HANDLING INSTRUCTION 7[1]

PHYSICAL SECURITY

1. INTRODUCTION

(1) Physical security means the application of physical and technical protective measures to prevent unauthorised access to confidential information and to set up barriers against theft or aggression.

(2) In order to protect classified information and to develop and protect the activities of the European Parliament in matters that require a certain degree of confidentiality, a number of minimum technical security measures shall be established and secure facilities shall be created.

2. PRINCIPLES

2.1 Protection of EU classified information (EUCI)

(3) Physical security measures shall be put in place for all premises where classified information and material are stored and/or handled. Physical security measures shall be accounted for from the planning stage.

2.2 Degree of physical security for EUCI

(4) Physical security measures shall be selected taking into account all relevant factors, including:

(a) the level of classification of information and/or material;

(b) the amount and form (for example hard copy/computer storage media) of the classified information held;

(c) the surrounding environment and structure of the premises housing classified information;

(d) the locally-assessed threat from risk management services which target the European Union and/or its Member States and from sabotage, terrorist, subversive or other criminal activities.

2.3 Objectives of the security measures

(5) Physical security measures shall be designed to:

(a) deny surreptitious or forced entry by an intruder;

---

[1] Decision of the Bureau of the European Parliament of 15 April 2013 concerning the rules governing the treatment of confidential information by the European Parliament

(b) deter, impede and detect actions by disloyal personnel (the spy within);

(c) allow for identification of personnel regarding access to classified information in accordance with the necessary authorisations; and

(d) detect and act upon any security breaches as soon as possible.

2.4 Principles of physical security

(6) Physical security shall be based on the principle of “defense in depth”, that is to say the application of a range of security measures organised as multiple layers of defence, and on delaying factors.

(7) Although physical security measures shall be site-specific, the following general principles shall apply:

(a) locations that require protection shall be identified;

(b) security measures shall be developed to provide “defence in depth” and delaying factors;

(c) the outermost physical security measures shall define the protected area and deter unauthorised access;

(d) the next level of measures shall detect unauthorised or attempted access and alert security staff;

(e) the innermost level of measures shall sufficiently delay intruders until they can be detained by the security staff force;

(f) the intervention time available to security staff is a direct result of the physical security measures designed to delay intruders;

(g) the physical security measures shall be designed to delay the intruder for longer than the time required by security staff to intervene in depth.

(8) The Technologies/Information Security unit of the Directorate-General for Security (DG Security) shall be responsible for implementing technical security standards and shall maintain a register of such norms and standards, open to inspection by the competent services of the other Institutions and by Parliament's classified information unit ("CIU").

2.5 Secure facilities

(9) Two types of physically protected areas shall be established for the physical protection of classified information:

(a) Secure Area;

(b) Secure Reading Rooms.

(10) For each secure facility, security operating procedures shall establish:

(a) the level of classified information which may be handled and stored in there;

(b) the surveillance and protective measures to be maintained;

(c) the individuals authorised to have unescorted access to the area by virtue of their need-to-know and security clearance;

(d) where appropriate, the procedures for escorts or for protecting classified information when authorising any other individuals to access the area;

(e) any other relevant measures and procedures.

(11) For each secure facility:

(a) a visibly defined and protected perimeter shall be established through which all entry and exit is controlled by means of a pass or personal recognition system;

(b) unescorted access shall be granted only to properly authorised individuals. All other individuals shall be escorted at all times or be subject to equivalent controls.

(c) electronic communications devices and electrical or electronic equipment are not allowed.

(12) The Security Authority shall certify that an area meets the requirements to be designated as a secure facility.

2.5.1 Secure Area

(13) A Secure Area is an area where information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above or equivalent, is handled and stored, meaning that, for all practical purposes, entering the area means gaining access to classified information. The secure area shall have a clearly delimited and protected perimeter, and all its entrances and exits shall be controlled.

(14) The Secure Area shall comprise the following facilities:

(a) Security Access Screening room (SAS): a reception room for screening, identifying and checking all occupants and visitors;

(b) Reading room: a room in which the procedure for consultation of classified documents - to maintain the confidentiality of the information contained in them - is applied;

(c) Registry room: the room in which information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above is registered (management zone);

(d) Secure Archive: an area with classified-information archiving space meeting differing standards based on document classification level;

(e) Communication room: a room for housing special communication equipment (transmission and receiving) and the IT system hardware needed (CIS and other) to safeguard classified information.

(15) The Reading room, Registry room and Communication room shall also be shielded against eavesdropping and electromagnetic radiation, and all persons and all equipment entering the area, including encrypted communication equipment, shall be controlled and, at regular intervals, as required by the competent security authority, shall be subjected to physical screening/inspection.

