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

Brussels 28/05/2010
HR.DS ARES (2010)288262

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON ASSET MANAGEMENT

ADOPTED BY MRS. IRÈNE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 28/05/2010

Version 28/05/2010

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.

Commission européenne, L-2920 Luxembourg. Telephone: (352) 43 01-1.

TABLE OF CONTENTS

1. ADOPTION PROCEDURE 3

2. INTRODUCTION 3

3. OBJECTIVES 3

4. SCOPE 4

5. RESPONSIBILITY FOR ASSETS 4

5.1. Inventory of assets 4

5.2. Ownership and management of information systems assets 5

Asset ownership 5

Implementation and protection of the asset 6

6. CLASSIFICATION OF ASSETS 7

6.1. Classification principles 7

6.2. Confidentiality levels 8

Four EU Classified information levels 8

Unclassified information levels: 8

Security markings and designators 10

6.3. Integrity level: 10

6.4. Availability level: 11

6.5. Information owned by external party or classification (partly) imposed 11

7. RETURN OF ASSETS 12

8. REFERENCES 12

9. RELATED DOCUMENTS 13

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 for 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

This document describes how responsibility for assets is defined and how information system and information processed therein must be classified. Classification means the definition of the security needs as described in Art. 8 of Commission Decision C(2006) 3602.

The classification of information system and information processed therein is a mandatory step in the process of identifying the security requirements and measures that are appropriate to the possible impact of damage resulting from a loss of confidentiality, integrity and availability. This classification must be performed at Directorate-General level as described in the section 3.4.1 of the Implementing Rules.

This classification takes into account existing and approved frameworks related to information value identification such as the Business Continuity Management and Risk Management frameworks.

This standard is complemented by the document: Guidelines on Asset Classification proposing three alternative methods to actually carry out a classification.

3. OBJECTIVES

The objective of this standard is to ensure that all important Commission assets receive the appropriate level of protection in a consistent way.

4. SCOPE

All assets associated with Commission information system and information processed therein must be taken into account for inventories and their classification. A non-exhaustive list of assets is given in section 5.1.

5. RESPONSIBILITY FOR ASSETS

Policy objective 2.1.1: All information systems assets, whether physical or logical, must be identified, indicating their value to the Commission.

Policy objective 2.1.2: All information systems must have a designated owner, accountable for their security protection and must have a designated responsible for the implementation and maintenance of appropriate controls.

5.1. Inventory of assets

Information system assets[1] are logical (information, software) and physical (network, hardware, sites) assets, as well as personnel and organisation that are associated with a Commission information system.

They must be identified and inventories/registries will record the assets deemed important[2] for the business objectives of the Commission, DG or service.

The inventories are created and maintained under the responsibility of, and within the domain of a designated owner (see section 5.2 for the identification of the owner).

The following list of assets related to information and information systems has to be considered for identification and inventory:

- Information assets whatever form it takes: for example in databases and data files, Commission or system documentation, contracts, user manuals, training material, operational or support procedures, guidelines, documents containing important results of the Commission's business, continuity plans, or fallback arrangements

- In addition, there are other assets that are used to store or process information, or have an impact on the security of the information assets. These other assets include the following:

  - Software: such as business applications, package or standard software (database management software, application server software, web server software, etc.), service, maintenance or administration software (backup software, etc.), operating systems, development tools and utilities,

---

[1] An asset is anything that has a value for the Commission

[2] A method explaining how to assess the importance of assets is described in the document Guidelines on asset importance assessment.

- Network: such as medium and support (cable, fibre, etc.), passive and active relay (router, switches, etc.), communication interface (WIFI connection devices, etc.), network interconnection devices (firewalls, gateways, proxies, etc.),

- Hardware: such as data processing equipments (transportable equipments, fixed equipments, processing peripherals, etc.), data medium (electronic medium, other media),

- Sites: such as places (building, offices, computer rooms, etc.), essential services (telephone lines and network, power supply, cooling and anti-pollution devices, etc.),

- Personnel and organisation: such as users, system administrators, developers, external personnel (subcontractors, suppliers, manufacturers, etc.), structure of the organisation, project or service organisation.

Details recorded within inventories have to describe the importance of each asset to the Commission and include at least: identification and brief description, the owner of the asset (and delegations given), Commission Entity, location and security classification of supported information.

5.2. Ownership and management of information systems assets

Asset ownership

- Owners must be designated for all information system assets, including systems under development.

- An owner is the person / organisational entity responsible and accountable for an asset.

- Owners must have sufficient authority and knowledge, allowing them to understand the business value of the assets they own and to balance security needs against cost considerations and business requirements.

- The owner of an information system asset and of the information processed therein is the System Owner as defined in Annex II.C of Commission Decision C(2006) 3602.

- The system owner:

  - Define, sign-off and periodically (recommended at least once a year) review the level of classification of the asset, based on business needs for protection of the asset (see section 6 on classification of assets). If necessary, the system owner can consult the data owner as described in the Decision C(2006)3602.

