service provider

(33) On behalf of the system owner a credentials service provider must establish access request mechanisms and procedures to uniquely identify each requester to access its information system, create an account and issue credentials and/or tokens. The system manager, an IT service provider or a corporate entity (e.g. DIGIT UAA, ECAS …) may be identified as the credentials service provider on behalf of the system owner. In case of self-registered users, these mechanisms may rely on automated means.

(34) These access request mechanisms and procedures must be designed to fit the requirements of the system owners in terms of responsibilities from generation of the access request to the authorisation of access/generation of credentials, i.e. identification of who (or what in case of allowed automation) is responsible for:

(a) Generating the access request

(b) Performing the verifications described below.

(c) Implementing the account (data entry) and generating the credentials.

(d) Approving the request after the verifications.

(35) The name of the requester must first be verified with the registration authority entitled to vouch for his/her identity before creating the account and issuing credentials or tokens.

(36) A unique UserID must be associated to the requester (and his/her account) to ensure a unique link between him/her and its future actions in order to provide accountability (see section "Identification: account and UserID").

[3] The method and process of identity verification and proofing are out of scope of this standard, but they must be designed to get the level of assurance required by the registration authority in accordance with the classification level of the information system and information to be accessed.

(37) The use of group IDs[4] is generally forbidden unless they are necessary for business or operational reasons, in which case their usage must be formally approved.

(38) Access rights must only be granted based on standard role-based profiles as defined under the accountability of the system owner; non-usage of those profiles must be formally authorised and documented:

(a) The account of the requester is created with the rights corresponding to the standard role-based profile(s) defined for his/her role under the accountability of the system owner.

(b) The standard role-based profiles must be implemented for each information system based on organisational responsibilities, the classification level of the resources to be accessed, types of users/roles and the types of information:

– Organisational responsibilities – different DGs or services.

– Classification – required levels of confidentiality, integrity, and availability (see also the Standard on Asset Management).

– Users/roles – public, users (e.g. EC DG/service staff, agency staff, delegation staff, consultants, contractors), VIP users, internal /external developers, internal/external support staff, internal/external administrators, system/application services.

– Types of information – live production information (data), production information backup, application software and its configuration, middleware software and its configuration, operating system software and its configuration, network configuration, documentation.

(c) The standard profiles must be implemented based on the segregation of duties principle:

– The system owner must identify any incompatible information system functions, which, when accumulated to one person, imply a business risk (lack of segregation of duties).

– Incompatible functions must not be accessible by a single person (see organisational principles in section 6).

(39) After account or access creation or change, the requester must be provided with confirmation/acknowledgment of the list of granted access rights, implying that he/she understands them and his/her related responsibilities[5].

---

[4] UserID granted to a group of people.

[5] Reminding obligations resulting from Informations System Security Policy and Non-Disclosure Agreement.

(40) The access must not be granted to a requester before the authorisation procedure has been completed.

(41) A register must be created and maintained by the system manager[6] which contains the list of all users requesting or having access to the information system with at least the following information: evidence on every user access request, decision about it and its actual implementation (access rights, roles profiles), any change of these access rights, including withdrawal, with reasons.

(42) For any change of an account, existing rights or privileges, the procedure described in this section must also be followed, i.e. using the same user access request procedures and steps.

(43) Users' access rights and privileges granted must be securely administered, i.e. only authorised personnel may view, add or delete those rights and privileges (security administration function).

7.4. User access termination

(44) A user's rights and privileges must be revoked immediately after they are no longer authorised or needed.

(45) The user's account must be disabled and their access rights and privileges must be revoked, either immediately upon receipt of the notification about the user's termination of employment, or on the expected day of termination.

(46) The user's registration records (e.g. identity, status and contract) must be updated.

(47) After termination of a user's employment, contract or agreement, his/her UserID must not be granted to another user.

8. PRIVILEGES MANAGEMENT

Policy objective 6.1.2 – The allocation and use of privileges must be restricted and controlled.

