EUROPEAN COMMISSION
DIRECTORATE-GENERAL
INFORMATICS

Director General

DIGIT

Directorate-General for Informatics

INFORMATION SECURITY POLICIES

INFORMATION SECURITY STANDARD (ISS) ON SECURITY MONITORING

Version:	1.0 - 27/10/2008
Status:	PUBLISHED
Reference Number:	ISS_SECURITY_MONITORING
Owner:	Francisco García Morán
	Director General
Author:	Philippe Schultz
	DIGIT LISO
Revised by:	
Approved by:	
Classification:	LIMITED
Publication date:	

Table of Contents

DOCUMENT HISTORY

Version	Date	Comments	Modified Sections
0.2	28/02/2008	Draft version	All

1. INTRODUCTION

This document is designed to support DIGIT General Information Systems Security and in particular DIGIT Topic-Specific Information Security Policies (TSISP) on Security Monitoring.

2. PURPOSE

This Information Security Standard (ISS) defines in further detail the rules (policy) applicable for a specific area: Security Monitoring.

3. SCOPE AND APPLICABILITY

See DIGIT GISP.

4. RELEVANT LEGISLATION AND REGULATIONS

See DIGIT GISP.

5. TERMS AND ABBREVIATIONS

See document "Security Terms and Abbreviations"

6. WRITING CONVENTIONS

See DIGIT GISP.

7. STANDARD REVISION AND COMMUNICATION

See DIGIT GISP.

To ensure the continuing suitability, adequacy, and effectiveness of this standard document, it will be revised every 2 years or, when necessary earlier according to the rules established in the GISP.

8. DETAILED TECHNICAL SECURITY REQUIREMENTS

8.1. Events generation

Where applicable, and technically possible, audit records, should include the following characteristics of events:

(1) (Unique) user/subject identity;

(2) Source IP, Destination IP, protocol used, and the action taken (where applicable);

(3) The date and time of the event;

(4) The outcome (success/failure);

(5) A mean to identify the impacted component of the system;

(6) The access path (network, physical/interactive, system level …)

(7) Type of event notification (ex: Information, Warning, Error, Success audit, Failure audit);

(8) sufficient information for the event to be self explaining;

(9) host identity (host name and IP address at minimum);

(10) records of successful and rejected system access attempts (ex: network addresses and protocols; account information for failed logon attempts);

(11) records of successful and rejected access attempts to data or other resources (ex: files accessed and the kind of access);

(12) Details on changes made to security and system configuration, system configuration files or system configuration repositories.

Every event occurrence must be logged. Event summarizing and/or correlation can be done at central security logs management infrastructure level.

Events shall be recorded in chronological order to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.

The data that arrives at the logging facility must be in the format of the software that recorded the activity. The logging facility may process the logging data into a common format. This process is called normalization and enables a timely and effective log analysis.

In response to specific situations, whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information, or in the event of intrusive or anomalous activity, the level of audit monitoring could have to be increased.

In response to particular events, especially under attacks causing large numbers of events to be logged having a negative impact such as slowing system performance (denial of service on audit functions), it may also be decided, with the approval or at the request of the security monitoring group, to reconfigure logging baselines, defined hereafter, for a short period of time.

Depending on the system classification, to be determined using the Topic-Specific Information Security Policy on Asset Management (to be developed), additional measures should be implemented as following. Until the Asset Management policies are approved, at least the STANDARD baseline mentioned hereafter should be implemented as default.

Where possible, users and privileged users (such as system administrators) shall not be able to manipulate components associated with the process in charge or generating security log information.

In particular, the following actions shall be protected:

- change in audit configuration parameters/files
- suspend of audit process
- change in audit module executable or source files

For systems classified C.STANDARD, I. STANDARD, A. STANDARD, and higher, the following minimum set of operations will be audited for execution.

(1) User/process Login and Logout information

(2) unsuccessful information (files/resource) access attempts;

(3) unsuccessful request for access rights (granting of)

(4) unsuccessful system/function access attempts, such as:

  (a) failed or rejected user actions (including authentication attempts, use of rights);

  (b) failed or rejected actions involving data and other resources;

  (c) access policy violations and notifications for network gateways and firewalls (including Source and destination IP, protocol used, action taken);

(d) alerts from proprietary intrusion detection systems or equivalent;

(5) all privileged operations, such as:

(a) unsuccessful use of privileges or use of privileged accounts or privileged rights (e.g. supervisor, root, administrator);

(b) unsuccessful actions performed by privileged accounts or privileged rights;

