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

Brussels, 04/07/2011
HR.DS5/GV/ac ARES (2011) 719444
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON OPERATIONAL MANAGEMENT

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 04/07/2011

Version 0.6_19/05/2011

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 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

The Commission's information needs are served by a wide variety of computerised information systems. Many of these systems are very sensitive and/or instrumental in supporting critical administrative functions of the Commission, and so they must be carefully managed to ensure that they operate correctly and securely.

Consequently, computer operations must be well managed and documented to minimise the risk of errors or security incidents. This standard contains some of the basic rules for the operation of Commission computer systems; additional rules are documented in other existing or forthcoming standards[1].

3. OBJECTIVES

This standard provides instructions to ensure the correct and secure operation of information processing facilities. In particular, this document focuses on the everyday procedures for operating and applying changes to IT systems, and the segregation of responsibilities and facilities to minimise security risks.

4. SCOPE

This standard applies to all IT systems that are operated by or on behalf of the European Commission, and to all facilities housing these systems. The measures mandated by this standard must be followed by all relevant personnel, including all

[1] Section 0 of this document includes a list of some other related EC information security standards that are referenced in this standard.

Commission officials, contractors and third parties who are responsible for operating Commission IT systems.

5. THREATS COVERED

Security controls defined in this information security standard will help to reduce the impact of the following threats (their description is in the *Standard on Information Security Risk Management*).

T26 – Tampering with software

T28 – Equipment failure

T29 – Equipment malfunction

T30 – Saturation of the information system

T31 – Software malfunction

T32 – Breach of information system maintainability

T33 – Unauthorised use of equipment

T36 – Corruption of data

T38 – Error in use

T39 – Abuse of rights

T42 – Breach of personnel availability

6. TERMINOLOGY

Back-up: the process of copying data to a separate store in order to protect it from unavailability or corruption of the principal store; also the data so stored.

Change Management: an IT Service Management discipline whose objective is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes to controlled IT infrastructure, in order to minimise the number and impact of any related incidents upon service.

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

IT Infrastructure Library (ITIL): a set of concepts and practices for Information Technology Services Management (ITSM), Information Technology (IT) development and IT operations, issued by the UK Government's Office of Government Commerce. Change Management is one of the ITIL disciplines.

Operating procedures: formal documentation of the approach to executing tasks related to the production and maintenance of hardware and software.

Restore: the process of copying data back to the principal store (or an alternative) from the back-up store.

SECOPS: Security Operating Procedures

Segregation of Duties: the principle of assigning tasks to different people so that no single person can commit abuses or frauds against the organisation'ssystems or processes.

7. BACKGROUND INFORMATION

Information systems operated by or on behalf of the Commission must be protected against operational problems, and there are a number of different areas in which rules must be applied to ensure their correct and secure operation. This document is one of a number of existing and forthcoming standards that outline these rules based on the Implementing Rules of Commission Decision C(2006) 3602, and it focuses on the measures to be implemented to ensure that the systems are operated in a well controlled environment.

The Commission runs thousands of Information Systems, and many thousands of end user workstations, in a very complex environment. Operational issues or incompatibilities between systems can easily cause problems, particularly of system availability but also relating to the integrity or confidentiality of information. These issues may be accidental or deliberate, and security measures must be in place to protect against both.

In view of the complexity of the Commission's IT systems and environments, it is essential that they are managed to a high level, and that the systems and procedures are standardised and formalised to facilitate systems maintenance.

8. OPERATIONAL PROCEDURES

Policy objective 5.1.1 – Documented operating procedures – Operating procedures must be documented, maintained and made available to all personnel who need them.

Policy objective 5.1.2 – Change management – Changes to information processing facilities, to systems and to the provision of services must be planned, tested, documented, communicated and approved.

Policy objective 5.7.3 – Security of system documentation – System documentation must be protected against unauthorised access.

8.1. Documented operating procedures

Documented operating procedures must be prepared for all IT systems. These procedures must be kept up to date at all times and made available to all personnel with a legitimate reason for needing them. The procedures must not be made available to unauthorised people since they may contain sensitive information about the EC's IT systems and architecture.

