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

Brussels, 27/09/2010
HR.DS5 ARES (2010) 630327
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON LOGGING AND MONITORING

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 27/09/2010

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

Preventive controls can go a long way in assuring the security of information and systems, but they cannot guarantee absolute security. Systems must also be supervised to check whether information security breaches have taken place so that corrective measures can be taken. This supervision is performed through logging and monitoring.

Information systems used by the Commission must record at least the basic information security-related events in logs so that they can be monitored in (near) real-time and/or reviewed after an incident has occurred. In many commercial sectors there are legal and regulatory requirements to perform information security logging and to retain the logs for specific periods.

3. OBJECTIVES

This standard provides mandatory instructions for the procedures to be used for logging and monitoring on all types of computer systems that are capable of generating information security-related log events, including servers, network equipment, workstations and mobile devices. Its aim is to ensure that a sound minimum of logging and monitoring is performed consistently across the Commission, without incurring unreasonable costs or administrative burdens.

4. SCOPE

This standard applies to all computer systems, 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 personnel and contractors.

5. THREATS COVERED

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

T12 – Loss of power supply

T13 – Failure of telecommunication equipment

T25 – Tampering with hardware

T26 – Tampering with software

T28 – Equipment failure

T29 – Equipment malfunction

T30 – Saturation of the information system

T31 – Software malfunction

T33 – Unauthorised use of equipment

T36 – Corruption of data

T37 – Illegal processing of data

T38 – Error in use

T39 – Abuse of rights

T40 – Forging of rights

T41 – Denial of actions

6. BACKGROUND INFORMATION

Many computer systems have functions to record significant events in log files in order to preserve a record for various purposes. The three main goals of logging are:

- Accounting – the process of collecting and recording information about events
- Audit – the systematic, independent and documented process for obtaining audit evidence and evaluating it objectively
- Monitoring – pro-actively monitoring systems for information security incidents

Logging functions are found in different types of IT systems, at both the operating system and the application level[1]. Many different types of events may be recorded, such as:

- Device start-up and shutdown
- User logins and logouts
- Processes starting and stopping
- Resource utilisation (e.g. processor, memory, disk space)
- Hardware and software failures
- Configuration changes
- Modification of sensitive data, particularly user privileges
- File access

Many, though not all, of these events are relevant to the confidentiality, integrity or availability of the information and systems, and so these events may need to be recorded and potentially monitored and/or used for forensic or diagnostic purposes.

Logs may be used for various purposes, including:

- Troubleshooting system or network problems
- Capacity planning
- Fulfilling legal or regulatory requirements
- Enabling audits to be performed
- Detecting and investigating information security incidents

Consequently, it is important that relevant events are logged. This standard focuses on information security issues, which mostly concern the last two purposes cited above although all are pertinent to different aspects of information security (e.g. capacity planning is relevant to system availability).

Logs may simply reside on a system until they are required for investigations; additionally, they may be monitored by human operators or automated systems in order to provide (near) real-time alerts of significant incidents. There is a wide variety of different ways in which this monitoring is performed, depending on factors such as the purpose, the technical environment, the options available and the cost. Sophisticated systems are available that collect and centralise log entries from many different devices, and can analyse these events to detect information security

[1] The terms "operating system" and "application" are intended to be taken in the widest possible sense and not to be defined precisely.

incidents that affect multiple systems (such as a virus outbreak or a hacker who is attacking several computers).

It is important to note that this standard focuses on information security, and that additional logging requirements may exist for other purposes; consequently, this standard may not be the sole source of logging requirements for any particular system.

7. TERMINOLOGY

Alert: An alert is a message that is sent to a system or a person as a notification of a significant event that may require immediate attention.

Audit: The systematic, independent and documented process for obtaining evidence of the performance of operational procedures and evaluating it objectively.

End user devices: This term is used in this standard to indicate any computer devices that are used directly by end users. These include fixed workstations, portable PCs, PDAs, smartphones and other similar devices. The term "Non-personal devices" is used in this standard to mean all other computer devices.