(c) unsuccessful use of system utilities and applications;

(d) unsuccessful change ownership of objects;

(e) change of privileges and access rights;

(f) user provisioning, de provisioning tasks

(g) password/credential generation, change or reset

(h) unsuccessful access to privileged capabilities;

(i) successful/unsuccessful changes to system security settings and controls in particular event logging parameters;

(j) successful/unsuccessful audit data access/read;

(k) successful/unsuccessful audit data deletion operations;

(l) successful/unsuccessful system time and date modifications;

(m) successful/unsuccessful system start-up and stop (and restart);

(n) successful/unsuccessful processes/services (daemon/instance) start and stop;

(o) successful/unsuccessful activation and de-activation of protection systems, such as auditing functions, access control functions, anti-virus systems;

(p) unsuccessful I/O device attachment/detachment;

(q) Network activity

- Unauthorised/Failed connection the system (including IP address of hosts requesting the service and service information)

- Connections to a system

– Connection duration, when applicable

(6) system alerts or failures such as:

(a) console alerts or messages;

(b) system log exceptions;

(c) network management alarms;

(d) alarms raised by the access control system;

For systems classified C.MODERATE, I.MODERATE, A.MODERATE, and higher, in addition to operations audited for systems classified at lower level, the following minimum set of operations will be audited for execution:

(1) successful information (files/resource) access attempts;

(2) successful system/function access attempts, such as:

(a) successful user actions (including authentication attempts, use of rights);

(b) access policy violations and notifications for network gateways and firewalls (including Source and destination IP, protocol used, action taken);

(c) alerts from proprietary intrusion detection systems or equivalent;

(3) all privileged operations, such as:

(a) successful change ownership of objects;

(b) successful I/O device attachment/detachment;

For systems classified C.HIGH, I.HIGH, A.HIGH, in addition to operations audited for systems classified at lower level, the following minimum set of operations will be audited for execution:

(1) all privileged operations, such as:

(a) successful use of privileges or use of privileged accounts or privileged rights (e.g. supervisor, root, administrator);

(b) successful actions performed by privileged accounts or privileged rights;

(c) successful use of system utilities and applications;

(d) successful access to privileged capabilities;

(e) Network activity

- Authorised connection the system (including IP address of hosts requesting the service and service information) and duration of the connection.

In addition to reviewing audit data, unauthorised activity/changes may also be discovered by actively monitoring the status of specific objects.

The following list of actions shall be also monitored:

- process list
- system job queues to ensure that no unauthorised back jobs or scripts are being run
- creation, reload, and compilation of objects to unsure no unauthorised changes have been made.
- audit processing failures such as, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Where technically possible and applicable, depending of the system security classification (see Information Security Standard), and where such a requirement is clearly identified by the system/service owner, to avoid failure in recording events, when logging errors occur, for instance in case of full log files, the system must suspend its functionality completely.

8.2. Event Logs Transmission

To provide reliable log delivery, connection-oriented protocols such as TCP must be used.

To provide transmission confidentiality and integrity protection, protocols implementing encryption such as TLS (or SSL), SSH or IPsec must be used. In addition, integrity protection and authentication of communicating parties must be implemented. Message digest functions using SHA-1 or MD5 are approved.

8.3. Event Logs Storage and disposal

Log Data and Log generation protection

Controls shall be implemented to prevent logs files and log generation process being edited (modified) or deleted by unauthorised subjects (persons or processes).

Controls shall be implemented to prevent gaps in data gathering for instance due to storage capacity being exceeded, resulting in either the failure or record events or over-writing of past recorded events.

This also includes preventing gaps in data gathering during extreme situations (unusual large number of log entries to be generated in a short period of time) such as denial of service attacks.

Unauthorised physical access to media containing log information shall be prohibited.

8.3.1. At system level (Local)

Log Data and Log generation protection

Where technically possible, system administrators shall not have permission to erase, modify or de-activate log functions/processes of their own activities.

To ensure that no leakage of sensitive security log information occurs, logs files SHOULD not be read by applications or processes other than those used for consolidation (centralisation), storage and inspection of log files by authorised personnel.

Read access to security log information will be limited to DBA/ System Administrators and LISO only.

Where technically possible, the log Rotation process (see Data retention hereafter) must not be under the control of DBA/System Administrators

Data retention

Logs shall be retained online at least 30 days and until being sent to the security log management infrastructure.