  - Accept and sign-off not only the controls associated with that classification but also the controls resulting from the risk assessment subsequent to that classification (see section 3.4.1 of the Implementing

Rules for the mandatory criteria based on classification levels to carry out a risk assessment after the classification).

- The IT service provider as defined in Annex II.G of Commission Decision C(2006) 3602 provides system owners with a range of structured and managed IT resources such as electronic communications networks, equipment and software. The IT service provider owns the provided resources or assets.

- On the request of the system owner to change the classification level, the Service Level Agreements (or equivalent operational agreements) agreed between the system owner and the IT service provider are reviewed. Subsequently, the IT service provider adapts the provided resources or assets to comply with the requirements of the new classification level.

- For practical purposes, the system owner can delegate some or all of his/her duties to other persons but the ultimate accountability will remain with the system owner, as indicated in the Decision C(2006)3602.

Implementation and protection of the asset

- The protection of the asset may be executed by the system manager directly under the responsibility of the system owner or subcontracted to an IT service provider.

- The IT service provider is responsible for the security of the resources it provides and must implement the security measures specified in the Service Level Agreements concluded with the system owner. These security measures are the result of the level of classification of the information system required by the system owner for all information systems and also of the risk assessment carried out by the system owner in case of specific information systems.

- These duties are described in the C(2006) 3602 decision under the System Managers and IT Service Providers section.

6. CLASSIFICATION OF ASSETS

Policy objective 2.2.1: Information and related information systems must be categorised on the basis of their security needs, i.e. levels of confidentiality, integrity and availability, using a systematic process based on their value to the Commission, criticality and sensitivity. These levels, which must be periodically reviewed, allow the need for, priorities for, and degree of security protection to be determined.

6.1. Classification principles

All assets associated with information and information systems need to be protected in relation to their business value.

Classification (or assessment of security needs) is the process of establishing the business impacts for the Commission of a loss of confidentiality, integrity and availability of its information and of synthesising them in classification levels.

Classification of information systems assets is a business decision and is under the accountability of the system owner.

The classification process is used to classify all physical and logical assets based on the classification of the information they are storing or processing.

- Classification is first done on **information**, regardless of the means used to store or to process them. When the information results from the aggregation of different information elements, the classification shall be performed taking into account the aggregated set of information elements.

- The classification of software and physical assets is inherited or derived from the classification of the information they are storing or processing.

- When an asset is related to two or more distinct classification levels of information, the classification of this asset must always adopt or be based on the highest classification level.

- When an asset has been classified at a certain level, any of its dependent assets (e.g. subsystem or component) inherits the same classification level.

- Any copy of information must bear the same confidentiality and integrity levels as the original information. The availability level may be different depending on the purpose of the copy.

- The classification process must take into account that the classification level may be time and / or event dependent.

- Assets that exchange information are interdependent and the coherence of the assets classification carried out by the respective system owners must be ensured in the workflow of such information.

6.2. Confidentiality levels

The required confidentiality level is obtained by assessing the extent of harm to the organisation that would result from unauthorised disclosure of the information and related assets.

The possible classification levels given below are determined by the Commission Decision C(2006) 3602 for unclassified information and by the Commission Decision 2001/844/EC for EU classified information.

Four EU Classified information levels

EU classified information levels must be applied to information or assets reserved for a limited number of persons on a need to know basis and whose disclosure to unauthorised persons would be prejudicial to the Commission, other Institutions, Member States or other parties. The four EU classified information levels[3] are described below.

- TOP SECRET UE/EU TOP SECRET: this classification shall be applied to information and related assets the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of its Member States.

- SECRET UE: this classification shall be applied to information and related assets the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of its Member States.

- CONFIDENTIEL UE: this classification shall be applied to information and related assets the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of its Member States.

- RESTREINT UE: this classification shall be applied to information and related assets the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of its Member States.

Unclassified information levels:

- LIMITED: an information system or information reserved for a limited number of persons on a need to know basis and whose disclosure to unauthorised persons would be prejudicial to the Commission, other Institutions, Member States or other parties, but not to an extent serious enough to merit EU Classified information status. However, as the scope of this definition is large this category is **broken down into** 2 sub-categories which correspond to two levels of prejudice in the following way:

    - LIMITED BASIC for information systems or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause moderate

[3] According to article 17.2 of the Decision 2001/844/EC, it is important that the classification into EU classified information levels is correctly and sparingly used, especially the top secret UE.

prejudice to the Commission, other institutions, Member states or other parties, but not to an extent serious enough to merit EU classification. Cases would include:

- moderately affect political or diplomatic relations;
- cause local negative publicity to the image or reputation of the Commission or other institutions;
- cause embarrassment to individuals;
- affect staff morale/productivity,
- cause limited financial loss or, moderately facilitate improper gain or advantage for individuals or companies;
- moderately affect the effective development or operation of EU policies;
- moderately affect the proper management of the EU and its operations.

