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
N° 1632 /SGDN/DCSSI
Référence : AGR/P/02.1

PROCEDURE

SECURITE DES CENTRES D'EVALUATION

Application : A compter de la date de publication

Diffusion : Publique

Vérifiée par	Validée par le sous-directeur de la régulation	Approuvée par le directeur central de la sécurité des systèmes d'information
Le responsable qualité [ORIGINAL SIGNE] *Le chef du centre de certification* Pascal CHOUR [ORIGINAL SIGNE]	Pascal CHAUVE [ORIGINAL SIGNE]	Patrick PAILLOUX [ORIGINAL SIGNE]

Suivi des modifications

Révision	Date	Modifications
1	25/06/2009	Création

TABLE DES MATIERES

1. Objet de la procédure

Cette procédure précise les règles minimales et les recommandations de sécurité applicables aux CESTI (Centre d'évaluation de la sécurité des technologies de l'information) intervenant dans le cadre du décret n° 2002-535 du 18 avril 2002 [DECRET].

Le respect des règles minimales est vérifié formellement dans le cadre des audits d'accréditation des CESTI. La DCSSI (Direction centrale de la sécurité des systèmes d'information) peut demander à tout moment de vérifier elle-même leur application.

2. Références

- [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 du document

Les règles (obligation de mise en œuvre) et les recommandations (bonnes pratiques) exposées dans le présent document sont organisées en sept thèmes, préalablement définis.

4. Thèmes

4.1. Gestion de la politique de sécurité

4.1.1. Définition

La politique de sécurité peut être définie comme étant « l'ensemble des lois, règles et pratiques qui régissent la façon dont les biens sont gérés, protégés et distribués au sein d'un organisme ».

L'objet premier de la politique de sécurité du CESTI est d'assurer la protection de ses biens sensibles, à savoir (liste non limitative) :

- les informations fournies par ses clients ;
- les informations produites à partir des informations fournies par ses clients ;
- les cibles d'évaluation fournies par ses clients ;
- les procédés d'attaques que le CESTI a développés ;
- les équipements que le CESTI a développés pour réaliser ses analyses de vulnérabilité ;
- la sécurité des échanges entre la DCSSI et le CESTI.

4.1.2. Règles et recommandations

Règle_politique-1 : le CESTI doit disposer d'une politique de sécurité écrite.

Règle_politique-2 : la politique de sécurité doit établir les engagements et la responsabilité de la direction du CESTI et être approuvée par elle.

Règle_politique-3 : les éléments pertinents de la politique de sécurité doivent être facilement accessibles aux personnes ayant à les mettre en œuvre.

Règle_politique-4 : la politique de sécurité du CESTI doit au minimum prendre en compte l'ensemble des règles énoncées dans le présent document[1].

Règle_politique-5 : toute dérogation aux règles énoncées dans le présent document doit avoir été approuvée formellement par la DCSSI.

Modalités :

Les éléments attendus par la DCSSI pour se prononcer sur une demande de dérogation sont les suivants :

- règles auxquelles il est nécessaire de déroger ;
- motifs nécessitant cette dérogation ;
- solution alternative proposée avec description des procédures organisationnelles associées et description de l'architecture technique s'il s'agit d'un moyen technique ;
- analyse de risque associée à la mise en œuvre de cette solution ;
- tout autre argumentaire permettant à la DCSSI de se faire un avis sur la solution proposée.

L'instruction de la demande de dérogation peut nécessiter un audit de la DCSSI et un complément d'audit du CESTI par le COFRAC dans le cadre de son accréditation.

Règle_politique-6 : la politique de sécurité doit prévoir et décrire un processus pour sa propre révision et validation.

Règle_politique-7 : la politique de sécurité doit prévoir un processus de mise à jour périodique de l'analyse de risque sur laquelle elle se fonde.

Recom_politique-1 : il est recommandé d'appuyer la politique de sécurité sur le document [PSSI].

4.2. Personnels

4.2.1. Définition

Les personnels dont il est question ici sont les salariés qui ont signé un contrat de travail avec le CESTI ou avec l'organisme dont il relève.