Event: An identifiable action that happens on a device and is recorded in a log entry. Typical events include an action taken by a user (such as logging onto the device), an automated action (such as the results of a scheduled job), a detectable hardware or software event (such as a hard disk failure) or an external input (such as a network port scan).

Host-based firewall: See Personal Firewall.

ICT: Information and Communication Technology.

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.

Local firewall: See Software Firewall.

Log: A generic term that can mean a single log entry or the whole logging process or file.

Log Entry: A record of a single event. Log entries are normally held in logfiles but may also be sent to remote systems (e.g. as an SNMP trap or a SYSLOG record that is sent to a central logging server).

Logfile: A file on a computer system containing log entries.

Monitoring: The process of pro-actively checking systems for information security incidents, normally by checking log messages and/or periodically verifying that the system is responding.

Network Firewall: A network firewall acts as a gateway between different networks blocking unauthorised access while permitting authorised communications.

Non-personal devices: Computer devices that are not used directly by end users, including application and database servers, authentication servers, firewalls, Intrusion Detection Systems, network devices etcetera.

PDA: Personal Digital Assistant, a small, hand-held computer.

Proxy server: a server that receives and forwards application requests across networks. Proxies can serve several purposes, including filtering for invalid, undesirable or malicious requests; caching data; anonymising requestors; scanning for viruses; applying encryption; logging requests etc. A 'Forward Proxy' is normally a proxy server that handles requests going outside a corporate network (e.g. for Internet browsing); a 'Reverse Proxy' handles incoming requests, e.g. to corporate web application servers.

Smartphone: a mobile telephone with additional functionality like a PDA.

SMTP Server: a server that sends and/or receives electronic mail messages using the Simple Mail Transfer Protocol (sometimes also called a *mail relay*).

SNMP: Simple Network Management Protocol, a standard protocol for monitoring computers across a network.

SNMP Trap: A message sent by a managed device, equivalent to a log entry. The message types TRAP and INFORM exist in SNMP but are normally referred to as SNMP Traps.

Software Firewall: A firewall that is installed on an end-user device or an application server in order to provide an additional layer of security. Also called a *host-based* or *personal firewall*.

SYSLOG: A standard for forwarding log messages in an IP network. SYSLOG messages are often collected and stored in centralised SYSLOG servers, where they may be further collated and analysed.

UTC: Coordinated Universal Time, the principal international standard for time (closely related to GMT).

8. AUDIT LOGGING

Policy objective 5.10.1 – Audit logging – Audit logs recording user activities, exceptions and information systems security events must be produced and kept for an agreed period to assist in future investigations or access control monitoring in accordance with Regulation (EC) No 45/2001 on data protection.

8.1. Minimum Requirements

Audit logs must be configured to record significant information security-relevant activities and events in the Commission's ICT systems. When information systems or devices are being selected or developed for use within the Commission, the logging and monitoring rules must be included as information security requirements.

Log entries must contain at least the following information for each event, where available:

- user ID
- event date and time
- terminal identity (e.g. name and/or IP address)
- event-related information (message or code)
- event success or failure indication.

Log entries should not include unnecessary data in order to keep logfile sizes manageable.

Whenever log entries are transmitted across a network (e.g. to a remote monitoring or archiving device), the protocol used should be selected carefully to ensure compatibility and security.

The minimum retention period for all log files is six months. The System Owner should determine whether logs need to be retained for a longer period, based on a risk assessment that takes into account audit, legal and regulatory, evidentiary or other requirements. Care must be taken to ensure that log events are not lost due to maximum logfile sizes being reached.

Audit logs must be protected against unauthorised access (see section 10 below). Where personal data are involved, the logs must be handed according to the procedures in Regulation (EC) No 45/2001 on data protection.

Adequate procedures must be in place to ensure that logging and monitoring controls are operating effectively, and periodic spot checks must be carried out to ensure that events are being logged properly.