(48) Special controls must be applied to role-based profiles with special privileges and high-privileged accounts (e.g. root, administrator, database administration accounts), and to access rights for powerful utilities.

(49) The purpose of privileged role-based profiles and accounts must be specified and authorised, access to them must be limited, and their use restricted to situations defined in the security plan in accordance with the following rules and controls:

---

[6] As indicated in Decision (2006)3602 the system manager can subcontract his duties to an IT service provider. This is true each time the system manager is referred to in this standard.

(a) Definition of standard privileged profiles based on the user profiles and system resources; the use of default/generic (non-nominative) account such as administrator or root and shared accounts is not permitted. In exceptional situations the use of such default/generic accounts can be allowed if no alternative is available; in these situations, a business justification must be filed together with the access request, and accountability will remain with an individual to whom the account is explicitly assigned.

(b) Granting of privileges based on these standard profiles whenever possible.

(c) A formal authorisation and revocation process for all privileges based on the principle of "need to use" (see below).

(d) Segregation between system and application administrators, and more generally a definition of incompatible profiles that must be segregated.

(e) Definition of the skills and competence required for each privilege.

(f) Only granting the minimum number of privileges that are necessary to ensure operations.

(50) At least the following rights must be considered as privileges and managed as defined in this section, but others may be added in the Security Plan as indicated above if decided by the system owner:

(a) System administrator rights for servers, desktops, laptops, firewalls, routers, PABX and PDAs.

(b) Administrator rights for mail systems, encryption tools, backup systems, databases, user administration and applications.

(c) Rights for installation of hardware and software.

(51) A formal user registration and de-registration procedure must be implemented by the system manager[7] with the help of their LISO for granting and revoking privilege accesses to all information systems and services, in line with following rules.

(a) Any user access request for privileged role-based profiles and accounts must be first authorised by the user's unit management and then forwarded to the system manager on behalf of the system owner for approval. It must contain:

– Rights and duties of the function for which a privilege is requested.

[7] As indicated in Decision (2006)3602 the system manager can subcontract his duties to an IT service provider.

– Name, employer, administrative unit.

– Type of privilege requested and related justification.

– Start and end dates (maximum period of 12 months).

– A notice as requested by Regulation (EC) 45/2001 on protection of personal data.

(b) Before approving and granting the privileged access, the following verifications must be carried out by the system manager with the help of the LISO:

– The requester is competent to use the requested privileges.

– The requester has a "need-to-use" and the principle of "segregation of duties" has been respected.

– For external staff, the end date of privileged access must not beyond the end date of his/her contract with the Commission.

– The requester has been given account management instructions, documentation and training on how to use the privileges, implying that he understands and accepts the privileged rights and related responsibilities.

(c) The privileges must be revoked at the end date of the authorisation or at the end date of the "need to use".

(52) As for non-privileged access, a register must be created and maintained by the system manager. This register will be submitted to the Security Directorate upon request.

(53) The system manager and their LISO must, at regular intervals, review the privileged accesses and accounts using a formal process.

(54) The credentials which are needed for a privileged access must not be shared with others.

(55) In case a user's role or employment position changes and requires a change of access to privileged role-based profiles or accounts:

(a) The change may only be done based on a properly authorised user access request, as described in this section.

(b) Any change of accesses to privileged role-based profiles and accounts must be registered in the dedicated register, with full details.

(c) The user must be given confirmation of the change.

9. IDENTIFICATION AND AUTHENTICATION MANAGEMENT

Policy objective 6.1.3 – The allocation and use of adequate access credentials (e.g. password) must be controlled through a formal management process.

9.1. Identification: account and UserID

(56) A user may be assigned one or more accounts in accordance with the rules described in the following points.

(57) For identification of a user's access to an account of an information system the user must use the identifier (UserID).

(58) Users may be provided with one or more accounts that must be distinguished through their unique UserIDs.

(59) Each account may only be used for the access of one user.

(60) For administrator or privileged access to Commission information systems the administrators/operators must use one or more unique accounts that are different from their standard (non-privileged) user accounts.

