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

Brussels,
HR.DS5/GV/ac ARES (2014)
SEC20.10.05/04 – Standards (2013-2015)

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON COMPLIANCE

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON

Version 1.0 16/07/2014

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

Information systems of the Commission must operate in compliance with any relevant obligations deriving from applicable laws and contracts. This standard describes a number of measures that must be in place to provide assurance of compliance.

In some cases, the activities that must be performed to check compliance may themselves present a risk to information systems security. Consequently, this standard also contains rules for the performance of technical compliance checks and rules to be applied in case of audit activities..

3. OBJECTIVES

This standard provides instructions to ensure that the Commission's information systems comply with all relevant obligations, including those deriving from applicable laws and contracts. They are also intended to protect Commission information systems and related information from potential breaches of security caused by compliance checks or audit activities.

4. SCOPE[1]

This standard applies to all IT systems that are operated by or on behalf of the Commission, including applications, databases, software, servers, workstations,

[1] This section describes the functional scope of this standard. The organisational scope is defined in Commission Decision C(2006) 3602, Article 2.

network equipment and mobile computing devices. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials and other servants, contractors and third parties[2] who are responsible for developing, maintaining or operating Commission IT systems.

This standard includes measures that must be taken to protect against the accidental or deliberate misuse of computer-assisted audit techniques that could be used when performing audits activities.

5. THREATS COVERED

Since this standard concerns checks over all security measures, it covers all of the threats listed in the *Standard on Information Security Risk Management*.

6. TERMINOLOGY

Audit: an audit is an activity that is performed by the Internal Audit Service (IAS), the Internal Audit Capabilities (IACs), European Court of Auditors (ECA) or the European Data Protection Supervisor (EDPS). The performance of such audits is out of the scope of this standard, although this standard contains measures to protect systems and data from misuse of audit facilities.

Compliance check: in this standard, a compliance check is an activity that is performed under the authority of the System Owner to verify compliance with any kind of requirement, particularly security requirements.

Intellectual Property Rights (IPR): a set of rights granted to creators and owners of works that are the result of human intellectual creativity under intellectual property laws. Depending on the nature and effect of the creation, intellectual property law protects such works through legal instruments such as patents, trademarks and copyrights. Software is also protected by IPR.

Legal compliance: this means that the systems comply with applicable legislation and contractual obligations. Legal compliance helps to protect the Commission against potential legal claims actions and related risks (e.g. penalties for not respecting data privacy or IPR on software packages).

Legal compliance checks: procedures performed to ensure that an information system complies with all applicable legal requirements. These checks are based on a verification of the implementation of the legal requirements.

Technical compliance: this means that the systems comply with the Commission's security implementation standards and their own system-specific security measures, as described in the Security Plan.

[2] For third party personnel, compliance with the Commission's internal rules and regulations should be included in the contracts with the contractor.

Technical compliance checks: technical reviews that aim to verify the existence and effectiveness of the technical security measures that are required by the security policies or by the Security Plan. These may be performed in several ways. The choice between the different types of technical compliance checks is a balance between thoroughness and the risk of causing an unwanted system failure if they are performed on operational systems. More aggressive tests generally provide more concrete and detailed results. In order to reduce the risk of unplanned downtime, tests can also be performed during non-working hours or on mirror / test systems. The main methods are (in increasing order of aggression and effectiveness):

- **Review of system documentation and configuration**: for example, checking for compliance with an established baseline or reference configuration.

- **Vulnerability scan**: a method of evaluating the security of a computer system or network by testing for weaknesses that might be exploited by attacks from a malicious source. Vulnerability scans are largely performed using automated software tools, and are also commonly used to identify vulnerabilities that require patching[3].

- **Penetration test**, a method of evaluating the security of a computer system or network by simulating an attack from a malicious agent and trying to exploit weaknesses in the computing environment. Penetration tests are performed using a combination of software tools and human expertise.

7. BACKGROUND INFORMATION

This standard contains rules concerning compliance checks and audits, which are different and mutually exclusive activities. Compliance checks are performed under the authority of the System Owner, while audits are performed under the authority of the IAS, IAC, ECA or EDPS. The rules in this standard apply to the System Owner and are without prejudice to the mandate of any auditors, and in the event of a conflict the regulatory framework governing audit activities should take precedence.

The application of the Commission's security standards is mandatory[4] but not sufficient. In addition, the Commission's information systems must comply with all applicable laws and contracts. As well as being a legal obligation and part of the responsibility of due care, compliance will reduce the risk of penalties for non-compliance and reduce risks that are the focus of the laws in question.

