Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

Direction centrale de la sécurité
des systèmes d'information

Paris, le 25 juin 2009

Référence : AGR/P/02.1 EN

PROCEDURE

SECURITY OF EVALUATION FACILITIES

Application: From date of publication.

Distribution: Public.

COURTESY TRANSLATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Version history

Version	Date	Modifications
1	25/06/2009	Creation

TABLE OF CONTENTS

1. Purpose of the procedure

This procedure specifies the minimal security rules and recommendations applicable to ITSEFs (Information Technology Security Evaluation Facilities) providing services in the framework of French Decree no. 2002- 535 of 18 April 2002 [DECREE].

Observance of the minimal rules is formally verified in the course of the accreditation audits to which ITSEFs are subjected. The DCSSI (Central Directorate for Information Systems Security) may request to verify their application itself at any moment.

2. References

- [DECRET] Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
- [LABREF14] Lab Ref 14, Exigences spécifiques, essais pour l'évaluation de la sécurité des technologies de l'information, révision 00 – Septembre 2007 (document disponible sur www.cofrac.fr).
- [PSSI] Guide pour l'élaboration d'une politique de sécurité des systèmes d'information, PSSI (document disponible sur www.ssi.gouv.fr).
- [IGI1300] Instruction générale interministérielle sur la protection du secret de la défense nationale, n° 1300/SGDN/PSE/SSD du 25 août 2003, et ses documents d'application.

3. Organisation of the Document

The rules (obligatory implementation) and recommendations (good practices) set forth herein are organised under seven themes. A short definition of each theme is first provided.

4. Themes

4.1 Security Policy Management

4.1.1. Definition

Security policy can be defined as "all laws, rules and practices governing the manner in which property is managed, protected and distributed within an organisation".

The primary objective of the security policy of an ITSEF is to ensure the protection of sensitive property, i.e. (non-exhaustive list):

- information supplied by its clients;
- information generated from the information supplied by its clients;
- evaluation targets supplied by its clients;
- attack processes that the ITSEF has developed;
- equipment that the ITSEF has developed to carry out vulnerability analysis;
- security of exchanges between the DCSSI and the ITSEF.

4.1.2 Rules and Recommendations

Political_rule-1: the ITSEF must have a security policy written down.

Political_rule-2: the security policy must establish the commitments and responsibilities of the ITSEF's board of directors and must be approved by it.

Political_rule-3: the relevant elements of the security policy must be easily accessible to people having to implement them.

Political_rule-4: the security policy of the ITSEF must at the very least take into account all rules laid down in this document[1].

[1] Bearing in mind that this entire set of rules is not enough to define a comprehensive security policy.

Political_rule-5: any derogation from the rules laid down in this document must have been formally approved by the DCSSI.

Method:
The DCSSI must receive the following information in order to decide whether to approve a derogation request:
- rules for which a derogation is necessary;
- reasons why the derogation is necessary;
- alternative solution proposed with description of associated organisational procedures and description of the technical architecture in the case of a technical procedure;
- analysis of the risks associated with implementing this solution;
- any other argument enabling the DCSSI to formulate an opinion regarding the proposed solution.

The examination of the derogation request may necessitate an audit by the DCSSI and an additional audit of the ITSEF by the COFRAC in the framework of its accreditation.

Political_rule-6: the security policy must include and describe a process for its own review and validation.

Political_rule-7: the security policy must include a process for periodically updating the risk analysis on which it is based.

Recom_politique-1: It is recommended that the security policy be based on the [PSSI] document.

4.2. Personnel

4.2.1. Definition

Personnel concerned by this document are those employees who have signed an employment contract with either the ITSEF or its parent organisation.

4.2.2. Rules and Recommendations

Personnel_rule-1: when recruiting personnel:
- stated professional qualifications and diplomas must be verified;
- references must be verified.

Personnel_rule-2: the security policy must specify the personal and criminal liability of ITSEF personnel with access to sensitive property.

Personnel_rule-3: ITSEF personnel must be familiar with the security policy and confirm this in writing before gaining access to any sensitive property.

4.3. Organisation of Security, Responsibilities

4.3.1. Definition

The organisation of security consists in attributing roles to each member of staff, giving them specific and enforceable responsibilities.