2.5.2 Secure Reading rooms

(16) Secure reading rooms are areas where classified information up to 'RESTREINT UE/EU RESTRICTED and other confidential information may be consulted and kept temporarily, in accordance with Handling Instructions 4 and 5, and stored in such a way that it is protected against any unauthorised access by means of internal controls.

3. PRACTICES

(17) The Secure Area shall meet specific protection standards. Physical security of the secure facilities is based on security layers:

(a) layer 1: perimeter:

(b) layer 2: premises;

(c) layer 3: vaults.

3.1 Layer 1: Perimeter

(18) This layer shall include:

(a) definition of the perimeter;

(b) perimeter access and perimeter intrusion detection system (PIDS);

(c) closed-circuit television (CCTV);

(d) security lighting;

(e) security personnel for incident response, patrols, visitor control, entry and exit searches.

(19) All constructions should be realised in such a manner that any attempt of an unauthorised penetration is obvious.

3.2 Layer 2: Premises

(20) This layer shall include:

(a) definition of structural elements: walls, floors, ceilings, windows, doors (including application of standards for resistance against attacks);

(b) closed-circuit television (CCTV);

(c) access control and movement policy (accreditation);

(d) intrusion detection system (IDS);

(e) security personnel for incident response, patrols, visitor control, entry and exit searches.

(21) Walls, partitions, ceilings and floors are permanent constructions and shall be connected without disruptions and without possibility of non destructive dismantling or removal.

(22) A distinction shall be made between designated entry points (doors) and passages exclusively reserved for emergency purposes (emergency exit).

(23) All entry and exit points shall be equipped with IDS and CCTV, in function of the type of use as decided and protected against any other form of use.

3.3 Layer 3: Vaults

(24) This layer shall include:

(a) standards for locks;

(b) standards for strong rooms.

3.4 Technical security measures

(25) The detail of the structural elements, including determination of the standards for resistance against attacks according to European standards in force for these matters, shall include:

(a) walls;

(b) floors - ceilings;

(c) windows;

(d) doors;

(e) locks;

(f) other.

(26) The protection of all technical spaces and miscellaneous openings (utilities) shall be defined with the following techniques:

(a) access control;

(b) Intrusion Detection System (IDS);

(c) visitor control:

– escorted/unescorted,

– visitor log,

– closed-circuit television (CCTV).

3.4.1 Walls

(27) All walls shall be solid-brick constructions built from floor to ceiling.

3.4.2 Windows

(28) All windows in the area, together with their frames, shall meet specific standards.

3.4.3 Access door

(29) The door unit shall be made up of a frame, a central block and metal fittings. It shall be certified as set out below.

3.4.4 Access control system

(30) Persons entering and leaving the secure area - except in an emergency - shall be identified by means of an access control system. It shall be made up of the following components:

(a) control PC, programmable access levels, event memories, plus printer;

(b) password-protected software;

(c) a single software package for operators to be familiar with;

(d) full overview of the entire system at any time;

(e) integrated alarm/event reporting;

(f) management software comprising calendars, time recorder, event log file and reporting functions.

(31) The access control system shall also include:

(a) badge readers, with numeric keypad (PIN code);

(b) badge mode: in and out.

(32) Badge readers shall be able to read the technology used in the Parliament.

(33) All entry and exit points shall be identified. A distinction between designated entry points (doors) and passages exclusively reserved for emergency purposes shall be made:

(a) main access point;

(b) secondary access points;

(c) emergency (exit) point.

(34) All entry and exit points shall be equipped exclusively for their use and, further, protected from being used for other purposes.

(35) The operating mode of the access control shall be "fail secure", meaning that:

(a) during normal functioning, entry and exit are solely possible using the badge/badge reader;

(b) in the event of an emergency inside the room, a deblocking device allows unlocking the door for exit the room;

(c) in the event of electrical power failure, the door of the room remains locked but a dedicated key allows continuous operation of the lock from outside.

(36) A secure cylinder in the door lock shall be installed. The keys for the secure cylinder shall be exclusively managed by the Security Service. The motorised lock shall be actuated by means of an easy-to-press pushbutton with key reset.

(37) All control, command and management boxes shall be installed inside the protected zone, and coupled to the IDS system (tampers).

(38) The access control system shall be conceived in a way to prevent unauthorised physical access (for instance, vandalism) and logical access (for instance, network) to the equipment (badge readers, controllers, etc.).

(39) All access to the Access Control system shall be audited and logged, and all information and data generated by the system shall be monitored by the Security control room.

(40) The level of security for access to secure areas could be enhanced by adding a biometric control facility identifying individuals on the basis of physical characteristics.