8.2. Events to be logged

This section details the minimum set of events that must be logged on different types of computer devices or applications.

Some of the categories below may be either dedicated devices or software running on systems that are multifunctional (e.g. an application server with a local firewall). The same logging rules must be applied in both cases.

The first table below lists the types of events that must be logged on all devices, irrespective of their function. The first part of the table details requirements for all devices (both end user devices and non-personal devices), and the second part details additional requirements for non-personal devices.

Table 1: Log requirements for all devices

Device Type	Required Logging
All devices	• Successful and failed logon attempts • Logout events • Alerts raised by the access control system • Activation and deactivation of protection systems (e.g. firewalls, intrusion detection systems or anti-virus software) • Events raised by protection systems • Initialisation, modification or deletion of audit trails • User account creation, modification or deletion
Non-personal devices (additional requirements)	• Starting / stopping processes (services, daemons etc.) • Changes to system configuration • Use of privileges • Errors and exceptions • Alerts raised by changes in environmental conditions (high temperature, rack door opening etc.)

The next table shows logging requirements for specific functions that must be applied **in addition** to the generic logging requirements in Table 1 above. These functions may be implemented on dedicated machines (such as network firewalls) or as software components on multifunctional devices (such as a firewall function or anti-virus software on an application server).

Table 2: Log requirements for specific functions

Device Type	Required Logging
Network firewalls	• Firewall traffic and other logs. Since logging on network firewalls is a particularly complex and sensitive topic, this is covered in detail in section 8.4 below.

Device Type	Required Logging
Personal firewalls	• Network traffic to and from the host computer as defined by the system owner (no specific requirements but see section 8.4 below for rules on network firewalls) • Administrative logins • Configuration changes • Firewall service start-up & shutdown
Intrusion detection / prevention systems	• Information security events to be determined during device configuration[2]
Authentication servers	• Authentication requests, including username and originating application/server
Proxy servers	• Proxy requests including results (accepted / rejected + reason etc.)
Anti-malware software	• Virus definitions and software updates • Manual scan launches and results • Malware incidents Note that these log events must be recorded at a central console or log aggregation device.
Remote access software	• Remote user logins & logouts • Registration, modification or deletion of user access tokens (where used)
Vulnerability management software	• Scans for updates • Successful or failed installation of updates
Routers and switches	• [No additional requirements]
Application software[3]	• As per the section above on "Non-personal devices" but at the application level • Changes to sensitive application data

[2] IDS/IPS log contents are too complex and proprietary to be detailed in this standard.

[3] Application software includes all business-related software and middleware, including Enterprise Resource Planning systems, database systems, presentation software etc.

8.3. Systems classified as SPECIFIC

The logging requirements shown above apply to all systems. Additional requirements may be applicable for systems that have high Confidentiality, Integrity or Availability requirements. Any system whose security requirements are classified as SPECIFIC[4] must have a documented logging policy and may require additional logging and monitoring controls. The logging policy should be based on the results of the system's information risk assessment.

The logging policy must cover the relevant information security requirements, and the relevant controls that must be implemented. Additional controls may include items such as the following (non-exhaustive list):

- Longer log retention periods
- Increased operating system logging
- Logging changes to all or specific application data
- Availability monitoring
- Higher level of alerting
- More frequent log reviews
- Log stores designed for forensic use (i.e. to preserve logs as legally valid evidence)

The level and type of controls will depend on many factors, such as the accessibility of the system from the outside world (and hence its vulnerability to attack).

Where logs are required to be manually reviewed, the period and event types to be reviewed must be specified in the logging policy (it may not be necessary to review all logged event types).

Additional auditing requirements may also be appropriate.

8.4. Network firewalls

Network firewalls present specific challenges regarding event logging due to a number of factors including their complexity, the quantity of logs generated and their critical position as key security devices. Firewall logs are very useful for network troubleshooting and for forensic investigations,

[4] See Commission Decision C(2006) 3602, Annex I, section C.

but the quantity of logs generated (especially on Internet-facing firewalls) can be extremely difficult to manage[5].