4.2.2. Règles et recommandations

Règle_personnels-1 : à l'embauche des personnels :

- les qualifications professionnelles et les diplômes annoncés doivent être vérifiés ;
- les références doivent être vérifiées.

Règle_personnels-2 : la politique de sécurité doit préciser les responsabilités personnelles et pénales des personnels du CESTI ayant accès aux biens sensibles.

Règle_personnels-3 : les personnels du CESTI doivent connaître la politique de sécurité et le confirmer par écrit avant tout accès aux biens sensibles.

[1] Sachant que cet ensemble de règles n'est pas suffisant pour définir une politique de sécurité complète.

4.3. Organisation de la sécurité, responsabilités

4.3.1. Définition

L'organisation de la sécurité consiste en l'attribution de rôles à chacun des personnels, leur conférant des responsabilités précises et opposables.

4.3.2. Règles et recommandations

Règle_organisation-1 : la politique de sécurité doit décrire l'organisation de la sécurité au sein du CESTI.

Règle_organisation-2 : un responsable sécurité ayant autorité sur les personnels du CESTI pour les aspects sécurité doit être nommément désigné.

Règle_organisation-3 : la politique de sécurité doit décrire les mesures prises pour assurer la protection des biens sensibles vis-à-vis des personnels internes et externes (prestataires, commissaires aux comptes, stagiaires…) n'ayant pas à en connaître.

Règle_organisation-4 : la politique de sécurité doit définir le « besoin d'en connaître » pour les différents personnels du CESTI (évaluateur, chef de projet, responsable technique du laboratoire, directeur du laboratoire, responsable qualité, responsable sécurité, etc.).

Règle_organisation-5 : la politique de sécurité doit prévoir la mise en œuvre périodique des contrôles de sécurité.

Règle_organisation-6 : la politique de sécurité doit préciser comment sont gérés les incidents de sécurité (constatation, déclaration, imputation, suivi, etc.).

Règle_organisation-7 : la politique de sécurité doit être connue des personnels du CESTI.

4.4. Classification des informations[2]

4.4.1. Définition

La classification d'une information est une mention destinée à indiquer le niveau de protection adapté à sa sensibilité. Elle est indiquée par un marquage appliqué à son ou ses supports physiques (papier, fichier, clé USB, disque dur, PC, réseau,…), associé à des règles de protection et à des autorisations d'accès. Par extension, on dit que le support lui-même est classifié.

4.4.2. Règles et recommandations

Règle_classification-1 : la politique de sécurité doit définir des niveaux de classification pour les biens sensibles ainsi que les règles à appliquer sur ces biens pour les actions de création, d'attribution, d'émission, de destruction, etc.

Règle_classification-2 : les niveaux de classification et les règles associées définies en annexe A du présent document sont applicables aux biens sensibles échangés entre le CESTI et la DCSSI.

Règle_classification-3 : un support doit être classifié à un niveau supérieur ou égal au plus haut niveau de classification des informations qu'il contient.

[2] Les règles et recommandations énumérées dans ce chapitre ne concernent pas les informations classifiées de défense pour lesquelles s'applique l'[IGI1300].

Recom_classification-1 : il est recommandé d'utiliser par défaut les niveaux de classification et les règles associées définies en annexe A du présent document au sein du CESTI pour ses échanges avec les développeurs et commanditaires.

Recom_classification-2 : il est recommandé de mettre en place un inventaire des biens sensibles, et plus particulièrement des biens classifiés.

Recom_classification-3 : il est recommandé au CESTI de détruire, sous son contrôle, tout support classifié dont il n'a plus l'usage.

4.5. Sécurité physique

4.5.1. Définition

La sécurité physique regroupe les moyens de surveillance et de contrôle des accès (filtrage, badges, …), de protection de l'information (armoires fortes, coffres, portes renforcées, dispositifs anti-effraction, …), de détection d'intrusion (vidéo-surveillance, contacts d'ouverture, détection de choc, détection de présence, …), d'alerte (centrale d'alarme, centre de supervision de la sécurité), de gardiennage, et d'intervention sur site.

