

Secrétariat général

Service des politiques support et des systèmes d'information

Sous-direction du schéma directeur et de la politique des systèmes d'information

# **Directive sécurité de l'hébergement informatique V2**

**FEVRIER\_2016**



MINISTÈRE DE L'ÉCOLOGIE,  
DU DÉVELOPPEMENT DURABLE  
ET DE L'ÉNERGIE  
[www.developpement-durable.gouv.fr](http://www.developpement-durable.gouv.fr)

MINISTÈRE DU LOGEMENT,  
DE L'ÉGALITÉ DES TERRITOIRES  
ET DE LA RURALITÉ  
[www.territoires.gouv.fr](http://www.territoires.gouv.fr)

# Table des matières

<b>1 - PRÉSENTATION DE LA DIRECTIVE.....</b>	<b>3</b>
1.1 - Contexte.....	3
1.2 - Objectif de cette directive.....	3
1.3 - Périmètre d'application de la directive.....	3
1.4 - Cycle de vie du document.....	4
1.5 - Gestion des dérogations.....	5
1.6 - Contrôle de mise en œuvre.....	5
1.7 - Conventions.....	5
<b>2 - ENJEUX RELATIFS À LA SÉCURITÉ DE L'HÉBERGEMENT.....</b>	<b>6</b>
2.1 - Enjeux relatifs aux centres d'hébergement informatiques.....	6
2.2 - Objectifs de sécurité des centres d'hébergement informatiques.....	7
<b>3 - ORGANISATION DE LA SÉCURITÉ DES CENTRES D'HÉBERGEMENT.....</b>	<b>7</b>
3.1 - Direction de l'entité.....	7
3.2 - Responsable sécurité du centre d'hébergement.....	7
3.3 - Exploitants d'un centre d'hébergement informatique.....	9
<b>4 - EXIGENCES DE SÉCURITÉ.....</b>	<b>11</b>
4.1 - Sécurité de l'infrastructure informatique.....	11
4.1.1 - Sécurité des réseaux.....	11
4.1.2 - Filtrage et cloisonnement.....	12
4.1.3 - Sécurité de l'exploitation.....	18
4.1.4 - Gestion de la mutualisation et de la virtualisation.....	25
4.1.5 - Sécurisation des mécanismes de commutation et de routage.....	26
4.1.6 - Sécurisation des ressources.....	27
4.1.7 - Gestion des serveurs de fichiers.....	29
4.2 - Sécurité physique.....	30
4.2.1 - Protection contre les menaces environnementales et les sinistres.....	30
4.2.2 - Protection contre les intrusions physiques.....	37
4.3 - Continuité et secours de l'hébergement informatique.....	41
4.4 - Organisation de l'exploitation.....	44
4.4.1 - Inventaire des ressources.....	44
4.4.2 - Formation et sensibilisation des exploitants.....	44
4.4.3 - Gestion de la documentation.....	45
4.4.4 - Gestion des incidents de sécurité.....	46
4.4.5 - Gestion du reconditionnement et de la fin de vie des ressources.....	47
<b>5 - EXIGENCES DE SÉCURITÉ VIS-À-VIS DES HÉBERGEURS EXTERNES.....</b>	<b>47</b>

# 1 - Présentation de la directive

## 1.1 - Contexte

Comme le précise la Politique Générale de Sécurité des Systèmes d'Information (PGSSI V2) du ministère, les informations ainsi que les systèmes informatiques qui permettent de les collecter, traiter, transmettre et stocker, constituent une part essentielle du patrimoine du ministère.

Ces systèmes d'Information sont exposés à de multiples menaces évoluant en permanence et pouvant gravement porter atteinte au ministère dont l'exposition et la complexité des SI ne font que croître. L'amplification des attaques informatiques aux motivations multiples, l'évolution constante des réseaux mafieux et l'espionnage d'États ont fait de la «*cyberdéfense*» un enjeu national.

Les **centres d'hébergement** constituent un **pilier essentiel des systèmes d'information**. Leur **sécurisation** représente donc un **enjeu majeur** pour le ministère.

L'offre d'hébergement du ministère comprend les centres nationaux (SG/SPSSI/CPIL, DGITM/DAM, DGAC), les centres locaux (DREAL, DIR, CROSS, CIGT...) ainsi que des centres d'hébergement externalisé dans le cadre de marchés.

Les exigences de sécurité définies dans ce document s'appliquent aux environnements non classifiés (de niveau **inférieur à confidentiel-défense**).

## 1.2 - Objectif de cette directive

La présente directive de sécurité de l'hébergement informatique s'inscrit dans la démarche de sécurisation des systèmes d'information du ministère et définit des **exigences de sécurité applicables et opposables aux centres d'hébergement**.

Elle vise à **améliorer le niveau de sécurité** des systèmes d'informations hébergés sur l'ensemble des centres d'hébergement du ministère, internes comme externes, et à **homogénéiser les pratiques** selon des exigences de sécurité conformes à la politique de sécurité des systèmes d'information de l'État (PSSIE).

Ces exigences précisent un **niveau de sécurité minimum** applicable qui peut être complété par des exigences supplémentaires lorsque cela est jugé nécessaire par les Maîtrises d'Ouvrage, les entités, ou les responsables des centres d'hébergement.

Les Maîtrises d'Ouvrage, les entités, et les responsables des centres d'hébergement définissent sur leur périmètre les dispositions à prendre (mesures opérationnelles, documents d'application...) pour application de la présente directive.

