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

Brussels, 30/09/2011
HR.DS5/GV/ac ARES (2011) 1039362
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON INFORMATION SYSTEMS SECURITY INCIDENT MANAGEMENT

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 30/09/2011

Version 0.10 20/09/2011

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

Whether accidentally or deliberately, events that could have a negative impact on information security occur frequently. From virus infections to equipment failures, human errors or hacking attempts, many different events can potentially breach the confidentiality, integrity or availability of EC information. This standard elaborates on Article 7, Security Incidents, of the Commission Decision C(2006) 3602 and the relevant policy objectives of its Implementing Rules (Annex 1, section 8).

With the appropriate controls in place as mandated by the Commission Decision C(2006) 3602 and its associated Implementing Rules and standards, many of these events should be prevented, detected and/or corrected by the systems and processes in place. Nevertheless, procedures must be in place to react swiftly and appropriately to incidents that require human intervention, and to address underlying causes or problems.

3. OBJECTIVES

This standard provides instructions for the essential elements that must be in place for the reporting of and response to events that may impact information confidentiality, integrity or availability. This is a broad definition since most ICT-related incidents have the potential to impact one of these three aspects of information security. Consequently, the standard also provides rules for determining the security relevance of such events so that they may be reported and escalated when appropriate, according to the risks involved.

4. SCOPE

This standard applies to all information systems, software, databases, networks and other Commission assets involved in handling or protecting EC information,

including but not limited to the following: servers, workstations, portable PCs, other portable computing devices (PDAs etc.), storage devices and network equipment. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties that handle EC information or computing assets.

5. THREATS COVERED

Security controls defined in this security standard will help to reduce the impact of all threats (see the *Standard on Information Security Risk Management*, Appendix B, for a full list of generic attack methods), since speedy and effective response procedures should help to mitigate the effects of security incidents.

6. TERMINOLOGY

Chain of custody: a formal record of the custody of evidence collected in the course of an investigation, used to avoid allegations of tampering or misconduct when the evidence is used during legal proceedings.

Event: A change of state which has significance for the management of an IT service; also an alert or notification of such a change of state.

Incident: Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. Specifically, an information systems security incident is an incident that entails a breach of the confidentiality, integrity or availability of EU information, or non-compliance with the Commission's security rules.

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.

Weakness: a lack or failure of an IT system or security countermeasure that could be exploited by a threat. Also sometimes referred to as a vulnerability (see the *Standard on Information Security Risk Management*, particularly section 3.2 of the annex, for more explanation of vulnerabilities).

7. BACKGROUND INFORMATION

7.1. Security Incidents and Weaknesses

This standard describes the measures that must be in place to respond to information security related incidents and identified security weaknesses, and to that end it is important to clarify what constitutes such an incident. Security incidents often differ from other incidents in a number of key areas that can make them especially sensitive, for example:

- They may be caused by deliberate acts, and therefore represent a significant threat to the organisation.

- Their impact may be far greater than simply the cost of remediation
- They may lead to legal processes, and therefore require careful handling and collection of evidence.

If unaddressed, a security incident may lead to further incidents or consequences, for example if a malicious agent has gained access to the organisation's systems

Examples of information systems security incidents may include:

- Virus infections
- Loss of service, equipment or facilities
- System hardware or software malfunctions or overloads
- Human errors
- Non-compliance with policies or mandatory security measures
- Breaches of physical security measures
- Uncontrolled system changes
- Access violations

Security weaknesses should be reported so that action can be taken to prevent threats that might exploit them. Examples of information security weaknesses may include:

- Virus software pattern files not updating on workstations
- Operating systems not being updated with security patches or fixes
- Physical security weaknesses such as non-functional locks or broken windows
- Problems with environmental controls such as malfunctioning air-conditioning systems
- Insufficient segregation of duties in application access control
- Known weaknesses or bugs in application software
- Insufficiently complex passwords
- Non-compliance with mandatory security procedures

7.2. Determining security-relevant incidents

Taking a broad definition of information security, most information system incidents can be classified as security incidents since, for example, many of them have an actual or potential impact on availability. However, it is not

necessary to treat all incidents in the same way, and this standard is intended to be applied only to incidents which are particularly security-relevant. These should be a small proportion of the total number of IT incidents.

Criteria for determining security-relevant incidents are given in section 9.1 of this document, and some examples are given in Appendix I.