4.5.2. Règles et recommandations

Règle_sécurité_physique-1 : le CESTI doit traiter ses projets dans des locaux aptes à protéger les biens sensibles qu'il manipule. Des moyens de sécurité physique doivent être mis en place pour freiner les tentatives d'effraction et de compromission des biens sensibles.

Règle_sécurité_physique-2 : le CESTI doit être en mesure d'effectuer une levée de doute en cas de détection d'intrusion dans des délais compatibles avec la résistance des moyens mis en œuvre pour assurer la protection de l'information.

Règle_sécurité_physique-3 : les moyens techniques de sécurité doivent enregistrer les incidents de sécurité détectés, les opérations d'administration, etc. afin de permettre leur exploitation ultérieure.

Recom_sécurité_physique-1 : il est recommandé au CESTI d'envisager une protection graduée et une défense en profondeur en fonction des biens sensibles considérés.

Exemple : une armoire forte simple peut être adaptée à la protection de quelques documents papiers d'un projet. On peut envisager une armoire forte comportant des extensions de protection (anti-intrusion, choc…) pour protéger un serveur qui contient la plupart des informations de l'ensemble des projets traités par le CESTI.

Recom_sécurité_physique-2 : il est recommandé au CESTI de mettre en place un système de contrôle des accès avec possibilité de graduer les droits d'accès en fonction des besoins.

Recom_sécurité_physique-3 : il est recommandé au CESTI de mettre en place des moyens permettant de limiter les risques de compromissions électromagnétiques.

Cas particulier :

Si le CESTI ou l'organisme qui l'héberge est habilité à traiter des contrats classés (voir [IGI1300]), la sécurité physique est supposée suffisante pour les activités du CESTI sous réserve que l'environnement prévu pour les marchés classés s'applique intégralement aux projets d'évaluation.

4.6. Contrôle des visiteurs

4.6.1. Définition

Sont considérées comme visiteurs, toutes les personnes ne faisant pas partie du personnel du CESTI tel que défini au paragraphe 4.2.1.

4.6.2. Règles et recommandations

Règle_visiteurs-1 : le CESTI doit définir quels sont les visiteurs autorisés à accéder librement de façon permanente ou temporaire dans ses locaux.

Règle_visiteurs-2 : le CESTI doit mettre en place un contrôle des visiteurs permettant de disposer, au moment de la visite et a posteriori, des informations minimum suivantes :

- le nom et le prénom du visiteur
- sa nationalité
- le type de la pièce d'identité présentée et son numéro
- les dates et heures d'arrivée et de sortie
- l'employeur du visiteur ou à défaut, son statut (étudiant, …)
- la personne rencontrée dans le CESTI
- la date et l'heure de sortie
- la photocopie du passeport pour les visiteurs étrangers hors Union Européenne.

Règle_visiteurs-3 : l'information concernant l'entrée et la sortie d'un visiteur doit être conservée 10 ans à partir de la date et heure de sortie du visiteur.

Règle_visiteurs-4 : une personne ayant un statut de visiteur doit être facilement et visuellement distinguable.

Règle_visiteurs-5 : le CESTI doit s'assurer que le visiteur n'a accès qu'aux locaux, informations, équipements, etc. nécessaires à l'objet de sa visite.

Recom_visiteurs-1 : il est recommandé d'informer explicitement les visiteurs sur les comportements interdits avant leur accès au CESTI (par exemple, l'usage des appareils photographiques, des enregistreurs, des ordinateurs portables, la circulation dans les locaux…).

4.7. Système d'information

4.7.1. Définition

Le système d'information est défini comme étant l'ensemble des moyens techniques et organisationnels permettant de produire, modifier, recevoir, émettre, archiver, détruire, etc., des informations.

On désigne par :

- SI1, le système informatique qui traite les informations sensibles associées aux évaluations ;
- SI2, le système informatique qui traite les autres informations du CESTI.

4.7.2. Règles et recommandations

Règle_SI-1 : le SI1 ne doit pas être connecté directement à un réseau externe.

Précision : Un SI1 raccordé par un réseau non sûr (du point de vue de la confidentialité) à un autre SI1 mais qui utilise des équipements de chiffrement en coupure répond à la règle.