Consequently, this section provides rules on some specific events that must be logged, and other events are not required to be logged. Note that this standard does not cover the firewall rules themselves, but only the logging option (which is typically a single element of each firewall rule).

The following traffic types must always be logged:

- All authentication requests (successful and failed)
- All VPN session requests (successful and failed)
- All packets denied by specific rules and by the "clean-up" rule[6]
- All successful packets whose destination is the firewall itself (firewall management traffic)

The following traffic types are not required to be logged for the purposes of this standard, since they are generally not significant for information security purposes[7]:

- Successful outbound FTP, HTTP and SSL packets from recognised proxy servers on standard ports (TCP ports 21, 80 and 443)
- Successful electronic mail requests to and from recognised email systems or mail relays
- Successful packets passing between internal unclassified IT security zones

Any decision not to log other types of traffic must be documented and justified.

In addition to the traffic logs, firewalls must log all events mentioned under "Non-personal devices" in table 1 above. In particular, all firewall ruleset modifications must be clearly logged.

---

[5] Issues relating to firewall logs mainly relate to very large volumes that are difficult and expensive to store and/or transmit to log aggregation devices. Large firewalls can generate millions of log entries, most of which are not significant and can be hard to process even with automated audit or analytical tools.

[6] The "clean-up" rule is normally the last rule in a firewall rulebase that blocks all traffic not covered by a previous rule. Often its only purpose is to specify logging options for this traffic, since by default many firewalls will block unmatched packets without logging them.

[7] Naturally, there may be exceptions to this rule. For example, a firewall administrator may wish to log packets going to specific domains for security or other reasons, such as troubleshooting connection problems.

8.5. Personal Data

Logging and monitoring activities must be operated in compliance with regulation (EC) No 45/2001 on data protection[8].

In case of any doubts arising during the application of this rule, the DPO and/or DPC should be consulted and this process and the eventual decision documented.

9. MONITORING SYSTEM USE

Policy objective 5.10.2 – Monitoring system use – Procedures for monitoring use or faults in information processing facilities must be established and the results of the monitoring activities reviewed regularly in accordance with Regulation (EC) No 45/2001 on data protection. When necessary, appropriate action must be taken.

9.1. General rules

The EC's applications and network environments must be monitored to ensure that threats are identified and alerts must be raised promptly.

Specifically, the following systems must be monitored:

- Firewalls (both network and host-based)
- Any other gateways to other networks
- Intrusion Detection / Prevention Systems
- Authentication servers

Application and database servers must be monitored for changes to privileges.

Monitoring systems must have the capability to aggregate and analyse information security incidents affecting multiple systems. Alerts must be sent automatically to system administrators so that they can react to potential threats.

Events monitored must include at least the following:

- Unauthorised access attempts such as:
    - Failed or rejected user logins or other actions

[8] Note particularly paragraph 30 of this regulation, which states: "It may be necessary to monitor the computer networks operated under the control of the Community institutions and bodies for the purposes of prevention of unauthorised use. The European Data Protection Supervisor should determine whether and under what conditions that is possible."

    - Critical notifications from network firewalls or gateways such as dropped traffic on specific rules (e.g. firewall management rules)

- System alerts or failures such as:
    - Console alerts or messages
    - System log exceptions
    - Network management alarms
    - Alarms raised by the access control system
    - System capacity alerts
    - Key Performance Indicators
- Changes to, or attempts to change, system security settings or controls

Particular attention should be paid to monitoring of systems that have been infiltrated, compromised or misused in the past, and to systems that are exposed to high risks (for example, systems that can be reached from the Internet).

Alerts raised by the monitoring system must be analysed and, where relevant, recorded as incidents in the Incident Management system and formally followed up[9]. If the monitoring system produces too many alerts to follow up in this way, this must be investigated in order either to better tune the monitoring system or to address the root cause of the events. The monitoring process and systems must be reviewed regularly to ensure that they are performing adequately and not suffering from too many false positives or false negatives.