The procedures must cover all regular system activities, such as:

- System start-up and shutdown
- Back-ups and restores (see the *Standard on Back-up*)

- Equipment maintenance (see the *Standard on Physical and Environmental Security*)
- Media handling (see the *Standard on Sanitisation of Media*)
- Computer room management
- System installation and decommissioning
- Updates of software (see the *Standard on Secure Systems Development* and the *Standard on Technical Vulnerability Management*)
- Management of audit log information (see the *Standard on Logging and Monitoring*)
- System monitoring and response procedures (see the *Standard on Logging and Monitoring*, and the *Standard on Information Systems Security Incident Management*)
- Bulk information transfers
- Information archiving

The operating procedures must specify the instructions in sufficient detail for the correct execution for each job, including (where relevant):

- Scheduling requirements including interdependencies with other systems
- Approval procedures
- Instructions for handling errors or other exceptional conditions which may arise during job execution, taking into account restrictions on the use of system utilities
- Output handling instructions, covering:
    - The use of relevant media (particularly where special media are used, such as headed paper or different media sizes)
    - Handling of EUCI output
    - Secure disposal of media from failed jobs
- Details of support contacts in case further assistance is required for troubleshooting
- Authorised personnel or required qualifications to execute the procedure
- Reporting to be produced

Operating procedures must be treated as formal documents and subject to a documentary change control process, with document owners and changes approved by management. They must be updated whenever the systems change or inadequacies are detected in the documents.

Where technically feasible, information systems should be managed consistently using the same procedures, tools and utilities. It is recommended that the hardware and software in use should be as homogeneous as possible, in order to simplify the operating procedures and documentation, and to reduce the risk of operational errors.

For any IT systems that are managed by contractors, in particular for data centre operations, the System Owner must ensure that appropriate formal operating procedures exist, following the requirements of this standard.

8.2. Change Management

8.2.1. Formalising the change management process

The change management process must be formally documented for each IT system or group of systems, detailing the key steps of the process and identifying the stakeholders.

All changes that go through the change management process must also be formally documented, and records held by the part of the organisation that administers the process.

Responsibility for approving changes must be formally assigned either to the System Owner or to a Change Control Committee, whose participants are clearly identified[2].

8.2.2. Defining Changes

The Commission's IT systems and all related facilities, systems and services must be subject to strict change management control. Changes to operational systems should only be made when there is a valid business reason to do so.

The scope of the change management process must be defined, with clear documentation of the types of changes that do or do not require change management control.

It is not possible to define every possible type of change and determine whether each type must undergo change control. However, the following types of change must be formally controlled through this process:

- Changes to information processing facilities
- Changes to information processing services

[2] The Change Control Committee will normally be chaired by the System owner, and include other major internal stakeholders.

- Changes of hardware performing processing or core data storage
- Changes to executable software (firmware, operating systems, middleware, application software[3]…), including potentially automated updates (such as Windows Update)
- Software configuration changes that can materially affect the results of processing operations
- Any operation that requires a restart of a production server or one of its services

The following changes may not need to be controlled in most environments[4]:

- Replacing a non-processing peripheral, such as a display unit, keyboard or mouse
- Anti-virus pattern file updates
- Software configuration changes that are cosmetic or otherwise do not materially affect the results of processing operations

Changes that are performed without going through the change control process should still be recorded in a change log to ensure that they can be traced.

8.2.3. Planned Changes

All proposed changes within the scope of change control must go through a formal, documented process, including the steps described below.

8.2.3.1. Planning

- Proposed changes must be identified, described and recorded
- All changes must be scheduled at appropriate times to minimise service unavailability, e.g. within pre-defined change windows, and taking into account other changes or system-related events
- Fallback procedures must be documented to enable recovery from an unsuccessful change
- Any new requirements for licenses, support, maintenance or administrative overhead must be checked, and arrangements made as necessary

[3] For systems developed by or on behalf of the Commission, the software change management process must also take into account the specific requirements of the Standard on Secure Systems Development.

[4] This depends on the sensitivity of the environment; in some environments, it may be necessary to control some or all of these changes too.

8.2.3.2. Testing

- Changes to IT systems must first be tested in a separate environment (or the reasons for not testing documented; for instance, it may not be necessary to test new hardware that is simply replacing existing faulty hardware)

- Checks must be performed on the live system after the change has been implemented, to ensure that it has been successful

8.2.3.3. Documentation

- The potential impacts of the change, including any security impact, must be analysed in a risk assessment before the change is approved[5]

- Updates to operating or user documentation must be made if required

- Records must be kept containing details of all changes.