This standard addresses two types of compliance:

[3] See the *Standard on Technical Vulnerability Management*.

[4] The standards adopted under the authority of Commission Decision C(2006) 3602 are mandatory for all information systems. Commission Decision 2001/844/EC, ECSC, Euratom and related documents are also mandatory for all systems handling EU Classified Information. See the appendices for further information.

- **Legal compliance**
- **Technical compliance**

The different sources of compliance requirements are described in more depth below.

Applicable Legislation

A list of the principal legal texts relating to information security in the Commission is given in Appendix I. Individual information systems may also be subject to additional legal requirements depending on the types of information held, the operations performed by the system, the jurisdiction(s) in which the system operates and any contractual obligations. There are a number of potential sources for such requirements at different levels. The different levels include:

- The Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) including the Protocols such as the Protocol on the Privileges and Immunities which also have a legal force at least equal to those of the Treaties, as well as all relevant acts of the Union, including, for instance, the Staff Regulations. All of these acts are interpreted by case law.

- Compliance with international laws and national legislation may be required, depending on the applicability of laws and regulations of the relevant Member States and third countries. The following areas of statutory and contractual requirements are particularly relevant:

    - Protection of personal data[5]
    - Cryptography
    - Intellectual property rights
    - Technical norms and standards[6]
    - Health and safety standards

Contractual Obligations

These are any specific obligations deriving from the agreements concluded on behalf of the Union with third parties.

---

[5] E.g. Regulation (EC) No 45/2001 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, OJ L 8, 12.01.2001, p. 1.

[6] Technical norms and standards may be mandatory or optional depending on the type of system and the applicable norms or standards. In particular, they may be required of systems that are operated by the Commission in partnership with other entities such as Member States' authorities.

Security Implementation Standards

Security implementation standards can be mandatory or voluntary[7]. The Commission has a set of mandatory standards which support Commission Decision C(2006) 3602, and which must be followed for all systems. Other standards may be made mandatory for individual information systems through specific policy decisions.

In addition, each System Owner may choose to follow other technical or organisational standards as relevant (where conflicts arise, the mandatory EC standards prevail).

System-specific Security Measures

Some of the Commission's information systems are required to have system-specific security measures, which are documented in the system's Security Plan[8]. These security measures are designed to reduce the specific risks of the system, and so failure to comply increases the likelihood of occurrence of identified risk scenarios.

For more information, see the *Standard on Information Security Risk Management*.

8. RULES ON LEGAL COMPLIANCE

Policy objective 10.1.1 – Identification of applicable legislation – All relevant statutory, regulatory and contractual requirements and the organisation's approach to meeting these requirements must be explicitly defined, documented and kept up to date for each information system and the organisation.

8.1. Identification of statutory, regulatory and contractual requirements

(1) The Commission's information systems and related processes must comply with applicable legislation, regulations and contractual obligations[9]. The System Owner must be familiar with the legal framework in which the system operates.

(2) In particular, all Commission information systems must comply with all applicable statutory and contractual requirements concerning areas that are governed by legislation (e.g. the protection of personal data, intellectual property rights and health and safety standards).

(3) The relevant statutory, regulatory and contractual texts must be identified and available for consultation.

---

[7] An example of voluntary standards is the ISO 27000 series of standards, which many organisations choose to follow as examples of good practice, although they are not legally required to do so.

[8] See *Commission Decision C(2006) 3602*, its *Implementing Rules* and the *Guidelines on Security Plans*.

[9] Some systems may have specific legislation or obligations towards third parties such as Member States. For example, the SIS and VIS systems are governed by their own specific Commission Decisions whose terms must be followed.

(4) Compliance requirements that may impact the security requirements in the areas of confidentiality, integrity and availability must be explicitly identified and documented in the IT security plan (see Appendix I for a list of laws that are applicable to all Commission systems). Those compliance requirements must be reviewed in the business impact assessment to identify the possible consequences of non-compliance. The organisation's approach to mitigate that risk must be defined and documented, and appropriate security measures implemented.

(5) In case conflicting requirements are identified, advice should be obtained from the Commission's legal services and this activity (both the request and the advice received) should be fully documented.

(6) As a consequence of the aforementioned constraints, there must be a periodic review of the legal obligations to ensure that they are up to date.