(61) The UserID of an account providing administrator or privileged access to an information system must be easily distinguishable from a UserID of an account providing standard user (non-privileged) access.

9.2. Authentication system: general requirements.

(62) The identity claimed by a user (UserID) must be verified by an authentication system that is based on one or more factors, i.e. "what the user knows", "what the user possesses" or "what the user is", in accordance with the classification level of the information system.

(63) Access to systems classified as STANDARD with information assessed as LIMITED BASIC must be controlled with an authentication system that is at least based on a "what the user know" factor (such as passwords) in accordance with the rules described in section 9.3."

(64) Access to systems classified as STANDARD with information assessed as PUBLIC can be controlled with an authentication system that is based on passwords ("what the user know" factor) in accordance with the rules described in section 9.3 but it is not mandatory.

(65) Access to systems classified as SPECIFIC must be associated with an authentication system that has to be defined after a risk assessment: number and type of authentication factors, and the types of authentication to be used.[8]

[8] Recommendations are described in the Guidelines on Access Control and Authentication.

9.3. Rules applicable to authentication systems based on password (LIMITED BASIC)

9.3.1. General rules

(66) The management of user password, from access creation to termination, must be done at two levels:

(a) First at the user level: the user responsibilities concerning the usage of passwords are defined in section 10.2 on password use.

(b) Computer processing level: the management of user password for information systems must exhibit some automatic enforcement features that are collectively called the user password management system. The features that need to be automated and enforced are specifically described in section 12.2 on the user password management system.

9.3.2. Creation phase

(67) The usage of a newly created account must be protected with an initial temporary password, which can be generated automatically or can be chosen as long as this initial password is unique and complies with the requirements for password quality, which are enforced by an automatic process (see section 12.2).[9]

(68) The initial password must be communicated to the user in a secure manner to prevent it from being read or modified by unauthorised persons.

(69) The initial password must be changed by the user during the first logon.

9.3.3. Operation phase

(70) Every change of password done by the user, initially or at any time, must comply with the standard requirements for password quality.

(71) No vendor-provided default passwords may be used. Any such default password must be changed immediately at the time of installation of the software/device in line with the requirements for password quality.

(72) In case the local or central service desk is requested to reset/change a password by the user, only a temporary password may be generated in line with the rules for initial password. However the user must first be authenticated by the service desk using a special procedure[10].

(73) In case of the absence of a user having exclusive access to a function or set of data, nobody else is authorised to request for, or change the user's

[9] Additional recommendations for password quality are described in the Guidelines on Access Control and Authentication.

[10] See the Guidelines on Access Control and Authentication for examples of such procedures.

password. This problem may only be solved using the formal user management process described at the beginning of section 7. However, an emergency procedure must be defined in case there is an urgent need to access a function or a set of data in case of absence of the user or administrator that has exclusive access to it (e.g. in case of illness). The activation of this emergency procedure, which can be based on envelope passwords in a safe, for example, must be approved by the system owner or his delegate.

9.3.4. Termination phase

(74) In case of employment termination or position change of a user that has exclusive access to a function or set of data, nobody else is authorised to request for, or change this user's password. This problem may only be solved using the formal user management process described at the beginning of section 7. However, an emergency procedure has to be defined as above in case there is an urgent need to access a function or a set of data in the cases referred to above. The activation of this emergency procedure must be approved by the system owner or his delegate.

(75) In case of employment termination or position change of a user with access to a shared account, the password for that account must be changed and only communicated to the remaining users of that shared account.

10. USER OBLIGATIONS

10.1. Account use

(76) Privileged user accounts must not be used for day-to-day user operations (production application access, e-mail usage, web browsing etc.). For such non-privileged user activities the standard and non-privileged accounts must be used.

(77) Each user of Administrative/Special access must refrain from abuse of these privileges: abuse of privileges or usurpation of privilege rights is a violation of the security policy and must be reported as a security incident.

10.2. Password use

(78) The rules about password use described in this section are valid for all information systems and must be complied with by the user (some parts are enforced by an automatic process as described in section 12.2).

