EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate DS - Security
Coordination and Informatics Security

Brussels, 18/02/2011
HR.DS5/GV/ac ARES (2011) 183003
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON PHYSICAL AND ENVIRONMENTAL SECURITY

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 18/02/2011

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

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

In order to protect the confidentiality, integrity and availability of computer systems and the information held therein, controls must be applied to assure their physical protection. These controls are intended to prevent physical damage and unauthorised physical access, whether accidental or deliberate.

Accidental damage may be caused by any number of factors, ranging from environmental conditions (such as bad weather, earthquakes etc) to simple accidents such as a person tripping over a cable and accidentally disconnecting it. Deliberate threats are normally either aimed at theft, causing physical damage (sabotage), or gaining logical access to computer systems for other purposes (such as espionage), which is greatly facilitated when physical access is possible. The controls described in this standard are intended to cover all aspects of physical security.

3. OBJECTIVES

This standard provides detailed instructions for the physical and environmental protection of all types of computer systems, including servers, network equipment, cabling and end user devices.

4. SCOPE

This standard applies to all premises that are occupied by the European Commission and/or that contain EC information systems, except for Class I and Class II security zones which are covered by the Commission Decision 2001/844/EC, ECSC, Euratom on Information Security. It also applies to physical computing assets that are used for EC systems, including systems that are owned, housed or operated by third parties on behalf of the Commission.

The scope includes but is not limited to the following: servers, workstations, portable PCs, other portable computing devices (PDAs etc), storage devices, network equipment and cabling. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties having access to these assets.

In relation to non-computing assets, such as HVAC systems, public utilities (electricity, water etc.) and telecommunication links, this standard applies to all installations within Commission premises.

5. THREATS COVERED

Security controls defined in this security standard will reduce the level of exposure to the following threats (their description is in the *Standard on Information Security Risk Management*):

T01 – Fire

T02 – Water damage

T03 – Pollution

T04 – Major accident

T05 – Destruction of equipment or media

T06 – Climatic phenomenon

T07 – Seismic phenomenon

T08 – Volcanic phenomenon

T09 – Meteorological phenomenon

T10 – Flood

T11 – Failure of air-conditioning

T12 – Loss of power supply

T14 – Electromagnetic radiation

T15 – Thermal radiation

T16 – Electromagnetic pulses

T17 – Interception of compromising interference signals

T18 – Remote spying

T19 – Eavesdropping

T20 – Theft of media or documents

T21 – Theft of equipment

T23 – Disclosure

T25 – Tampering with hardware

T26 – Tampering with software

T27 – Position detection

T33 – Unauthorised use of equipment

T36 – Corruption of data

6. TERMINOLOGY

Administrative zone: a physical area where officials and other staff regularly work.

Class I / II Security Zone: a specifically defined physical area on Commission premises which has a higher security requirement than standard zones.

Delivery and Loading Area: an area that is dedicated to the receipt of incoming items (e.g. mail or goods) and/or the despatch of outgoing items.

HVAC: an acronym for Heating, Ventilation and Air Conditioning, some of the basic environmental controls that are required in computer rooms.

Physical intrusion detection system: the process or technology for detecting physical intrusion into premises, i.e. unauthorised people gaining physical access to secured areas. This term is used in this standard to distinguish it from "Intrusion detection systems", which in information security terms are usually host- or network-based systems that detect malicious activities.

PIN: Personal Identification Number, a common acronym for a code used (often together with a physical token) to authenticate a user.

PIR: Passive Infra-Red, a type of detection system that captures infra-red radiation to detect intruders.

Public zone: a physical area where access is not restricted (e.g. reception areas or public meeting rooms).

Secure zone: a physical area where servers and other technical equipment are located. Secure zones are subject to higher levels of physical protection than Administrative zones.

Server room: a term used in this document to denote a secure zone, or a part thereof, which contains computer servers.

Technical room: a term used in this document to denote a secure zone, or a part thereof, which contains other technical equipment such as network switches, telephone equipment, patch panels or control panels. There is often a technical room on each floor of a building.

7. BACKGROUND INFORMATION

7.1. System and Information Classification Levels

This standard specifies the minimum level of protection that must be applied to EC information systems, both classified (EUCI) and non-classified (non-EUCI), but additional measures may be required for systems designated as "SPECIFIC". Non-EUCI is split into three levels of confidentiality;

PUBLIC, LIMITED BASIC and LIMITED HIGH. Information systems are also classified as MODERATE, CRITICAL or STRATEGIC for integrity and availability.

When designing security controls for zones, the classification levels of confidentiality, integrity and availability of the systems and information stored and handled therein should be taken into account.