4.3.2. Rules and Recommendations

Organisation_rule-1: the security policy must set forth the organisation of security within the ITSEF.

Organisation_rule-2: A security manager with authority over ITSEF personnel concerning security

must be appointed.

Organisation_rule-3: the security policy must set forth the measures taken to ensure the protection of sensitive property with regard to internal and external personnel (service providers, auditors, interns, etc.) who have no "need to know".

Organisation_rule-4: the security policy must define the "need to know" rules for different personnel of the ITSEF (evaluator, project manager, technical laboratory prime, laboratory manager, quality officer, security officer, etc.).

Organisation_rule-5: the security policy must include the periodical implementation of security checks.

Organisation_rule-6: the security policy must specify how security incidents are managed (identification, declaration, attribution, follow-up, etc.).

Organisation_rule-7: ITSEF personnel must be familiar with the security policy.

4.4. Classification of Information[2]

4.4.1. Definition

The classification of a piece of information is an indication of the appropriate level of protection given its degree of sensitivity. It is indicated by means of a mark applied to its physical media support (paper, file, USB key, hard drive, PC, network, etc.). Said mark is associated with rules governing its protection and access authorisations. We say that the media itself is also, by extension, classified.

4.4.2. Rules and Recommendations

Classification_rule-1: the security policy must define the different levels of classification for sensitive property as well as the rules that must be applied for the creation, attribution, issuing, destruction, etc. of such property.

Classification_rule-2: the levels of classification and associated rules defined in Appendix A hereto are applicable to sensitive property exchanged between the ITSEF and the DCSSI.

Classification_rule-3: Media must be classified to a level superior or equal to the highest level of classification represented by the information contained therein.

Classification_recom-1: it is recommended that the ITSEF use, by default, the classification levels and associated rules defined in Appendix A hereof in its exchanges with developers and sponsors.

Classification_recom-2: it is recommended that an inventory of sensitive, and in particular classified, property be put in place.

Classification_recom-3: it is recommended that the ITSEF destroy, under its supervision, any classified medium of which it no longer has use.

4.5. Physical Security

4.5.1. Definition

Physical security includes surveillance and access control (filtering, badges, etc.), protection of information (security cupboards, safes, reinforced doors, anti-intrusion devices, etc.), intrusion detection (closed-circuit television, door alarms, breakage alarms, motion detectors, etc.), alert (alarm system, security monitoring centre), security staff and on-site intervention.

[2] The rule and recommendations set forth in this chapter do not concern defence-classified information, to which [IGI1300] applies.

4.5.2. Rules and Recommendations

Physical_security_rule-1: the ITSEF must conduct its projects on premises ensuring the protection of the sensitive data it handles. Means of ensuring physical security must be put in place in order to counter any attempts at intrusion or the compromising of sensitive data.
Physical_security_rule-2: In the event that an intrusion is detected, the ITSEF must be able to carry out the necessary verifications within the time required by an intruder in order to compromise the means put in place to ensure the protection of information.
Physical_security-3: the technical methods of security used must save any security incidents detected and operations carried out by administrators, etc. so that this information may be used at a later date.
Physical_security_recom-1 it is recommended that the ITSEF employ various levels of protection and in-depth protection according to the sensitive property in question.
E.g. a simple security cupboard may be suitable to protect a few paper documents relating to a project. A security cupboard including additional protective features (anti-intrusion, breakage, etc.) could be used to protect a server containing the majority of information concerning all projects handled by the ITSEF.
Physical_security_recom-2: it is recommended that the ITSEF put in place a system for controlling access, with the possibility of grading access rights as required.
Physical_security_recom-3: it is recommended that the ITSEF put in place measures in order to limit the risk of electromagnetic compromise.

Special case:

If the ITSEF or its parent organisation is authorised to handle classified contracts [IGI1300], physical security is presumed to be adequate for the purposes of ITSEF activities, on the condition that the environment dedicated to classified contracts applies in full to evaluation projects.

4.6. Visitor Access

4.6.1. Definition

Any persons not belonging to the ITSEF personnel as defined in paragraph 4.2.1. shall be considered as visitors.