8.2.3.4.Approval

- Formal approval of the proposed change must be granted in advance by the system owner or a change control committee, including acceptance of the assessed risks of the change (see 8.2.3.3 above)

8.2.3.5. Communication

- Information on the change must be communicated to all relevant parties in sufficient time before the change takes place to permit them to take any necessary actions

- Training on the changes for users and operators must be considered and provided if needed

- Relevant parties should be notified of the status (success/failure) of the change after it has been performed

8.2.4. Emergency Changes

An emergency change control procedure must be included in the change control process documentation in case a change is required urgently, for example to correct a system failure. This procedure must follow the standard procedure as closely as possible, taking into account the need for quick action in the event of an emergency.

The emergency change procedure may permit some of the controls that are normally performed before the implementation of the change to be performed afterwards. In particular, potential risks of the change must be

[5] In some cases, such as when replacing faulty hardware, this step may be trivial, and it is sufficient to note that the risk is minimal. For major changes, the risk assessment may be significantly more complex.

assessed before an emergency change is executed and appropriate testing must be performed to the extent possible within the timeframe.

Approval for an emergency change must be given before the change by the System Owner or the IRM, or a delegate who is authorised to give approval during an emergency. The change must subsequently be reviewed by the System Owner or change control committee, and either accepted or reversed.

8.3. Security of System Documentation

System documentation includes all documentation relating to the design, development, implementation, operation or disposal of an information system. Typically, this may include;

- Development project documentation (e.g. RUP artefacts[6])
- Testing documentation
- Implementation documentation
- Security configuration
- Operational documentation (including SECOPS)
- User instructions

System documentation may contain sensitive information such as descriptions of technical infrastructure, applications, processes, procedures, data structures and authorisation procedures. This information may be of use to malicious individuals, and so it must be restricted.

System documentation may include both documentation provided by the supplier and that created by or on behalf of the Commission. Customised or system-specific documentation is more likely to be sensitive since it may contain specific information such as IP addresses or security configuration.

System documentation containing sensitive information (hereafter called "sensitive system documentation") must be identified and inventoried.

Sensitive system documentation must be evaluated for classification as appropriate, in the same way as any other Commission information, and protected accordingly. In particular, documentation for systems handling EUCI may need to be classified at the same level as the information handled (and possibly higher, taking into account the effect of data aggregation). Access lists for sensitive system documentation must be restricted to the minimum required and approved by the System Owner.

[6] The RUP@EC methodology is presently used to guide development projects within the EC. RUP@EC defines a number of key documents, termed "artefacts", which are part of the system documentation.

Sensitive system documentation must be stored securely, whether it is in electronic or non-electronic form. Appropriate measures must be in place such as:

- Access to electronic documents must be restricted to approved users through logical security controls (e.g. Access Control Lists)
- Access to non-electronic documents must be restricted through the use of physical security controls, such as locked offices or storage facilities

Sensitive system documentation must not be sent in unencrypted form across public networks. Where sensitive system documentation is held outside Commission premises (e.g. for remote support or outsourcing), similar levels of protection must be applied.

9. SEGREGATION OF DUTIES AND FACILITIES

Policy objective 5.1.3 – Segregation of duties and segregation of facilities – Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of information systems. Development, test and operational facilities must be separated to reduce the risks of unauthorised access or changes to the operational system.

9.1. Segregation of duties

Segregation of duties is a method of reducing the risk of accidental or deliberate system misuse. Good practices ensure that no individual employee can complete a significant transaction in its entirety. This objective is achieved by separating the tasks and associated privileges for a specific process among multiple users[7].

In relation to the Commission's IT systems, the following roles should all be segregated from each of the others. Job descriptions must describe the responsibilities of each role in a way that supports the segregation of duties.

- System owner and business users
- System developers
- Change control staff
- System administrators
- Security officer
- Auditors

[7] For general rules on the segregation of duties within the EC, see the *Internal Control Standard on Processes and Procedures*, issued by the Internal Audit Service.

In some cases, staff numbers may not always permit a proper segregation of duties. In this case, compensatory controls and audit functions should be used to prevent or detect possible abuse. An individual staff member may fulfil different roles for different systems (e.g. Auditor for one system, and Security Officer for another) as long as there is no overlap between the functionality of the systems or conflict of duties between the two roles.

9.2. Segregation of facilities

Development, test and operational facilities must be segregated to reduce the risks of unauthorised access or changes to the operational systems. The segregation of computer facilities will help to enforce the segregation of duties described above. Although it is often difficult to implement, this measure is important to preserve the security of the operational systems and data. If full segregation is not feasible, other adequate mitigating control measures may be used instead.