- LIMITED HIGH for information systems or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause consequential prejudice to the Commission, other institutions, Member states or other parties, but not to an extent serious enough to merit EU classification. Cases would include:
  - cause embarrassment to political or diplomatic relations;
  - cause damage to the image or reputation of the Commission or other institutions in maximum three member states;
  - cause distress to individuals;
  - cause consequential reduction in staff morale/productivity;
  - embarrass EU or Member States in commercial or policy negotiations with others;
  - cause financial loss or facilitate improper gain or advantage for individuals or companies;
  - affect the investigation of crime;
  - breach legal or contractual obligations on confidentiality of information;
  - affect the development or operation of EU policies;
  - affect the proper management of the EU and its operations.

- PUBLIC: an information system or information whose public disclosure would not damage the interests of the Commission, the other Institutions, the Member States or other parties.

Security markings and designators

Moreover an additional and optional security marking can be attached to information at one of the above confidentiality levels of security (except Public level) identifying the categories of persons or bodies that are the recipients of the information or authorised to access it, like:

- Commission internal: only for use within the Commission
- Limited: only for use within the European Institutions and Members States
- Limited DG/Service: only for use within the nominated DG/Service
- Personal: only to be opened by nominated person

In addition a "security designator" approved by the Security Directorate may be added to the classification of documents, either to limit the validity of the classification, or when there is a need for limited distribution and special handling in addition to that designated by the security classification.

The approved lists of security markings and designators that may be used at the Commission are given in the "Security Notice 01: The use and application of security designators and markings". (See Security Directorate website)

6.3. Integrity level:

The required integrity level is obtained by assessing the extent of harm to the organisation that would result from partial loss, corruption or unauthorised modification of the information asset.

Three integrity levels are determined by Commission Decision C(2006) 3602:

- MODERATE: this "low" classification shall apply to information and related assets the loss of integrity of which might threaten the internal working of the Commission.
- CRITICAL: this "medium" classification shall apply to information and related assets the loss of integrity of which might threaten the position of the Commission with regard to other Institutions, Member States or other parties.
- STRATEGIC: this "high" classification shall apply to information and related assets the loss of integrity of which would be unacceptable to the Commission, other Institutions, Member States or other parties.

6.4. Availability level:

The required availability level is obtained by assessing the final / maximum consequences of a loss of availability of the information asset.

Three availability levels are determined by Commission Decision C(2006) 3602:

- MODERATE: this "low" classification shall apply to information and related assets the loss of availability of which might threaten the internal working of the Commission.

- CRITICAL: this "medium" classification shall apply to information and related assets the loss of availability of which might threaten the position of the Commission with regard to other Institutions, Member States or other parties.

- STRATEGIC: this "high" classification shall apply to information and related assets the loss of availability of which would be unacceptable to the Commission, other Institutions, Member States or other parties.

It is also recommended to assess the time-criticality of the recovery mechanisms that must be applied if the information asset is unavailable, i.e. assessing the maximum period of outage of the asset that is acceptable for the business, which is named Recovery Time Objective (RTO) [4].

6.5. Information owned by external party or classification (partly) imposed

In case of information originated from, or owned by an external party with which the Commission has concluded a security or a service level agreement, the Commission must use the classification defined by this external party.

Similarly, if the classification of the asset is partly imposed (or known) the classification exercise can be faster and the effort focused on the classification parts/steps that are not yet known.

---

[4] This is explained in the document: "Guidelines on Asset classification".

7. RETURN OF ASSETS

Policy objective 2.1.4: Upon termination of their employment, contract or agreement, all Commission staff, contractors and third-party users must return all Commission information systems assets in their possession: for example security tokens granted to teleworkers, laptops or PDAs.

- When a person employed by the Commission, either as Commission staff, contractor or third-party user, is terminating his/her relationship with the Commission, his/her immediate manager/responsible must ensure all Commission's property in the his/her custody is returned before (s)he leaves the Commission.

- A termination checklist available in each DG must include important security measures and actions to be done under the responsibility of the immediate manager of the terminating person, such as the return of Commission property and the removal of site and system access rights.

- The terminating person must inform his/her immediate manager about all company property s(he) possess. This includes portable computers, library books, documentation, building keys, access badges, credit cards, PDAs, mobile phones and any other Commission property that must be listed in the DG termination checklist.

- Upon termination of employment, a terminating person, as Commission staff, contractor or third-party user, must not retain, give away or remove from the Commission's premises any Commission information other than personal copies of information classified as public and personal correspondence directly related to the terms and conditions of their employment.

- All other Commission information in the custody of the departing person must be provided to the employee's immediate manager at the time of departure. This information must be in readable form, i.e. not encrypted.

8. REFERENCES

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

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

International standard ISO/IEC 27001 – Second edition 2005-06-15

International standard ISO/IEC 17799 – Second edition 2005-06-15

Framework for Business Continuity Management in the Commission {Sec(2006) 898 and 899}

Security Notice 01: The use and application of security designators and markings (See Security Directorate website)

Towards an effective and coherent risk management in the Commission services SEC(2005)1327

Decision 2001/844/EC, CECA, Euratom 29/11/2001

9. RELATED DOCUMENTS

Guidelines on asset classification

Standard on risk management

Guidelines on asset importance assessment