Règle_SI-2 : les SI1 et SI2 doivent être protégés contre les intrusions et les logiciels malveillants.

Règle_SI-3 : les SI1 et SI2 doivent être administrés.

Règle_SI-4 : le cloisonnement selon le besoin d'en connaître doit être assuré sur le SI1.

Recom_SI-1 : il est recommandé de préciser dans la politique de sécurité les règles applicables à l'installation de logiciels sur les SI1.

Recom_SI-2 : il est recommandé de systématiquement chiffrer les informations sensibles mémorisées sur les SI1.

Cas particulier :

Si le CESTI ou l'organisme dont il relève disposent de l'aptitude informatique pour traiter du classifié de défense et si le CESTI utilise les mêmes moyens informatiques que ceux prévus pour le traitement du classifié de défense, le système informatique est supposé répondre aux exigences de sécurité pour la confidentialité des données et le cloisonnement des projets d'évaluation dès lors que l'environnement et l'organisation prévus pour le classifié de défense s'appliquent à l'ensemble des biens sensibles associés aux évaluations.

Annexe A Niveaux de classification et règles applicables entre les CESTI et le centre de certification

1. Classification des informations, des supports et des biens sensibles

Rappel : La classification d'une information[3] est définie par un marquage appliqué à son ou ses supports physiques (papier, fichier, clé USB, disque dur, PC, réseau,…), associé à des règles de protection et à des autorisations d'accès. Par extension, on dit que le support lui-même est classifié.

On convient ici qu'un « bien » est soit une information, soit un support d'information.

2. Niveaux de classification

Niveau	Règles
RESTREINT [NOM]	Protection du bien classifié à l'intérieur des entités concernées. Exemple : RESTREINT CESTI : seuls les personnels du CESTI et de la DCSSI ont accès au bien classifié.
CONFIDENTIEL [NOM]	Protection du bien classifié à l'intérieur d'un groupe de personnes.
SECRET [NOM]	Accès limité à des personnes nommément identifiées

L'attribut [NOM] peut être :

- le nom de code d'une évaluation (exemple : CAMELIA, ROSE, …) ;
- un domaine d'activité d'une organisation donnée (exemple : INDUSTRIE, COMMERCIAL, …) ;
- un ensemble d'acteurs (exemple : CESTI, …).

L'attribut [DEFENSE] pour les niveaux CONFIDENTIEL et SECRET est réservé aux seuls usages définis par la réglementation concernant la protection du secret de la défense nationale ([IGI1300] et documents associés et est hors du champ d'application de la présente procédure.

3. Règles concernant les biens classifiés

Les règles et procédures décrites ci-dessous ont été élaborées en considérant que le bien classifié était une information (cas le plus courant). Certaines de ces règles et procédures devront parfois être interprétées si le bien classifié est un support matériel ou un équipement matériel.

3.1. Durée de la classification

La durée de la classification peut être indiquée avec le marquage du niveau de classification. A l'issue, le bien classifié est classifié au niveau inférieur (ou déclassifié s'il est classifié au niveau RESTREINT [NOM]). Si cette durée n'est pas indiquée, la règle est la suivante :

Niveau	Règles
RESTREINT [NOM]	5 ans pour un bien classifié RESTREINT [NOM] avant sa déclassification.
CONFIDENTIEL [NOM]	5 ans pour un bien classifié CONFIDENTIEL [NOM] avant sa classification en RESTREINT [NOM].
SECRET [NOM]	10 ans pour un bien classifié SECRET [NOM] avant sa classification en CONFIDENTIEL [NOM].

[3] Les règles et recommandations énumérées dans ce chapitre ne concernent pas les informations classifiées de défense pour lesquelles s'applique l'[IGI1300].

3.2. Copie de biens classifiés

Niveau	Règles
RESTREINT [NOM]	Pas de restriction.
CONFIDENTIEL [NOM]	Copie par la partie réceptrice après accord et sous contrôle du responsable de sécurité de la partie réceptrice.
SECRET [NOM]	Copie par la partie réceptrice après accord de la partie émettrice.