7.2. Physical Security Zones

This document refers to the different physical security zones that are defined and applied by the Commission for the protection of its assets, premises and personnel. These physical zones are defined by the Security Directorate in collaboration with OIB and OIL.

The Commission Decision 2001/844/EC, ECSC, Euratom on Information Security defines Class I and Class II security zones for the handling of EUCI, and detailed specifications for these zones are maintained separately by the Security Directorate (see the *Normes et Critères applicables aux Services de la Commission – version 2006*).

Additional security zones are not formally defined for other EC offices, although they are commonly divided into Administrative zones (where officials and other staff regularly work) and Secure zones (where servers and other technical equipment are located). Secure zones have additional physical security measures and their access is restricted to limited numbers of authorised personnel.

The term "Public zones" is commonly used for areas that are outside many of the physical access controls, such as reception areas or public meeting rooms. Delivery and Loading Areas are also defined, which are intended for the arrival or despatch of mail or goods and where additional controls must be implemented against specific threats, such as bombs hidden in incoming deliveries.

7.3. Physical Security Perimeters

The perimeter of a zone is its outside boundary, in three dimensions. The physical security perimeter consists of all walls, windows, ceilings, floors and access points at the boundaries of the zone.

Access points may exist for human access (doors or other security barriers), for delivery or despatching of goods, or for technical purposes (cable runs, air conditioning vents etc.). Vulnerabilities in the physical perimeter, such as unlocked windows, non-solid walls or partitions, can also create unintended access points which should be eliminated.

The perimeter of the administrative zone will normally cover all of the premises occupied by the Commission, with the exclusion of any public zones such as the reception area. Secure zones may be entirely surrounded by administrative zones (e.g. for technical rooms within an office building), or they may have an external perimeter (e.g. a separate data centre).

7.4. Third Party Premises

As stated in the Scope (section 4), this standard is also applicable to third party premises where EC system are housed or operated. Contracts with third parties must include appropriate requirements for physical and environmental security in accordance with this standard, and provisions for auditing the relevant security measures.

7.5. Document Structure

The rules in this standard are split into three main chapters. The first two, "Secure areas" (section 8) and "Protecting against external and environmental threats" (section 9), concern physical zones within Commission premises (or other premises housing EC systems). The third, "Equipment security" (section 10), relates to physical protection of the devices themselves, when they are within or outside Commission premises.

8. SECURE AREAS

Policy objective 4.1.1 – Physical security perimeter – Security perimeters with appropriate barriers and entry controls must be used to protect areas that contain information and information processing facilities.

Policy objective 4.1.2 – Secure areas – Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Work in secure areas must follow specific security rules.

Policy objective 4.1.3 – Securing offices, rooms and facilities – Physical security for offices, rooms and facilities must be designed and installed. Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

8.1. General Rules

Physical security perimeters must be defined for all premises housing Commission information and information systems. The physical security controls for these premises must comply with this document and any other relevant Commission standards[1], such as technical standards on building construction, doors, windows or locks.

Physical access controls must address at least the following elements:

- Identification and protection of all entrances and exits
- Access control systems
- Procedures for visitor reception and logging

[1] The Security Directorate can advise on building security standards.

- Guards (controlling entrances, reacting to requests or alarms and performing patrols)

- Physical intrusion detection systems (alarms)

Care must be taken regarding buildings where the Commission is not the sole occupant to ensure that the internal perimeter of the Commission premises is secured by physical security controls as described above. In particular, potential access points such as technical passages or cable runs and potential vulnerabilities such as non-solid walls or easily broken windows must be reviewed and secured against the possibility of physical intrusion.

Information processing zones containing EC information systems (including those managed by sub-contractors working within Commission premises) must be separated from zones that contain information systems of third parties. In practice, this separation may be provided through the use of measures such as separate locked cages in computer rooms. These physical separation measures must be protected and monitored in accordance with the rules in this standard.

A physical security boundary must exist between each of the zones described in section 7.2 above to ensure that the zones are physically segregated.

Systems and related equipment should not be located in zones that are higher than required (according to this standard or the results of the asset classification or risk assessment) in order to avoid people having to enter higher security zones unnecessarily.

Clear written security instructions must be given to the security guards by the Security Directorate for the security of all offices, rooms and facilities. These instructions must cover issues such as regular building patrols (where applicable), specific issues to check, and procedures in the event of an incident that could involve a breach of information security (such as the theft of computer equipment). Specifically, the incident procedures must contain provisions for the Security Directorate to be notified as soon as possible in the event of an incident that could impact information security (e.g. theft or damage of computer equipment).