4.6.2. Rules and Recommendations

Visitors_rule-1: the ITSEF must define which visitors are to be granted either permanent or temporary free access to its premises.

Visitors_rule-2: the ITSEF must control visitors' access in such a way that it disposes, both at the time and subsequent to the visit, of the following minimum information:

- The visitor's first and last names
- Their nationality
- The type of identification presented and number
- The dates and times of arrival and departure
- The visitor's employer or, otherwise, their status (student, etc.)
- The contact person within ITSEF
- The date and time of departure
- A photocopy of their passport for visitors from outside the European Union.

Visitors_rule-3: information concerning the arrival and departure of a visitor must be conserved for 10 years as from the date and time of the visitor's departure.

Visitors_rule-4: any person with visitor status must be easily and visually identifiable.

Visitors_rule-5: the ITSEF must ensure that the visitor only has access to the premises, information,

equipment, etc. necessary for the purpose of their visit.

Visitors_recom-1: it is recommended that visitors be explicitly informed of prohibited conduct before accessing the ITSEF (e.g. use of cameras, recording devices, laptops, circulating within the premises, etc.)

4.7. Information System

4.7.1. Definition

The information system is defined as all technical and organisational means for producing, modifying, receiving, issuing, archiving destroying, etc., information.

We use the following definitions:

- IS1, as the information system for processing sensitive information associated with evaluations ;
- IS2, as the information system for processing other information belonging to the ITSEF.

4.7.2. Rules and Recommendations

IS_rule-1: the IS1 must not be directly connected to an external network.

Note: an IS1 connected by an insecure network (from a confidentiality point of view) to another IS1 but which uses encryption equipment betwween these IS1, satisfies this rule.

IS_rule-2: IS1s and IS2s must be protected against intrusions and malware. **IS_rule-3**: IS1s and IS2s must be administrated.

IS_rule-4: there must be partitioning according to the need to know on the IS1.

IS_recom-1: it is recommended that the rules applicable to the installation of software on IS1s be defined in the security policy.

IS_recom-2: it is recommended that sensitive information stored in IS1s be systematically encrypted.

Special case:

If the ITSEF or its parent organisation have the IT capability to process defence-classified property and if the ITSEF uses the same IT resources as those used for processing defence-classified property, the IT system is presumed to satisfy the security requirements concerning data confidentiality and the partitioning of evaluation projects, on the condition that the environment and organisation dedicated to defence-classified property applies in full to sensitive property associated with evaluations.

Annexe A Levels of Classification and Applicable Rules between ITSEFs and the Certification Body

1. Classification of Information, Media and Sensitive Property

Note: The classification of a piece of information[3] is indicated by a mark applied to its physical media (paper, file, USB key, hard drive, PC, network, etc.). Said mark is associated with rules governing its protection and access authorisations. We say that the media itself is also, by extension, classified.

"Property" shall here refer both to the information itself and to the media support on which it is saved.

2. Levels of Classification

Level	Rules
RESTRICTED [NAME]	Classified property is restricted to the entities concerned. E.g. RESTRICTED ITSEF: only ITSEF and DCSSI personnel have access to the classified property.
CONFIDENTIAL [NAME]	Classified property is restricted to a group of individuals.
SECRET [NAME]	Access restricted to persons designated by name.

The [NAME] attribute may be:

- The code name of an evaluation (e.g. CAMELIA, ROSE, etc.)
- An area of activity carried out by a given organisation (e.g. INDUSTRY, SALES, etc.)
- A group of actors (e.g. ITSEF, etc.).

The [DEFENCE] attribute for CONFIDENTIAL and SECRET levels is restricted for use only as defined by the regulations concerning the protection of a secret of national defence [IGI1300] and their associated documents, and falls outside the scope of this procedure.

3. Rules Concerning Classified Property

The rules and procedures described below have been drawn up on the understanding that classified property refers to information (as is usually the case). Some of these rules and procedures must sometimes be adapted if the classified property refers to physical media or equipment.