7.3. Evidence

Collection of evidence concerns the forensic investigation of security incidents. The methods used in collecting evidence may vary according to the intended use of the evidence. For example, different levels of proof, and hence rigour in the investigation, are required for internal investigations compared to preparation for legal cases.

It will probably not be necessary to collect evidence for most security incidents, other than what is needed to solve the problems encountered. However, the European Commission must be prepared to collect evidence in a formal and structured way when required.

Typically, the types of evidence that may need to be collected for an information systems security incident include:

- Computer hardware
- Information media (hard disks, floppy or optical disks, USB sticks or memory cards etc.)
- Event logs (such as PC or network logs, Internet activity logs from proxy servers etc.)
- Video tapes or files from surveillance cameras
- Paper documents

8. REPORTING SECURITY EVENTS AND WEAKNESSES

Policy objective 8.1.1 – Reporting information systems security events – Information systems security events must be reported through designated channels as quickly as possible. In the case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data processed by Commission information systems, the system owner needs to inform the Data Protection Officer.

Policy objective 8.1.2 – Reporting security weaknesses – All employees, contractors and third-party users of information systems and services must be required to note and report any observed or suspected security weaknesses in systems or services through designated channels.

8.1. Reporting information systems security events

A formal information systems security incident reporting procedure must be in place together with an incident response and escalation procedure. A point of contact must be established within each organisational unit (e.g. DG) for the reporting of information systems security incidents. This point of contact must be known throughout the organisation, must always be available during the specified hours of operation and must provide adequate and timely response, with logging of the incident.

All users[1] must be made aware of their responsibility and the procedure for reporting any information systems security incidents as quickly as possible. Past or realistic incidents should be used as examples in user awareness efforts.

The reporting procedure must include:

- Instructions for reporting incidents and weaknesses (see section 8.2 below).
- Instructions on the correct behaviour in the event of an incident or weakness, such as noting all important details and not attempting remedial measures but reporting the incident straight away.
- Feedback processes to ensure that the user is appropriately informed of the outcome of the reported incident or weakness.

Malfunctions or other anomalous system behaviour may be an indicator of a security breach and should therefore always be reported.

The security incident reporting procedure must include the following elements:

- A way to determine whether the incident or weakness is security related (see section 9.1 below)
- Systematic notification of all security-relevant incidents and weaknesses to the Local Information Security Officer
- Notification to the Data Protection Officer in case of an incident relating to personal data
- A procedure for determining security incidents and weaknesses which must be reported to the Security Directorate and to the superior of the LISO.

All security-relevant incidents must be formally recorded and followed up as described in section 9 below. Security incidents involving EU Classified Information must always be reported to the Security Directorate.

[1] See the *Standard on Human Resources Security* for more information on the different categories of users of EC information systems.

Security incidents that are reported directly to the Security Directorate may be investigated directly, or they may be passed to the relevant service in DIGIT or other DG for appropriate action.

8.2. Reporting Security Weaknesses

A formal information security weakness reporting procedure must be in place, with a point of contact that must be known throughout the organisation, must always be available during the specified hours of operation and must provide adequate and timely response, with logging of the incident.

All employees, contractors and third party users must be made aware of their responsibility and the procedure for reporting any information security weaknesses as quickly as possible. Realistic weaknesses should be used as examples in user awareness efforts (see examples in section 7.1 above).

The reporting procedure may be the same as that used for reporting information systems security incidents, and must include the same elements (see section 8.1 above).

All security weaknesses must be formally recorded and followed up (see section 9.1 below).

9. MANAGEMENT OF SECURITY INCIDENTS AND IMPROVEMENTS

Policy objective 8.2.1 – Responsibilities and Procedures – Information systems security incidents must be managed to ensure a quick, effective and orderly response. Procedures must be established to recover from an incident.

Policy objective 8.2.2 – Learning from Information Systems Security Incidents – Mechanisms must be in place to enable the type, volume and cost of information systems security incidents to be quantified and monitored. This information gathered about incidents must be used, either to indicate the need for additional or improved security measures against future recurring or high-impact incidents, or to assist in the information systems security review process.

9.1. Processing security incidents

A formal process including responsibilities and procedures for handling security incidents and weaknesses must be in place and fully documented.