(79) Passwords must be kept confidential. Passwords for individual accounts must not be disclosed or given to other person in any circumstances

(80) The passwords must not be written down or recorded unless the record could be stored securely, preferably by an approved method or tool.

(81) Users must avoid using the same passwords for working and non-working purposes.

(82) Users must choose quality passwords.

(83) The passwords must be changed regularly in accordance with the policy approved by the system owner for the information system.

(84) Users must avoid re-using or re-cycling old passwords.

(85) Passwords must not be included in any automated logon process, e.g. stored in macros, script files or function keys.

(86) In case the user has forgotten his/her password or has other problems with access rights, the user must contact the service or help desk.

(87) Users must immediately contact the service or help desk and/or the LISO whenever there is an indication of a system or password compromise.

10.3. Unattended user equipment

(88) During temporary absence at their workplace users must log off the PCs/terminals or activate the password-protected screen saver.

(89) After finishing their work users must close their active sessions and log off the PCs/terminals.

(90) Any exceptions to these rules may only be approved by the System Owner and must be properly documented.

11. REVIEW OF ACCESS RIGHTS

Policy objective 6.1.4 – Users' access rights must be reviewed at regular intervals (e.g. internal change in job or duties)

(91) Every user's access rights must be reviewed at least once a year using a formal process.

(92) Privileged accounts and privileged role-based profiles must be reviewed at least every six months using a formal process.

(93) A user's access rights and privileges must be checked after any change of the user's status (e.g. promotion, demotion, transfer or termination) as follows:

(a) Check that rights and privileges remain appropriate.

(b) Check that obsolete and invalid ones have been deleted.

(c) Check that redundant or apparently unused UserIDs have been disabled or removed.

(94) In case of differences between authorised and actual rights and privileges, the excessive access rights and privileges must be disabled immediately and the user, the user's line manager (or contracting party for external users) and LISO must be informed of the changes.

(95) Access rights for users who have changed roles or positions or left the European Commission must be immediately changed or removed.

12. OPERATING SYSTEM ACCESS CONTROL

Policy objective 6.3.1 – Access to the operating system must be restricted to persons with a need to use it in accordance with a defined access control policy.

12.1. Secure logon procedures

(96) The logon procedure must be designed, implemented and configured to prevent unauthorised access and to disclose the minimum of information about the system before the user logs in. A secure logon procedure must comply with the following requirements:

(a) It must inform the user about the date and time of the previous successful logon.

(b) During the logon procedure the information system must display a notice warning that the information system may only be accessed by authorised users.

(c) It must only offer limited help messages about the procedure such that they would not aid unauthorised users.

(d) The information entered by a user during a logon attempt may only be validated as a complete set. If an error occurs the system must not give any indication on which part of the information is correct or incorrect (UserID or password etc.).

(e) It must limit the number of unsuccessful logon attempts during specified time intervals. The limit and the time intervals must be configurable:

– For STANDARD information systems with LIMITED BASIC information the number of unsuccessful logon attempts must be limited to 5; after reaching 5 unsuccessful attempts further logon attempts must be rejected during the next time interval of 15 minutes by default; after this time interval of 15 minutes with no new attempt the counter must be reset and new logon attempts may be made.

– For SPECIFIC information systems these limits will be determined after risk assessment.

(f) It must be able to record successful and unsuccessful attempts and generate an alarm when the maximum number of unsuccessful attempts is reached.

(g) It must not display the credential (e.g. password) keyed in by a user and this credential must not be transmitted in the clear over a network.

12.2. User credentials management system

The management of user passwords for information systems must exhibit some automatic and enforcement features that are collectively named a user password management system, or just subsystem in this section.

(97) First of all any credentials management system must use the official Commission user authentication services (e.g. Active Directory, ECAS, CED, etc) unless it is not possible and this non-compliance is fully justified.

(98) The credentials management system must allow users to select, change and maintain their passwords themselves. Any change of password must be based on proper authentication of the user (providing previous password) and must prevent any disclosure of the passwords during the operation.