The number of different environments that are needed may differ according to the requirements for development and testing. They must be formally identified and comply with the following rules:

- The operational environment must run in a LAN segment that is isolated from the test and development environments' regular traffic. Therefore, separate servers and databases will be used for the operational environment.

- Software may only be transferred to the operational environment after authorisation by the System Owner (see section 8.2 above and the *Standard on Secure Systems Development*).

- Compilers, editors and other development tools or utilities must not be accessible from operational systems when not required for operational purposes.

- The test system environment(s) must emulate the operational system environment as closely as possible.

- See the rules in the *Standard on Secure Systems Development* must be followed regarding the use of production data in test and development systems.

Users must have separate user profiles for operational and test systems which are designed according to the security and functional requirements of each system. For example, security requirements in test systems may be less stringent than in operational systems.

10. THIRD PARTY SERVICE DELIVERY MANAGEMENT

Policy objective 5.2.1 – Service Delivery – Services delivered by third parties involving accessing, processing, communicating or managing the Commission's information or information processing facilities or adding products or services to information processing facilities must have appropriate integrated security controls.

These security controls, the service definition and the delivery levels must be documented in service delivery agreements so as to ensure they are properly implemented, operated and maintained by the third party.

Policy objective 5.2.2 – Monitoring and review of third-party services – The services, reports and records provided by the third party shall be managed by designated Commission personnel, regularly monitored and reviewed, and audits shall be carried out regularly.

10.1. Service delivery

Services delivered by third parties involving accessing, processing, communicating or managing the Commission's information or information processing facilities, or adding products or services to information processing facilities, must have appropriate integrated security controls. See the *Standard on Secure Systems Development* regarding the definition of system requirements, with particular reference to the sections relating to systems or services obtained from third parties.

The contract and/or service delivery agreement must include all of the following that are relevant to the service provided:

- A full and clear definition of the service and the information handled by the third party
- Responsibilities for information security assigned to a suitably qualified individual at the third party, whose appointment must be approved in advance by the Commission
- Security measures in accordance with the Commission Decision C(2006) 3602
- Metrics defined with acceptable service levels
- Regular reporting on these metrics
- Procedures for resolving unsatisfactory service levels
- Procedures for reporting and handling service problems
- Procedures for reporting and handling security incidents
- Business continuity plans
- Service termination procedures to ensure that all Commission information is securely returned or destroyed by the third party
- Right-to-audit clauses

When existing systems or services are outsourced, the Commission must plan the necessary transitions and ensure that security is maintained throughout the transition period.

The Commission must ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disasters (see the *Standard on Business Continuity Management*).

Changes to defined services or service levels must be formally managed. The security measures and metrics must be reviewed whenever such changes are made to ensure that they remain appropriate. Changes must be approved by the System Owner before they are implemented.

10.2. Monitoring and review of third-party services

The Commission must maintain overall control and visibility into all information security aspects for sensitive or critical information or information processing facilities that are accessed, processed or managed by third parties.

The responsibility for managing the relationship with a third party must be assigned to designated Commission personnel (a specified individual or service management team). In case of outsourcing, the Commission needs to be aware that the ultimate responsibility for security aspects of information processed by an outsourcing party remains within the Commission, although the third party may be responsible for operating security measures on the Commission's behalf.

Supervisory activities over third party services must include the relevant items from the following list:

- Checking service levels or other metrics
- Reporting and follow-up of service problems / outages
- Reporting and follow-up of security incidents
- Reporting on the effectiveness of security controls
- Reviewing logs or audit trails
- Requesting and reviewing audit reports
- Reviewing reports of service termination activities

The Commission must retain visibility into outsourced security-related activities such as change management, identification of vulnerabilities and information security incident reporting/response through a clearly defined reporting process, format and structure.

Sufficient Commission technical skills and resources must be assigned to perform these supervisory tasks.

11. SYSTEM PLANNING AND ACCEPTANCE

Policy objective 5.3.1 – Capacity management – The use of resources must be monitored and tuned, and projections made of future capacity requirements to ensure the required system performance.

Policy objective 5.3.2 – System acceptance and authorisation – Acceptance criteria for new information systems, upgrades, and new versions must be established. Suitable tests for the system(s) must be carried out during development and prior to acceptance to ensure that all relevant security policies and requirements are met before the system is authorised and used.