Security incidents and weaknesses cover a wide range of possible events, and may be raised by users notifying a helpdesk or through regular systems surveillance activities (see for example the *Standard on Logging and Monitoring*). The documentation of the security incident management process must include an analysis and categorisation of incidents[2], with an analysis of the impact on Confidentiality, Integrity and Availability and an

[2] The document "Categorisation of Incidents" issued by DIGIT on 19/11/2010 may be of use for guidance.

identification of the security countermeasures related to the incident in order to identify any vulnerabilities.

The basic criteria for determining whether an incident is security-relevant are given below. These criteria cannot cover all cases, and it is the responsibility of the helpdesk or support staff to whom the incident is assigned in order to determine whether each incident is security-relevant and whether it needs to be reported or escalated as described later in this section.

Incidents must be considered as security-relevant if one or more of the following conditions apply[3]:

1. The incident has already caused a measurable security impact (e.g. loss of integrity or confidentiality of EU Classified Information)

2. The incident has the potential to directly cause a significant impact to the security or reputation of the Commission, or a significant financial cost

3. The incident is related to Confidentiality, Integrity or Availability, and cannot be remedied by existing countermeasures or standard incident response procedures

4. The incident has particular organisational or political significance (e.g. when it may have a negative effect on other organisations or member states)

5. The incident, if unchecked, is likely to lead to further, more serious security-related incidents

6. The Commission may need to take disciplinary or legal action against the perpetrator

Categorising incidents will also help in compiling statistical reports. A number of incident categories must be defined, such as:

- Information systems failure and loss of service
- Malware (viruses etc.)
- Denial of Service
- Unauthorised access
- Breaches of confidentiality and integrity
- Misuse of information processing facilities
- Errors resulting from incomplete or inaccurate data

[3] Some examples of potential security-relevant incidents are given in Annex I.

Incidents must be classified in order to help to determine and prioritise the incident response, and define the response timeframes. The classification method may be chosen to suit the organisation, but will typically include elements such as the impact, urgency, severity or priority.

The incident handling process must cover all of the following core elements:

- Organisation and responsibilities: who is responsible for reporting, recording, responding, escalation, taking corrective action, approving actions, informing affected staff, approving closure etc.

- Clearly defined reporting and escalation paths and criteria (see below)

- Contact procedures and availability: contact points must be provided for both internal and external parties, and users must be able to report incidents 24 hours a day (although the response timeframes will depend on the system's service window and availability requirements). Reporting facilities may include a dedicated email box, phone number, web application etc.

- In the case of service outage, the potential duration must be estimated and a procedure to trigger business continuity plans available if this exceeds the acceptable limit.

- Tools and other resources that may be required (e.g. information sources, system documentation, blank media, laptop with diagnostic software…).

- Procedures for the detection, analysis, containment and remediation of the different categories of incidents, including guidelines on actions that are recommended or forbidden. It is not permitted to launch counterattacks against a hacker.

- Communication plans with contact details and procedures (where relevant) for internal and external parties that may be involved in incident management (e.g. the Security Directorate, DIGIT, network providers, the EC spokesman service, local authorities…).

- Documentation procedures: all steps taken must be recorded in detail in an incident record, including the name(s) of people involved, dates/times and actions taken. Evidence may need to be collected and stored, particularly for deliberate attacks (see section 10 below).

- Review of actions taken, particularly in emergency circumstances where actions must be taken without prior planning or approval.

- Formal sign-off for closure with interested parties where relevant, such as the person reporting the incident, the Local Information Security Officer, the Systems Manager, the Security Directorate and the system owner.

- Review of incidents with a view to improving resilience or incident response procedures (see section 9.2 below).

- Any relevant legal considerations (for example, the Data Protection Officer must give authorisation before starting an investigation involving personal data).

The incident handling personnel must have good knowledge of the networks, systems and applications involved, and be familiar with their normal behaviour so that they can recognise abnormal behaviour. The incident management process must therefore include regular reviews of logs and statistics and any other pertinent information, and staff must be selected with very good technical knowledge and analytical skills.

The reporting and escalation procedure must be clearly defined in the process. Criteria must be determined and documented for the reporting and escalation from the LISO to the Security Directorate.

The LISO must report security-relevant incidents to the Security Directorate when they meet one or more of the following criteria:

1. The incident concerns EU Classified Information

2. The incident has the potential to cause a high impact to the security or reputation of the Commission, or a high financial cost

3. The incident has a high organisational or political significance

4. The incident cannot be remedied by the DG's own resources

5. The incident requires specialist, forensic or judicial investigation (e.g. when the Commission is likely to take disciplinary or legal action)

The LISO may also report other incidents that do not meet these criteria, based on his or her own judgement. The Security Directorate will decide whether to investigate incidents that are reported to it.