(41) The connection box shall be installed within the area and above the door. All door cables (magnetic contact, green box and buzzer) shall be connected there to a terminal connected to the main cable running to the area connection box.

(42) The main system rack shall contain the intrusion detection unit, door controllers, extension facility, power supply, relays, fire contact, remote management network, numbered terminals and all other items required for the system to operate properly, all of which shall be fitted to an assembly deck. All cables and wires shall be identified. The rack shall be fitted with cable grommets and be ventilated. It shall be lockable and tamper-proof. The area connection box shall be mains-powered (230V/50Hz/16A) (main source) or, in the event of a mains failure, powered by batteries fitted to a separate battery panel (secondary source).

(43) The batteries shall be sealed, no-maintenance nickel-cadmium or lead-acid batteries with a five-year life span. Their capacity shall be such that the system can fully operate. The battery autonomy period for the access doors shall be 30 hours.

(44) Batteries shall be kept permanently charged by means of suitable chargers. Sources shall be inverted by means of a switch. One power supply stream and its battery shall power the master unit. The other power supply and its battery shall be used for slave control. The back-up batteries may be fitted in a separate rack next to the main system rack. Batteries shall not be placed on top of each other. The racks shall be fitted with cable grommets and be ventilated. They shall be lockable and tamper-proof.

3.4.5 Intrusion detection system (IDS)

(45) The Secure Area shall be protected by an independent intrusion detection system (IDS). All necessary peripherals shall be connected to it, with status monitoring and tamper and disconnection control.

(46) The IDS shall be connected to the remote management control centre. Traffic between them shall be handled by means of the Internet protocol suite, i.e. the protocols used for data transfer over the Internet: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The IDS shall be connected to the movement detectors and

magnetic contacts at the door. It shall comprise all equipment needed to detect intrusions within the controlled area and shall respond accordingly when it is in surveillance mode.

(47) Tamper contacts shall be in place; keypads, movement detectors, the junction box and the master unit shall be protected by an anti-pullout device; and the circuits linking the various components and the IDS shall be permanently connected to the surveillance loop.

(48) The IDS shall meet the following criteria:

(a) Confidentiality

Design information on system upgrading and commissioning shall be regarded as confidential.

(b) Signal transmission

Data shall be digitally transmitted in real time to a monitoring centre meeting industry standards and to the Security Directorate's remote management control centre. The following information shall be transmitted:

(i) intrusion alert;

(ii) surveillance-enabled status (total or partial);

(iii) tampering;

(iv) battery and mains power supply failure;

(v) surveillance-enabled and surveillance-disabled status (total or partial) (passive on/off);

(vi) transmission testing at least once every 24 hours;

(vii) 'surveillance enabled late' and 'surveillance disabled early' status, identifying the user concerned to the monitoring centre (active on/off).

(c) Control keypad

All IDS functions shall be actuated via the numeric control keypad. It shall, in particular, flag up the type and location of each event. The keypad shall also be fitted with a local alarm signal (buzzer). It shall emit audible signals when particular functions are actuated, during the exit and entry delay period, and when numeric keys are pressed (validation).

The numeric command keypad for arming/disarming the area shall be installed either behind or in front of - but near - the area access door.

The alarm system installed in the secure area shall be separate from the building's own intruder alarm system.

The CIU shall be immediately notified of any alert in the Secure Area.

(d) Dual-technology detection

The area shall be fitted with dual-technology or bivolumetric detectors, combining hyperfrequency and passive infrared detectors within a single unit, under microprocessor control, suitable for any environment. They shall be activated or deactivated by switching circuits with jumpers: alarm memory, pulse counting, PIR or microwave detection.

(49) The intrusion detection system (IDS) shall include:

(a) an alarm system control panel: local commands, commands at distance;

(b) PIN code management;

(c) volumetric detection: dual technology with anti-masking;

(d) magnetic contacts for:

(i) doors,

(ii) windows,

(iii) miscellaneous openings,

(iv) racks, secured containers, cabinets;

(e) seismic detectors on windows and walls;

(f) glass break detectors on windows;

(g) buzzer (local alarm signal).

(50) All control, command and management boxes shall be installed inside the protected zone and coupled to the IDS (tampers).

(51) The IDS shall be conceived in a way to prevent unauthorised physical access (for instance, vandalism) and logical access (for instance, network) to the camera and recorded images.

(52) All access to the IDS shall be audited and logged and all information and data generated by the IDS shall be monitored by the security control room.