Staff responsible for operating and/or responding to monitoring systems should be segregated from staff who use or administer the systems in the course of their normal duties.

As for logging, monitoring controls must be documented in the logging policy for all systems classified as SPECIFIC for security purposes (see section 8.3 above). Additional monitoring controls should be considered for all such systems.

[9] See the Standard on Information Systems Security Incident Management

10. PROTECTION OF LOG INFORMATION

Policy objective 5.10.3 – Protection of log information – Logging facilities and log information must be protected against tampering and unauthorised access in order to meet the required retention period or requirements to collect and retain evidence in accordance with Regulation (EC) No 45/2001 on data protection.

10.1. Log Retention

System logs are critical organisational records and must be protected in order to comply with the requirements for log retention given in 5.10.1 Audit Logging. The detailed log retention requirements must be documented in a Log Retention Policy.

The retention period for backups must also be considered in relation with the Log Retention Policy, where logfiles are backed up. In particular, if there is a requirement to delete logs after a specified period, backups must also be deleted.

10.2. Log Protection

Logging facilities must be protected against deliberate and accidental threats, notably:

- Log files being edited or deleted to hide misuse
- Alterations to the messages that are recorded
- Log file limits being exceeded leading to logs being discarded, overwritten or deleted

Logs, logging facilities and log configuration tools must be protected so that only authorised administrators have access and no end users may delete or alter logs. If separate log archiving facilities are used, the administrators for these facilities should be different from the administrators for the systems generating the logs in order to prevent misuse by system administrators. Access to logs must be granted on a strict need-to-know basis.

Critical log files must be backed up to a secure, remote location. The System Owner must define which log files are considered critical, based on the system risk assessment and with advice from the LISO, and document this in the Log Retention Policy.

To facilitate the implementation of this control, it is recommended that an automatic log archiving system be put in place that collects log entries from relevant systems and stores them securely in a central system. Log consolidation may be performed as long as this is consistent with any legal requirements.

The Log Retention Policy must include a statement on whether the log entries must be kept for potential use as legal evidence. If so, the solution

implemented for log archiving must be checked to ensure that the treatment of log entries maintains their validity as legal evidence (see the Standard on Information Systems Security Incident Management).

11. CLOCK SYNCHRONISATION

Policy objective 5.10.4 – Clock synchronisation – As correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases, system clocks must be synchronised regularly with an agreed accurate time source, especially between the Commission's various processing platforms.

11.1. General rules

System clocks are used to record the date and time of events in log entries, and the correct setting of clocks is important to ensure their accuracy. Inaccurate audit logs may hinder investigations and damage the credibility of log entries used as evidence.

Where a computer or a communications device has the capability to operate a real-time clock, this clock must be regularly synchronised with a master clock. Clocks must be set to the time of their local time-zone, and must change to reflect daylight savings. Where the facility exists to set the time-zone (i.e. as an offset from UTC), this should be used.

Clocks of user devices (PCs, PDAs etc.) must be set to their home time-zone[10]. They must be synchronised at least at log-on and log-off. Clocks of servers and network devices must be synchronised periodically (at least once a day) using a secure clock synchronisation protocol to prevent attacks using false NTP packets.

Spot checks must be performed regularly to ensure that system clocks are correct and properly synchronised. The procedure for clock synchronisation must be documented.

12. ROLES AND RESPONSIBILITIES

System Owners: responsible for defining the events to be logged.

System Managers: responsible for managing the operation of logging and monitoring solutions and, where relevant, for ensuring that IT service providers comply with the logging and monitoring requirements.

IT Service Providers: responsible for operating logging and monitoring solutions.

[10] Most likely the time-zone of the office from which they were issued.

13. REFERENCES

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

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

Regulation (EC) No 45/2001 on data protection

Standard on Risk Management

Standard on Information Systems Security Incident Management

14. RELATED DOCUMENTS

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

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

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

NIST SP 800-92 Guide to Computer Security Log Management