3.3. Destruction de biens classifiés

La destruction d'un bien classifié se fait par la destruction de son support physique.

Niveau	Règles
RESTREINT [NOM]	Destruction par la partie réceptrice.
CONFIDENTIEL [NOM]	
SECRET [NOM]	Destruction par la partie réceptrice avec PV de destruction.

	Moyens de destruction	
Niveau	**Papier et autres supports souples**	**Supports rigides magnétiques, mémoires de masse électroniques…**
RESTREINT [NOM]	Broyage, incinération, procédés chimiques, destruction sous contrôle par un prestataire.	Formatage bas niveau, surcharge, pilonnage, procédés chimiques.
CONFIDENTIEL [NOM]		
SECRET [NOM]	Broyage coupe croisée, incinération, procédés chimiques.	Pilonnage, procédés chimiques.

3.4. Transmission d'un bien classifié

Tout bien classifié doit être adressé à la personne habilitée à recevoir les biens classifiés chez la partie réceptrice. En cas de doute, le transmettre au directeur ou responsable technique du CESTI ou au chef du centre de certification.

3.4.1. Cas général, par voie postale ou par porteur

Niveau	Règles
RESTREINT [NOM]	Transmission par voie postale, sous double enveloppe : - enveloppe externe banalisée contenant l'enveloppe interne ; - enveloppe interne mentionnant la classification, le destinataire et contenant les biens classifiés, un bordereau d'envoi et un accusé de réception[4].
CONFIDENTIEL [NOM]	Transmission par voie postale, sous double enveloppe : - enveloppe externe banalisée contenant l'enveloppe interne ; - enveloppe interne **sécurisée** mentionnant la classification, le destinataire et contenant les biens classifiés, un bordereau d'envoi et un accusé de réception[4].
SECRET [NOM]	Transmission **directe de l'émetteur au destinataire ou par porteur agréé**, sous double enveloppe : - enveloppe externe banalisée contenant l'enveloppe interne ; - enveloppe interne sécurisée mentionnant la classification, le destinataire et contenant les biens classifiés, un bordereau d'envoi et un accusé de réception[4].

Dans les règles du tableau ci-dessus, les différences par rapport au cas précédent sont notées en gras.

[4] Pour permettre son renvoi par courrier simple, l'accusé de réception ne doit comporter ni mention de classification, ni indication de la nature de l'envoi.

Sont considérés comme porteurs agréés, pour les transmissions entre la DCSSI et les CESTI les personnels du CESTI, le propriétaire de l'information ou les personnels du centre de certification de la DCSSI.

Les CESTI et la DCSSI peuvent désigner d'un commun accord d'autres porteurs agréés, permanents ou occasionnels.

3.4.2. Informations classifiées chiffrées par un procédé validé par la DCSSI, transmises par voie postale ou par porteur

Niveau	Règles
RESTREINT [NOM]	Transmission par voie postale sous simple enveloppe.
CONFIDENTIEL [NOM] SECRET [NOM]	Transmission par voie postale sous double enveloppe : - enveloppe externe banalisée contenant l'enveloppe interne ; - enveloppe interne sécurisée mentionnant la classification et le destinataire, contenant le support, un bordereau d'envoi et un accusé de réception.

3.4.3. Informations classifiées, transmises par un réseau de communication non protégé

Niveau	Règles
RESTREINT [NOM]	Transmission chiffrée par un procédé validé par la DCSSI. Exceptionnellement et sous réserve d'acceptation par les deux parties et le propriétaire des informations, transmission en clair.
CONFIDENTIEL [NOM]	Transmission chiffrée par un procédé validé par la DCSSI.
SECRET [NOM]	Exceptionnellement et sous réserve d'acceptation par les deux parties et le propriétaire des informations : transmission chiffrée par un procédé validé par la DCSSI.

Annexe B Chiffrement des échanges entre les CESTI et la DCSSI

Le logiciel ACID, fourni par la DCSSI aux CESTI, est apte à protéger les échanges entre la DCSSI et les CESTI. La gestion des clés est assurée par la DCSSI. Seules les clés du réseau « CESTI » doivent être utilisées.