Additional rules are given below for Public zones, Administrative zones, Secure zones, and Delivery and Loading Areas. Instructions for Class I and II security zones are outside the scope of this standard.

8.2. Rules for Specific Zones

The following sections include rules that are applicable to each type of zone.

8.2.1. Public Zones

Public zones should be included in the surveillance and patrol areas for the security guards.

8.2.2. Administrative Zones

Administrative zones must be protected by entry (or physical access) controls including:

- physical entry controls (such as solid doors, turnstiles or PNG[2]) and/or guards at the external perimeter
- access controls, such as an authentication card, to authorise entry to these areas
- formal visitor entry controls
- a securely maintained audit trail of visitor access
- visible identification worn by all staff (access badge)
- a policy of challenging unescorted persons not displaying a badge authorising access to the zone

Visitors must be accompanied inside these zones.

Doors and windows on the perimeter of the zone must be closed and locked when the building or room is unattended.

Rooms where IT equipment is stored (IT stock rooms) may be located within an administrative zone but they must be protected by at least a locked door with access control.

8.2.3. Secure zones

Secure zones must follow all of the rules defined for Administrative zones, together with the additional rules below.

- Third party support service personnel must be granted restricted access to secure zones only when required. This access must be authorised and all work done by third party personnel must be supervised.
- Directories and internal telephone books identifying locations of secure zones must not be readily accessible by the public.
- Access rights to secure zones must be regularly reviewed and updated.
- Secure zones must be protected with at least the following controls. Further details (e.g. technical standards for approved locking devices) may be obtained from the Security Directorate.

[2] Passage Non Gardé (unguarded entry point)

- The access door must be alarmed and monitored, and burglar resistant. It must be equipped with an approved locking device and should be connected to the system that controls access to the zone.

- Windows and frames must all be burglar resistant and equipped with burglar resistant glass. Security bars must be installed on the inside of all windows. It must not be possible to look inside the room from outside.

- The perimeter walls of the secure zone must be solid, i.e. not partitions or temporary walls that can be easily removed or broken through.

- Access to these rooms must be restricted to authorised personnel. Cleaning and maintenance work may only be performed under the supervision of an authorised person.

- Access control systems must be dual-factor, e.g. a card and a PIN.

- No user offices may be situated within server rooms or technical rooms.

- Physical intrusion detection systems must be in place and activated whenever the secure zone is left unattended. The systems must be permanently monitored to trigger a response upon intrusion detection. Detectors should use at least passive detection technology (e.g. PIR).

- All control panels (e.g. for HVAC or physical security systems) must be protected against unauthorised access and accidents[3], and firmly anchored to the walls.

- Technical rooms must be designed to provide effective security, as described above, and should preferably have solid walls and no windows.

8.2.4. Delivery and Loading areas

Materials entering or leaving the premises must do so via designated access points that are designed for this purpose and have appropriate controls to prevent unauthorised access or misuse. Deliveries must be expected and any despatch of goods must be authorised.

Controls over delivery and loading areas must include:

- Access from outside the premises must be restricted to identified and authorised personnel.

[3] Accidents may include damage or the accidental (dis)activation of a control, e.g. by someone unknowingly pressing a switch.

- Access controls must be in place to prevent delivery personnel from gaining access to other parts of the building.

- Incoming material must be inspected for potential threats before it is moved into the building from the delivery area.

- Incoming material should be registered in accordance with asset management procedures on entry to the site.

9. PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

Policy objective 4.1.4 – Protecting against external and environmental threats – Physical protection against damage from natural or man-made disaster must be designed and applied proportionally to the risk.

This standard contains general rules for protecting against external and environmental threats. Other rules may exist in different standards, notably the *Standard on Business Continuity Management*, which must be followed in addition to these rules.

The design and layout of information processing facilities must provide protection from physical and environmental hazards.

All equipment must be properly vented, and the temperatures and humidity in server and telecom rooms must be monitored and maintained in a range that is appropriate for the operation of the equipment therein.

Lightning and surge protection must be provided for information processing facilities.

Appropriate fire fighting equipment must be provided and suitably placed. Server and telecom rooms must be equipped with both automatic fire suppression systems and manual CO_2 fire extinguishers that are appropriate to the environment. All fire suppression and other safety systems must comply with the relevant norms and the health and safety legislation applicable within the Commission. Fire alarms must be tested at least once a month, and fire drills must be performed at least twice a year to ensure that personnel are aware of the evacuation procedures.

Protection against flooding or other water damage (such as leaks from the ceiling) must be in place, as appropriate to the physical circumstances of the zone. Factors such as water pipes in the ceiling, the existence of a water supply in the room or the room being located below ground level should be taken into consideration.