(99) The choice of quality passwords and their secure usage by users must be enforced by the credentials management system, which must support the following functionality, including for initial passwords where relevant:

(a) After entering a new password, the user must be invited by the subsystem to confirm the new password by entering it a second time.

(b) The subsystem must check the length and the character set of the newly entered password and, in case of non-compliance with the conditions, it must refuse the new password.

(c) The subsystem must enforce the password lifetime.

(d) The subsystem must force users to change their initial temporary password at their first logon.

(e) Shortly before password expiration the subsystem must notify the user of the remaining period of time before the password expiration and encourage the user to change it in the meantime.

(f) After password expiration the subsystem must force the user to change it.

(g) The subsystem must maintain a history of the previous user passwords and must prevent their re-use.

(h) The parameters for maximum password lifetime, their quality or structure and history must be configurable depending on the system classification, as described under the specific standard statements below.

(i) The passwords must be stored separately from application data.

(100) To prevent their disclosure or unauthorised change, the passwords must be stored, either locally or centrally (e.g. in directory services) in hashed form and may only be accessible by the authorised and specific authentication service.

(101) Passwords transmitted through a network must be protected from being read, changed or replayed by any unauthorised persons, including system managers and IT service providers.

Specific standard statements

(102) For any information system classified as STANDARD with confidentiality level LIMITED BASIC (i.e. not PUBLIC), the password management system must enforce the following parameters for password structure, lifetime and history:

(a) A password must not contain the UserID string.

(b) A password must contain characters from 3 of the 4 following character sets – lower case letters, upper case letters, numbers, and non-alphanumeric characters.

(c) A password must have at least 10 characters.

(d) The maximum password lifetime is 180 days and its minimum is 1 day.

(e) The password management system must store the history of the last 5 passwords.

(103) The password management system for general Internet access must enforce the following parameters:

(a) A password must contain lower case letters, upper case letters and numbers.

(b) A password can contain non-alphanumeric characters.

(c) A password must have at least 6 characters.

(d) The password lifetime may be unlimited and the password management system doest not need to save its history.

12.3. Session time-out

(104) After a configurable period of user inactivity at the local desktop, the password-protected screen saver must be activated: for information systems classified as STANDARD the maximum period for screen saver activation must be 10 minutes.

(105) After a configurable period of user inactivity in an open session to the information system or application the session must be disconnected and the user must authenticate again for a new connection: for information systems classified as STANDARD the maximum period for session disconnection must be 30 minutes.

12.4. Use of system utilities

Policy objective 6.3.2 – The use of system utilities[11] that might be capable of overriding system and application controls must be restricted and tightly controlled. There must be procedures in place to control the installation of software on operational systems.

(106) The requirements in the section on privilege managements are applicable to this section.

13. APPLICATION AND INFORMATION ACCESS CONTROL

13.1. Information access restrictions

Policy objective 6.4.1 – Access to information and application system functions must be restricted in accordance with a defined access control policy.

(107) The access control policy must be defined in line with the requirements and controls of section 6, 7.1 and 7.2, and in particular the need-to-know principle for all types of users (e.g. system administrators, developers, helpdesk staff, end users…).

(108) Application services may only access production and configuration data of the application.

(109) Application backup (without production data) may only be accessible by application managers and operators.

14. MONITORING AND LOGGING FOR ACCESS CONTROL

Access to audit logs must be treated in the same way as the access to operating systems and system utilities.

Detailed rules for protection and usage of audit logs and tools, types of events recorded by audit subsystems, and their parameters are defined in the Standard on Logging and Monitoring .

15. REFERENCES

Commission Decision C(2006) 3602 of 16/8/2006

Implementing Rules for Commission Decision C(2006) 3602 of 16.8.2006.

Standard on Asset Management.

Standard on Risk Management.

[11] In the context of this document, access to system utilities is part of access to the operating system, which is understood as access to privileged functions and privileged objects of the operating system.

Guidelines on Access Control and Authentication.

Standard on Network Security.

Standard on Logging and Monitoring.

ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements.

ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management.

NIST SP 800-63-1 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, December 2008.