11.1. Capacity management

Capacity management[8] is an important control to ensure the continued availability of IT systems and resources. Current and future capacity requirements must be reviewed to ensure that resources are acquired in time to prevent availability issues.

All relevant resources that are used for the provision of IT systems should be included in the capacity management, including:

- Workstations
- Servers
- Internal computer resources such as processors or memory
- Storage space (hard disks, NAS/SAN devices, archives…)
- Media (tapes or other offline storage)
- Network bandwidth, cabling and switch capacity
- Shared network resources (e.g. firewalls, proxies and DNS servers)
- Data centre premises, rack space etc.
- HVAC systems
- Electrical power supply
- Personnel

Suitable metrics must be established to measure the capacity and level of use of the relevant resources, and they must be reviewed at regular intervals, to be determined as appropriate (e.g. data centre capacity may only need to be reviewed once a year, whereas storage space may need to be reviewed monthly).

[8] Or Capacity Planning, as it is often termed, although capacity planning is actually one part of the capacity management process.

Capacity reviews must take into account current and projected trends in the organization's information processing capabilities, and the lead times required for acquiring additional capacity or resources. Projections of future capacity requirements must include new business and system requirements.

This information should be used to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

When capacity issues are identified, suitable actions must be undertaken to resolve them before they cause availability problems. The obvious response to capacity issues may be to procure additional resources; however, other actions should also be considered, such as:

- Identifying and correcting problems causing abnormal use of resources (memory leaks, generation of large temporary or log files etc.)
- Investigating the cause of sudden peaks or spikes of resource usage
- Optimising the use of resources to reduce the capacity requirements
- Deleting or archiving old or unused data
- Reviewing usage to identify non-business-related items (such as MP3 files stored on file servers)
- Using spare capacity from other systems (although care must be taken not to use capacity that is actually needed, even if only in exceptional circumstances)

11.2. System acceptance and authorisation

The requirements and criteria for acceptance of new IT systems must be clearly defined, documented, agreed and tested.

New information systems, major upgrades, and new versions may only be migrated into production after obtaining formal acceptance. The following issues must be addressed prior to formal acceptance being provided:

- The system must be evaluated to establish its security requirements[9] and categorised as specified in the Commission Decision C(2006) 3602, or in Commission Decision (2001/844/EC, ECSC, Euratom) for systems handling EUCI
- Appropriate security controls must be in place based on the system categorisation and, where required, a risk assessment

[9] This may not be necessary for existing systems which are already categorised and where neither the system nor the threat environment have changed materially since the previous evaluation.

- Performance and computer capacity requirements have been reviewed and analysed as necessary
- SECOPS and routine operational procedures have been documented (see section 8.1 above)
- Business continuity requirements have been analysed and are in place or planned (see the *Standard on Business Continuity Management*)
- Evidence exists that installation of the new system will not adversely affect existing systems, particularly at peak processing times
- If the operation, support or maintenance of the system is outsourced, appropriate contractual arrangements are in place (see section 10.1 above)
- Training in the operation and use of new systems has been planned
- Ease of use of the system has been considered, as this affects user performance and reduces human error

The acceptance criteria must be documented and formally accepted by the System Owner, the IRM and the LISO of the DG that owns the system, since they each have different responsibilities towards the Commission's IT systems.

For further information on system acceptance, see the *Standard on Secure Systems Development*.

12. ROLES AND RESPONSIBILITIES

System Owner: responsible for ensuring that the operational management procedures in this standard are applied. Also responsible for approving changes and for authorising new systems, together with the IRM and the LISO.

IRM: jointly responsible for accepting new systems, together with the LISO and the System Owner. Also in charge of the operational management of systems under his/her control.

IT Service Providers: responsible for operating IT systems and services in accordance with the requirements of this standard

LISO: responsible for accepting new systems based on their compliance with the Commission's security policies and for overseeing the secure management of the Commission's systems.

13. REFERENCES

Note that standards marked (*) are in draft at the time of writing of this standard.

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

- Implementing rules for Commission Decision C(2006) 3602 of 16.8.2006.
- Standard on Information Security Risk Management (*)
- Standard on Information Systems Security Incident Management (*)
- Standard on Back-up
- Standard on Secure Systems Development (*)
- Standard on Physical and Environmental Security
- Standard on Sanitisation of Media (*)
- Standard on Logging and Monitoring

14. RELATED DOCUMENTS

- International standard ISO/IEC 27001:2005
- International standard ISO/IEC 27002:2005