Online logs SHALL be rotated (with preserving its original format) on the following basis:

- for standard systems baseline: once a day, at end of day (12 PM)
- for moderate systems baseline: twice a day, at end of day (12 AM, 12 PM)
- for high systems baseline: at the top of every hour

The integrity of original (rotated) log files shall be preserved by

- Generating a message digest for each log files

– Performing a back-up of these files on a daily basis.

Archived (off-line backed-up) log files shall be kept for a period of 180 days.

Original logs may be used as evidence in case of forensics investigations. Hence, when a legal investigation is officially notified, logs shall be retained, in their original format (without normalisation or transformation), as necessary, and at least until being gathered using approved forensics disk imaging techniques.

8.3.2. At central security log management infrastructure level

Log Data and Log generation protection

Stored log information and log generation process shall be protected against tampering (unauthorised modification) and unauthorised access including access by network and system administrators (excluding the central security log management infrastructure system administrators).

Read access to these security log information will be limited to the security monitoring group.

Unauthorised physical access to media containing log information shall be prohibited.

Unauthorised physical access to log archive storage (see Data retention hereafter) must be limited to persons of the Security monitoring group.

Data retention

Logs shall be retained online 30 days. Then, logs shall be kept offline.

The integrity of offline log files shall be preserved by

– Generating a message digest for each log files

– Where possible archiving the log file on a protected, isolated storage container based on append-only media like a write-once/read many (WORM) disk or drive.

– Performing a back-up of the log archive storage container on a daily basis.

Archived (off-line) log files shall be kept for a period of 1 year.

9. DETAILED ORGANISATIONAL SECURITY REQUIREMENTS

9.1. Events Log analysis (Audit Data Review)

9.1.1. At system level (Local)

At system level, security analysis of log information shall be performed by qualified personnel to provide expert level analysis of security events.

Collected data SHOULD be analysed at least daily to detect, using system administrators expertise with the support of automated systems, any compromise or attempted compromise of system security.

Depending on the system classification, to be determined using the Topic-Specific Information Security Policy on Asset Management (to be developed), additional measures should be implemented as following. Until the Asset Management policies are approved, at least the STANDARD baseline mentioned hereafter should be implemented as default.

For systems classified C.STANDARD, I. STANDARD, A. STANDARD, and higher, the audit data will be reviewed for the following:

- Excessive logon attempts failures by single or multiple accounts
- Logons at unusual/non-duty hours
- Unusual or suspicious patterns of activity

a) Account management actions such as create users and add users to groups

b) Unsolicited password resets

c) Unsolicited resources permissions modification (ex: access control permissions modification)

d) Use of privileged user rights (Use of privileged commands)

e) Changes to system configuration (configuration files/registry …), including modification of the filtering rules for a network filtering component,

f) Execution of unknown or unauthorised programs

g) Attempt to circumvent auditing

h) Unplanned system restarts and changes to system time

i) Changes to system security policy

j) Change to security domains (ex: create of break trust relationships)

k) Using other users credentials

l) Logging interactively with daemon/services account credentials

m) Misuse of privileges (processing data without authorisation)

n) Unauthorised use of console ports

o) Unauthorised change to system configuration (hardware and software components/storage structure)

p) Unauthorised export to media/backup of information

q) Failed attempts to access information indicating a possible pattern of deliberate browsing

- Attempt to use unauthorised accounts or rights
- Attempt to access unauthorised resources (hosts, files, services …)

r) Account lockouts

- In case of a network filtering system unusual traffic patterns including

a) successful and unsuccessful login attempts on the filtering system

b) packets that are blocked upon arrival at the filtering system;

c) packets that are blocked upon departure from the filtering system;

d) packets that arrive or depart within a designated time interval;

e) denied connections initiated from external network

f) denied connections initiated from the internal network.

For systems classified C.HIGH, I. HIGH, A. HIGH, in addition to audit data reviewed for systems classified at lower level, the audit data will be reviewed for the following:

- Successful attempts to access restricted system or data files
- Command-line activity by a user that should not have that capability
- In case of a network filtering system:
    - Change in network or objects contents

9.1.2. At central security log management infrastructure level

Analysis at the central security log management infrastructure level can find patterns of events across multiple systems, such as coordinated or widespread attacks (e.g., malware, distributed denial of service), and attacks that go between the systems.

This security monitoring shall be performed in near-real-time to provide rapid responses to serious security events and helps to minimize the impact of security incidents.

In addition to audit data reviewed at system level (locally), at central level, the audit data will be reviewed for the following:

- Unusual or unauthorized activity by System Administrators
- All system and security administration actions in particular
    - Account management activities
    - System Object access
    - Sensitive Process start and stop