When incidents are investigated by the Security Directorate, it has the authority to take actions including stopping the system or preventing access to it (e.g. blocking Internet access). Staff in the DG where the incident occurred (including the LISO) must not take any further investigatory or remedial actions without instructions from the Security Directorate. The LISO must support the Security Directorate in the investigation as directed.

The Security Directorate may, at its own discretion, escalate incidents to external parties such as CERTs or other authorities, local police, or suppliers.

9.2. Learning from Security Incidents

A process which includes the elements below must be in place for the review of information systems security incidents to enable the organisation to improve its controls for the prevention or remediation of such incidents in the future.

Regular meetings must be held by interested parties such as the Systems Manager, the Local Information Security Officer, the head of the Incident Response team and any other relevant persons to review recent incidents. The goals of these meetings are to identify ways to improve the existing security controls or processes in order to prevent or reduce the impact of future incidents.

Statistics on incidents must be prepared to assist in this review, analysing them by characteristics such as category, severity and cost.

Incident records must be reviewed for issues such as:

- Specific weaknesses that are not adequately controlled
- Recurring incidents indicating an underlying weakness (e.g. inadequate patch management)
- Errors or inadequacies in the response procedures
- Missing tools or resources for proper incident management

The issues identified may lead to potential improvements in areas such as:

- Updating the Commission's information systems security policy and related standards
- Adding or reinforcing preventive or detective security measures
- Amending business processes to make them more resilient in case of security incidents (particularly system unavailability)
- Improving response procedures
- Acquiring additional competences (personnel, training, information sources etc.)
- Acquiring additional hardware or software

10. COLLECTION OF EVIDENCE

Policy objective 8.2.3 – Collection of Evidence – Where follow-up action against a person or organisation after an information systems security incident involves an investigation, evidence must be collected upon request of the Security Directorate whereby the collection of digital evidence must respect a computer forensic protocol.

10.1. General rules

NB Most security-related incidents do not require forensic evidence to be collected, and can be resolved through the standard incident management processes. The procedures described in this section only

apply when evidence must be collected for detailed analysis or for potential action against the perpetrator of the incident.

This control objective is intended to describe a procedure for the collection of evidence primarily for internal purposes. It does not, therefore, specifically mandate a level of rigour in evidence collection that is suitable for criminal investigations or other investigations for legal purposes, although serious security incidents can lead to law suits, and so the procedure for the collection of digital evidence must follow a computer forensic protocol.

Evidence collection procedures must comply with appropriate legislation. In particular, evidence collection must respect the provisions concerning data privacy (Regulation (EC) No 45/2001 on data protection) which can easily be breached by investigations, causing the evidence to be unusable and potentially causing legal issues for the Commission and/or its staff.

The IT staff involved in the implementation of this control must be made aware of the best practices governing the collection of evidence so that, when necessary, they can safely collect usable evidence[4].

10.2. Collection of evidence for security incidents

As described in section 8.1 above, some security incidents must be reported to the Security Directorate. At its own discretion, the Security Directorate may decide to perform an investigation (NB all incidents involving EU Classified Information will be investigated, as stated in Commission Decision 2001/844/EC, ECSC, Euratom).

If the Security Directorate decides that the investigation is to be performed as a formal investigation, then stricter rules must be observed for the gathering and retention of evidence (see section 10.3 below). A formal investigation may only be launched with the specific agreement of the Director-General of the Directorate-General for HR and Security, and after consulting the Data Protection Officer.

After the arrival of the investigating team, the LISO may be involved as the contact point between the team and the user organisation, and should assist the team as required.

The person assigned to lead the investigation must have the required level of training and awareness to collect and store the evidence while respecting data protection rules. A key example is the capture of snapshots of systems as early as possible in the investigation process. Snapshots can be useful both for evidence and for analytical purposes (it is best to take separate copies for the two purposes), and staff must be capable of capturing system data, particularly from volatile media, with as little impact as possible on the data being collected.

[4] RFC 3227 "Guidelines for Evidence Collection and Archiving" provides guidelines for the collection of evidence that may be useful.

Detailed notes must be made during the investigation, including dates and times, and documenting all steps taken and results found.