3.1. Term of Classification

The term of the classification period may be indicated along with the classification level mark. At the end of this period, the classified property is classified at a lower level (or declassified if classified at the RESTRICTED [NAME] level). If the term of classification is not indicated, the rule is as follows:

Level	Rules
RESTRICTED [NAME]	5 years for property classified as RESTRICTED [NAME] before its declassification.
CONFIDENTIAL [NAME]	5 years for property classified as CONFIDENTIAL [NAME] before its classification as RESTRICTED [NAME].
SECRET [NAME]	10 years for property classified as SECRET [NAME] before its classification as CONFIDENTIAL [NAME].

3.2. Copying Classified Property

Level	Rules
RESTRICTED [NAME]	No restriction

[3] The rules and recommendations set forth in this chapter do not concern defence-classified information, to which [IGI1300] applies

CONFIDENTIAL [NAME]	May be copied by the receiving party with the consent and under the supervision of the receiving party's security manager.
SECRET [NAME]	May be copied by the receiving party with the consent of the disclosing party.

3.3. Destruction of Classified Property

The destruction of classified property is carried out by the destruction of its physical media support.

Level	Rules
RESTRICTED [NAME]	Destruction by the receiving party.
CONFIDENTIAL [NAME]	
SECRET [NAME]	Destruction by the receiving party with certificate of destruction.

	Means of destruction	
Level	**Paper and other flexible media**	**Rigid magnetic media, electronic mass memory devices, etc.**
RESTRICTED [NAME]	Shredding, incineration, chemical processes, supervised destruction by a service provider.	Low-level formatting, overwriting, physical destruction, chemical processes.
CONFIDENTIAL [NAME]		
SECRET [NAME]	Cross-shredding, incineration, chemical processes	Physical destruction, chemical processes.

3.4. Sending Classified Property

Any classified property must be addressed to the person authorised to receive classified property at the receiving party's end. If in doubt, it should be sent to the Director or Technical Manager at the ITSEF or to the Head of the Certification Body.

3.4.1. In general, by Post or by Courier

Level	Rules
RESTRICTED [NAME]	Transmission by post, in two envelopes: - Plain outer envelope containing the inner envelope; - Inner envelope indicating the classification and addressee and containing the classified property, a packing slip and proof of receipt slip[4].
CONFIDENTIAL [NAME]	Transmission by post, in two envelopes: - Plain outer envelope containing the inner envelope; - **Secure** inner envelope indicating the classification and addressee and containing the classified property, a packing slip and proof of receipt slip[4].

[4] In order to be returned by simple post, the proof of receipt slip must not show either any indication of classification or any indication as to the nature of the property sent.

SECRET [NAME]	**Direct handing over from the sender to the recipient or by authorised courier**, in two envelopes: - Plain outer envelope containing the inner envelope; - Secure inner envelope indicating the classification and addressee and containing the classified property, a packing slip and proof of receipt slip[4].

In the rules contained in the above table, differences with respect to the previous case are highlighted in bold.
For property sent between the DCSSI and ITSEFs, authorised couriers shall mean ITSEF personnel, the owner of the information or DCSSI certification body personnel.
The ITSEFs and the DCSSI shall appoint other authorised couriers, either permanent or occasional, by common consent.

3.4.2. Classified Information Encrypted by a Process Validated by the DCSSI, Sent by Post or by Courier

Level	Rules
RESTRICTED [NAME]	- Transmission by post in a single envelope.
CONFIDENTIAL [NAME] SECRET [NAME]	Transmission by post, in two envelopes: - Plain outer envelope containing the inner envelope; - Secure inner envelope indicating the classification and addressee and containing the classified property, a packing slip and proof of receipt slip[4].

3.4.3. Classified Information, Sent Via an Unprotected Communications Network

Level	Rules
RESTRICTED [NAME]	Encrypted transmission via a process validated by the DCSSI. Unencrypted transmission only on an exceptional basis and subject to agreement by both parties and by the owner of the information.
CONFIDENTIAL [NAME]	Encrypted transmission via a process validated by the DCSSI.
SECRET [NAME]	Encrypted transmission via a process validated by the DCSSI only on an exceptional basis and subject to agreement by both parties and by the owner of the information.

Annexe B Encryption of exchanges between ITSEFs and the DCSSI

The ACID tool provided to ITSEFs by the DCSSI is considered apt to protect exchanges between the DCSSI and ITSEFs. The DCSSI manages keys. Only “ITSEF” network keys must be used.