All systems providing environmental protection must generate alerts when abnormalities are detected. The alerts must be processed via the appropriate incident management procedures.

All systems providing environmental protection must be regularly checked and maintained according to the manufacturers' recommendations. A review of the security measures in place should be performed at least annually by the EC official

or department that is responsible for the zone, or by the IT Service Provider as appropriate.

10. EQUIPMENT SECURITY

Policy objective 4.2.1 – Equipment siting and protection – Equipment must be protected from physical and environmental threats and from opportunities for unauthorised access. Power and telecommunications cabling carrying data or supporting information services must be protected from threats arising from interception or damage.

Policy objective 4.2.2 – Equipment maintenance – Equipment must be correctly maintained to ensure its continued availability and integrity.

Policy objective 4.2.3 – Security of equipment off-premises – Equipment, information or software must not be taken off-site without prior authorisation. Adequate protection must be applied to off-site equipment, taking into account the different risks of working outside the Commission's premises.

This section details the measures that must be taken to protect computer hardware within offices, server or telecom rooms or other facilities. It focuses on protection of the individual devices, whereas the previous sections concerned the protection of areas where systems reside.

In case computer equipment or information within the scope of this standard is used in a physical security zone of a lower level than that where it should normally be located, additional compensating controls must be implemented (see also section 10.3 below for the security of equipment taken off-site).

10.1. Equipment Siting and Protection

The following rules must be taken into account to protect equipment:

- Equipment must be sited in an appropriate physical zone, based on the levels of confidentiality, integrity and availability of the information that it stores or handles. Servers must be sited in secure zones.
- Physical access to IT systems, including network infrastructure (active components such as routers and switches), must be limited to authorised personnel.
- Equipment installed in general office environments must be protected against theft.
- Records must be maintained of all movements of hardware (excluding mobile devices).

Power and telecommunications cables must also be protected. In particular, measures must be taken to protect important cables that are installed outside protected zones (Secure or Technical zones), such as:

- Main power cables serving multiple devices
- Network cables connecting different physical or logical zones
- Network cables connecting switches (e.g. a local switch serving an office floor to a central switch)

Care must be taken to ensure that these cables are protected appropriately against accidental or deliberate damage, and against wiretapping. The measures to be taken must be selected according to the risks (e.g. the classification of data passing through the cable, and its susceptibility to physical damage and wiretapping[4]).

10.2. Equipment Maintenance

The following rules for equipment maintenance must be implemented:

- Equipment must be maintained in accordance with the supplier's recommended service intervals and specifications.
- Records must be kept of all suspected or actual faults, and of all preventive and corrective maintenance
- Only authorised maintenance personnel may carry out repairs and service equipment.
- Appropriate controls must be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the Commission. Where necessary, sensitive information must be cleared from the equipment or the maintenance personnel must be sufficiently cleared and supervised by authorised personnel (see the *Standard on Sanitisation of Media*). Any equipment that is removed from Commission premises for maintenance must be logged and tracked.

10.3. Security of Equipment Off Premises

The use of any information processing equipment (except mobile devices) outside the organisation's premises must be authorised by the System Owner (see the *Standard on Asset Management*) or an approved delegate before the equipment is taken or used off premises.

When equipment is to be taken or used off premises, appropriate measures must be taken to protect it and the information held on it according to its classification (particularly for confidentiality). These measures must be described in the request to the System Owner for approval to take the equipment outside the premises.

---

[4] Relevant factors include whether data passing through the cable is encrypted; the cable's material (copper versus fibre-optic), shielding etc.

See the *Standard on Mobile Computing and Teleworking* for information on the security of mobile devices used outside EC premises.

11. ROLES AND RESPONSIBILITIES

Security Directorate: responsible for ensuring that premises (including administrative offices, server rooms, technical rooms etc) comply with requirements for physical security and environmental protection.

System Owners: responsible for ensuring that computer hardware is physically located in appropriate zones.

End Users: responsible for using workstations and mobile devices only in appropriate physical locations, and for taking care when transporting or using mobile devices (particularly portable PCs) in public places. End users must also be aware of the application of physical security controls, such as preventing tailgating and not discussing sensitive information in public areas where they may be overheard.

12. REFERENCES

Commission Decision (2001/844/EC, ECSC, Euratom) of 29/11/2001

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

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

Normes et Critères applicables aux Services de la Commission – version 2006

Standard on Information Security Risk Management (draft)

Standard on Business Continuity Management

Standard on Sanitisation of Media (draft)

Standard on Asset Management

Standard on Mobile Computing and Teleworking (draft)

13. RELATED DOCUMENTS

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

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