8.2. Intellectual Property Rights

Policy objective 10.1.2 – Intellectual property rights – Appropriate procedures must be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

(7) In relation to information technology, intellectual property rights (IPR) include software or document copyright, design rights, trademarks, patents and code licences (proprietary or open source). In a wider sense, it also covers areas such as music and video copyrights, logos, drawings etc. Intellectual property rights and the corresponding legal obligations must be respected.

(8) Software products are usually supplied under a license agreement that specifies license terms and conditions, for example, limiting the use of the products to specific machines or limiting copying to the creation of back-up copies only[10]. The IPR of software developed by or on behalf of the Commission must be explicitly covered by the contractual arrangements with the developers (the IPR should normally belong to the Commission)[11].

(9) Legislative, regulatory, and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organisation, or that is licensed or provided by the developer to the organisation, can be

[10] Note that open source software is also often protected by a General Public License, or similar, whose terms and conditions must also be followed.

[11] See, for example, the IPR clauses in the General Terms and conditions for Information Technology Contracts, which are applicable to all framework contracts concluded by DIGIT

used. Copyright infringement can lead to legal action which may include criminal proceedings.

(10) Measures must be taken to prevent IPR breaches, including:

(a) Acquiring software only through known and reputable sources to ensure that copyright is not violated

(b) Maintaining awareness of policies to protect IPR

(c) Maintaining appropriate asset registers (e.g. a software inventory; see the *Standard on Asset Management*) and identifying all assets with requirements to protect IPR

(d) Maintaining proof and evidence of ownership of licenses, master disks, manuals etc.

(e) Implementing controls to ensure that the maximum number of licensed users is not exceeded

(f) Complying with terms and conditions for software and information obtained from public or third party networks such as the Internet

(g) Ensuring that software is deleted and/or media destroyed if required at the end of a period of licensing

(11) Regular checks must be performed to ensure compliance with IPR requirements. These checks are a type of legal compliance check, and should be designed to cover issues such as the following:

(a) Checking installed copies of software against license numbers for authorised software on EC devices (including non-operational devices)

(b) Checking for unauthorised (unlicensed and/or unapproved) software

9. RULES ON TECHNICAL COMPLIANCE AND AUDITS

Policy objective 10.2.1 – Technical compliance checking – Information systems must be regularly checked for compliance with security implementation standards and with their own security measures.

Policy objective 10.3.1 – Information systems audit controls – Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimise the risk of disruption to business processes. Access to information systems audit tools must be protected to prevent any possible misuse or compromise.

9.1. Technical compliance checking

9.1.1. General Rules

(12) Technical compliance checking involves the examination of information systems by or on behalf of the System Owner[12] to ensure that technical controls have been correctly implemented. This type of compliance checking requires specialist technical expertise.

(13) Technical compliance checks must be performed periodically based on the security classification of the system, and the scope may be adjusted to cover different aspects in consecutive checks. A technical compliance check must be performed on any new system or major system upgrade before it is put into operation. Different types of technical compliance checks exist (see section 6 above), and the System Owner must decide which are the most appropriate.

(14) The scope of technical compliance checks must be related to the security requirements of the information system under review. The checks should be designed to verify the compliance of the system with its security requirements (including at least Commission Decision C(2006) 3602 and the associated documents[13]). An individual review may concentrate on a subset of security requirements, but all security requirements should be checked periodically (e.g. over a period of three to five years).

(15) Technical compliance checks must only be performed by authorised persons with appropriate qualifications.

(16) The results of technical compliance checks must be reported to the System Owner and to the LISO. Findings that show errors or omissions in an information system's implementation of security measures (as per the Commission's security policy or the system's security plan) must then be handled by the incident management procedure[14].

9.1.2. Rules for Penetration Tests

(17) Rules for penetration tests are given in the *Standard on Secure Systems Development* (§11.3). These rules must be followed whenever the technical compliance checks include penetration tests. The IT service provider and other affected stakeholders should be informed of the penetration tests.

---

[12] As opposed to an audit, as defined in section 6 above.

[13] Specifically, the Implementing Rules and the accompanying standards (of which this document is one).

[14] See the *Standard on Information Systems Security Incident Management*.

9.2. Security measures for information systems audits

(18) This section contains rules to protect information systems and data from any accidental or deliberate misuse of audit facilities such as access rights or automated audit tools. These rules do not cover and must not impede the audit activities themselves, which are not included in the scope of Commission Decision C(2006)3602.

(19) Audits are regularly performed on information systems for various purposes, including compliance with security standards as well as financial audits and internal control reviews. Audits can require a high level of access to systems and data, and software tools used for auditing can include powerful utilities that can bypass normal security controls.