3.4.6 Closed-circuit television (CCTV)

(53) The secure-area access door shall be CCTV-monitored; imagery shall be relayed to the building's reception desk and the Security Directorate's remote management control centre. The camera shall be connected to an image recording system for subsequent consultation by authorised individuals. It shall be installed at a location regarded as security-sensitive. Whenever the door is opened - from within or from outside - a recording sequence shall be initiated.

(54) Cameras shall comply with the requisite standards, shall have the requisite characteristics and shall be vandal-proof.

(55) Recording shall be carried out in compliance with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

(56) Access to the recorder shall be restricted on the basis of user names and passwords. Recordings may be viewed only by persons duly authorised by the CIU, and only the designated administrator may delete video sequences.

(57) The CCTV system shall:

(a) cover outside perimeter, access and exit points, checkpoints;

(b) cover inside access and exit points, checkpoints, rooms, vital installations and equipment;

(c) per location, define the type of cameras: static, pan-tilt-zoom, infrared;

(d) per camera: for parameterisation purposes, define the required level of identification: face, person, activity, global scenery;

(e) provide operation and visualisation equipment (computer, screens);

(f) provide recording and storing equipment and backup capacity;

(g) dispose of appropriate light to preserve optimal observation (min 1 lux).

(58) All control, command and management boxes shall be installed inside the protected zone and coupled to the IDS (tampers).

(59) The CCTV shall be conceived in a way to prevent unauthorised physical access (for instance, vandalism) and logical access (for instance, network) to the camera and recorded images.

(60) All access to the CCTV shall be audited and logged and all information and data generated by the CCTV system shall be monitored by the Security control room.

3.5 Monitoring

(61) Monitoring of the Security equipment shall be assured by the Security Directorate:

(a) on site;

(b) work schedule: 24/7/365;

(c) communication means shall be established;

(d) operational procedures for incident response;

(e) operational procedures for operation of technical equipment.

(62) Monitoring shall be carried out by security personnel properly trained, qualified, and security cleared, and operational procedures for incident response, patrols, and inspections should be established.

3.6 Racks

(63) Foresee and organise racks or secured containers to regroup all surveillance equipment:

(a) access control system;

(b) intrusion detection system (IDS);

(c) closed-circuit television (CCTV);

(d) racks and secured containers are coupled to the IDS system.

3.7 Electrical supplies

(64) An emergency power generator/group shall be set up in order to guarantee and maintain security and safety for a minimum of 24 hours, in the event of loss of electrical power from the normal electricity network.

(65) Battery-based no break solution, in separate and appropriate cabinet, coupled to the IDS system (tamper) shall be set up and all electrical supplies shall be monitored.

3.8 Vaults and locks

(66) Secure cabinets and containers shall be fitted with mechanical or electronic combination locks, or their equivalent, and shall comply with the standards commensurate with the level of classification of the information which they are to be used to store. They shall be installed within the secure area.

(67) Containers shall be rated according to their degree of resistance to both force and surreptitious intrusion. Four different types of containers may be used.

(a) Type 4 containers: these containers are approved for storage of all EUCI, including information classified as TRES SECRET UE/EU TOP SECRET, within the secure area. They shall have a high degree of resistance to an intruder using force and using an extensive range of hand and power tools as well as to covert or surreptitious entry. They shall offer resistance to the prising of doors, drawers or lids to facilitate fishing or probing.

(b) Type 3 containers: these containers are approved for storage of information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET within the secure area. They shall have a degree of resistance to an intruder using force and using a limited range of hand tools as well as to covert or surreptitious entry. They shall resist flexing, twisting or jolting that may distort the carcass and allow the insertion of probes or devices in order to gain access to the container.

(c) Type 2 containers: these containers are approved for storage of information classified as CONFIDENTIEL UE/EU CONFIDENTIAL within the secure area. They shall be of substantial design and construction and offer resistance to the casual or opportunist intruder who has not been prepared for the attack and only has use of items that are readily to hand.

(d) Type 1 containers: these containers are approved for storage of information classified as RESTREINT UE/EU RESTRICTED. They do not have a particular security design features, but shall be securable and judged to offer a certain level of security integrity.

(68) Locks for containers shall be rated according to their degree of resistance to unauthorised opening. Four different types of locks may be used:

(a) Type 4 locks: these locks shall have a high degree of resistance to expert and professional intrusion using exclusively developed skills and resources judged not to be available commercially;

(b) Type 3 locks: these locks shall have a high degree of resistance to expert and professional intrusion using exclusively developed skills and resources available commercially to a professional locksmith;

(c) Type 2 locks: these locks shall have a degree of resistance to a skilful intruder having minimal resources;

(d) Type 1 locks: these locks shall have a moderate degree of resistance to unauthorised opening.

(69) Locks for containers of type 3 or 4 shall provide audit facilities.