The evidence to be collected is likely to include relevant log entries. The level of logging performed as standard is covered in the *Standard on Logging and Monitoring*. Additional logging facilities may be activated as required during an investigation in order to capture additional evidence. This additional logging is to be defined ad hoc by the officers involved in the investigation. The system time on computers that logs are taken from should be checked, and any variance from the Commission's standard time[5] noted.

Evidence such as logs, computer hardware or copies of media / memory status is only to be collected during specific investigations for explicit purposes.

Evidence must be stored safely for the duration of the case and then kept for a period that is sufficient for facing possible further legal cases. Evidence that is collected is owned by the investigating team, and should be classified at an appropriate level.

10.3. Formal investigations

If the incident requires formal investigation then stricter procedures must be applied to evidence that is collected in order to maximise its legal value. In this case, the rules in section 10.2 above must be followed closely, as well as the following:

- All staff actively participating in the collection and analysis of evidence must be adequately trained and qualified.
- Access to EU Classified Information in the context of a formal investigation must be given in accordance with the rules governing such information.
- A formal protocol must be followed for the computer forensic investigation.
- Where possible, investigations should be carried out by two members of staff – one person performing the procedures and the other documenting all actions taken.
- Where computer media are collected as evidence, they should be copied and preserved in their original state, and the analysis performed on copies.
- Evidence logs must be kept to document all evidence that is collected and all actions performed with the evidence (collection, examination, analysis etc.).

[5] See the Standard on Logging and Monitoring, section 11 – Clock Synchronisation

- Chain of Custody forms must be used to record who has custody of the evidence and where it is located at all times from the moment of collection. This increases the assurance that pieces of evidence have not been tampered with during the investigation.

11. ROLES AND RESPONSIBILITIES

System Owners: responsible for overseeing the resolution of security incidents and weaknesses.

IRMs: responsible for defining operational procedures and resolving security incidents; also responsible for collaborating with formal investigations as required.

LISOs: responsible for controlling procedures and overseeing responses to security incidents and weaknesses; also responsible for collaborating with formal investigations as required.

IT Service Providers: responsible for providing information and resources to the System Owner, the LISO and other authorised investigators.

Security Directorate: responsible for providing guidance on all special cases upon DG's request, and for conducting formal investigations. Also responsible for maintaining tools and detailed procedures for formal investigations.

DIGIT: responsible for managing security incidents in cooperation with the Security Directorate.

12. 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.

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

- Standard on Information Security Risk Management (*)

- Standard on Logging and Monitoring

- Standard on Human Resources Security (*)

- Regulation (EC) No 45/2001 on data protection

13. RELATED DOCUMENTS

- Security Notice 15, Handling & reporting breaches of security and compromise of EU Classified Information (01/06/2005)

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

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

- International standard ISO/IEC 18044:2004

- RFC 3227 Guidelines for Evidence Collection and Archiving

- NIST SP 800-61 Computer Security Incident Handling Guide

- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response

14. APPENDIX I – EXAMPLES OF POTENTIALLY SECURITY-RELEVANT INCIDENTS

The following table lists some examples of incidents, and indicates whether each incident should be considered as security-relevant.

Table 1 – Examples of potentially security-related incidents

Incident Description	Applicable Conditions[6]	Escalation required?
A virus or spam mail is received, and is detected and eliminated by the existing automated tools (anti-virus & anti-spam software)	None	No
A virus is received and detected by the anti-virus software, but cannot be cleaned	2, 3, 5	Yes
Generic phishing attacks are received by users (e.g. purporting to be from a bank and requesting users to log into a fake website)	None	No
Targeted phishing attacks are received, e.g. aimed at specific people within the Commission and/or including EC information	4, 5	Yes
An alert is raised indicating likely imminent equipment failure (e.g. a hard disk)	None	No
An equipment failure has caused a temporary outage of a non-critical system	None	No
An equipment failure has caused a temporary outage of a critical system	1	Yes
A user has forgotten his or her password and requests a reset	None	No

[6] This column refers to the list of conditions above the table. If one or more of the conditions applies, then the incident should probably be classed as security-relevant.

Incident Description	Applicable Conditions[6]	Escalation required?
A user reports that someone else appears to have used his or her login credentials	2, 5, 6	Yes
A user reports the theft of a portable computer containing sensitive information	2	Yes
A user reports the loss or theft of a Director General's smartphone	4	Yes

It can be seen from the examples above that the decision whether the conditions mentioned are applicable is not always straightforward. In case of doubt, the LISO should be consulted for advice.