(20) To limit the risk of security breaches caused either during audits or using audit tools, the following rules must be observed:

(a) The System Owner must review and address any potential security issues arising from audit requirements.

(b) The checks must be limited to read-only access to software and data, unless explicitly requested by the auditors and authorised by the System Owner.

(c) Resources required for performing the checks must be explicitly identified and made available.

(d) All access and use for audit purposes must be monitored and logged to produce an audit trail.

(21) To prevent unauthorised use, information systems audit tools must be given a level of protection that is appropriate to the risks relating to their potential for abuse. Appropriate protection may consist, for example, of highly restrictive access control lists to prevent unauthorised users from exploiting these tools.

(22) Credentials used by auditors must be disabled or revoked at the end of the audit fieldwork.

10. ROLES AND RESPONSIBILITIES

System Owners: ensures that their information systems and related processes comply with all relevant legal and contractual requirements as well as applicable security standards and policies. These responsibilities may be delegated, e.g. to the System Security Officer.

11. REFERENCES

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

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

Standard on Asset Management

Standard on Information Systems Security Incident Management

Standard on Information Security Risk Management

Standard on Secure Systems Development

Standard on Technical Vulnerability Management

12. RELATED DOCUMENTS

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

13. APPENDIX I – APPLICABLE LAWS

This appendix contains a list of the principal legal texts relating to information security in the Commission. These texts contain the basic legal requirements that are applicable to all of the Commission's information systems[15], wherever they are located or used.

This appendix contains some Directives which are not directly applicable to EU institutions, although they may become applicable through national law or through voluntary compliance by the Commission.

13.1. General laws with security implications

- Treaty on European Union & Treaty on the Functioning of the European Union – not specifically relevant for information systems, but these are the treaties upon which more specific Union law is based.
- Regulation No 31 (EEC), 11 (EAEC) laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union
- Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
- Commission Decision on Alert States and Crisis Management – Commission Decision 2007/65/EC of 15 December 2006

[15] The scope of some of the documents is restricted to a subset of systems, e.g. 844 only applies to systems handling EU Classified Information and 45/2001 only applies to systems handling personal data.

13.2. Laws related directly to information security

- Council Regulation on the protection of Euratom classified information – Regulation (Euratom) No3 of 31 July 1958
- Commission Decision on Tasks and Responsibilities of the Security Office – Commission Decision C(94)2129 of 8 September 1994
- Commission Decision on Information Security and amendments
    - Commission Decision of 29 November 2001 (2001/844/EC, ECSC, Euratom) amending its internal Rules of Procedure
    - Classification terms in "franglais" in all language versions – Commission Decision of 3 February 2005 (2005/94/EC, Euratom) amending Decision 2001/844/EC, ECSC, Euratom
    - The Commission Security Board – Commission Decision of 31 January 2006 (2006/70/EC, Euratom) amending Decision 2001/844/EC, ECSC, Euratom
    - Common minimum standards on industrial security – Commission Decision of 2 August 2006 (2006/548/EC, Euratom) amending Decision 2001/844/EC, ECSC, Euratom
- Commission Regulation on the application of Euratom safeguards – Commission Regulation (Euratom) No 302/2005 of 8 February 2005
- Commission Decision on the Security of Information Systems (see Appendix II)
    - Commission Decision of 16 August 2006 C(2006) 3602
    - Implementing rules adopted on 29/05/2009
    - Standards and Guidelines related to the Decision C(2006)3602

13.3. Laws on information protection and retention (including personal data)

- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive")
- Council and EP Regulation on the Protection of Personal Data (2001) – Regulation (EC) No 45/2001
- Council and EP Regulation on Public Access to Documents (2001) – Regulation (EC) No 1049/2001
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
- Commission Regulation on Access to Confidential Data for Scientific Purposes (2002) – Commission Regulation (EC) No 831/2002

- Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

14. APPENDIX II – COMMISSION DECISION C(2006) 3602

Commission Decision of 16 August 2006 C(2006) 3602 concerning the security of information systems used by the European Commission is the main piece of Commission legislation relating to the security of all information systems. It is supported by a number of supporting documents (including Implementing Rules, Standards and Guidelines). Information systems must comply with the rules given in all of these documents (the Guidelines are optional).

The Decision and all supporting documents are published on the website of the Security Directorate. System Owners should check the Security Directorate's pages on the Commission's Intranet for the latest versions of these documents.