## 1.3 - Périmètre d'application de la directive

La présente directive s'inscrit dans le corpus documentaire SSI du ministère (cf. Instruction - Article 6) permettant de faciliter et/ou de préciser la mise en œuvre de la PGSSI V2.

Actualisée en réponse aux exigences de la PSSIE, elle **s'applique à l'ensemble des centres d'hébergement (internes et externes) qui hébergent des systèmes d'information d'une ou de plusieurs entités du ministère définies dans la PGSSI V2 (cf. Instruction – Article 2)**.

**Le chapitre «Exigences de sécurité vis-à-vis des hébergeurs externes» s'applique en complément pour les systèmes d'information hébergés chez des tiers.** La gestion des tiers au sens large devra être traitée par ailleurs et intégrée au corpus documentaire SSI (e.g. dans une «*Aide à la gestion des tiers*»).

Les thématiques abordés dans cette présente directive sont de type organisationnel et technique.

Thématiques organisationnelles	Thématiques techniques
<ul style="list-style-type: none"> <li>■ <b>Organisation de la sécurité des centres d'hébergement</b> (responsabilités en termes de sécurité de l'hébergement).</li> <li>■ <b>Organisation de l'exploitation</b> (gestion ressources humaines, sensibilisation, documentation)</li> <li>■ <b>Exigences dans le cas des hébergeurs externes</b> (exigences applicables au ministère et à aux hébergeurs externes)</li> </ul>	<ul style="list-style-type: none"> <li>■ <b>Sécurité physique</b> (protection incendie, climatisation, électricité, contrôles d'accès physique etc.).</li> <li>■ <b>Sécurité des infrastructures</b> (cloisonnement réseau, mutualisation/virtualisation, sécurité des équipes et des outils d'exploitation).</li> <li>■ <b>Continuité et secours de l'hébergement informatique</b> (sauvegarde, secours des données et des infrastructures)</li> </ul>

La directive sécurité de l'hébergement informatique ne traite pas des exigences de sécurité du développement. Elle mentionne néanmoins les conditions qui doivent être remplies par une application avant d'être mise en exploitation dans un centre d'hébergement. Ces conditions devront être traitées par ailleurs et intégrée au corpus documentaire SSI dans un document de déclinaison méthodologique, (e.g. «Méthodologie d'intégration de la sécurité dans les projets de développements d'applications»).

Les informations classées de niveau «Confidentiel-Défense» ou supérieur n'entrent pas dans le champ de la présente directive.

## 1.4 - Cycle de vie du document

La PGSSI V2 (Instruction – Article 7) précise que la sous-direction en charge de la politique des systèmes d'information établit et met à jour le corpus documentaire SSI dans son ensemble et les documents de référence complémentaires permettant de faciliter et/ou de préciser la mise en œuvre de la PGSSI V2.

La présente directive pourra être amenée à évoluer dans le temps.

En référence à la PGSSI V2 (cf. Instruction - Article 7), le processus de modification est le suivant :

- collecte par la sous-direction en charge de la politique des systèmes d'information des demandes d'évolution, qui peuvent émaner de tout service ayant un rôle de prescription sur les règles de sécurité à appliquer à l'hébergement informatique (Maîtrises d'Ouvrage, Responsables des centres d'hébergement...) ;
- proposition d'évolution par la sous-direction en charge de la politique des systèmes d'information ;
- validation de ces évolutions par le CSSI (Comité Sécurité des Systèmes d'Information).

Ces acteurs sont en charge de faire évoluer la présente directive afin de la maintenir constamment à jour au regard du contexte, des enjeux et des technologies déployées.

## 1.5 - Gestion des dérogations

En cas d'impossibilité justifiée de mise en application d'une exigence de la présente directive, une demande de dérogation doit être formalisée.

- La demande de dérogation est motivée par le demandeur, qui peut être en fonction de la nature de la dérogation un exploitant du centre d'hébergement, la maîtrise d'ouvrage métier ou toute personne à qui cette responsabilité aura été formellement déléguée (e.g.: responsable sécurité d'un centre d'hébergement).
- La demande de dérogation est instruite par la sous-direction en charge de la politique des systèmes d'information. L'avis du CSSI peut être requis en fonction du niveau de risque lié à la demande de dérogation.
- La décision de dérogation est soumise à la validation de la direction de l'entité auquel est rattaché le centre d'hébergement.

Le respect de ce processus permet de se prémunir contre l'introduction de failles de sécurité pouvant générer un risque de sécurité pour les systèmes d'information du ministère.

## 1.6 - Contrôle de mise en œuvre

Le contrôle de la mise en œuvre des exigences de sécurité de la présente directive rentre dans les dispositions que les entités sont tenues de mettre en place en application de la PGSSI V2 (cf. Instruction – Titre IV).

La mise en œuvre des règles de la présente politique doit donner lieu à la formalisation d'un plan de contrôle. Les contrôles doivent être conduits annuellement et donner lieu à un plan d'actions visant à corriger les éventuels manquements détectés. Les contrôles et le suivi de l'application du plan d'actions sont de la responsabilité de l'agent chargé du contrôle.

## 1.7 - Conventions

Les conventions suivantes sont adoptées dans ce document :

- Toutes les exigences de sécurité édictées dans le présent document sont numérotées et précédées de la mention « HEB » pour hébergement suivi d'un indicatif de trois lettres faisant référence au chapitre dans lesquelles elles figurent.

Par exemple, la deuxième exigence du chapitre *Organisation de la sécurité des centres d'hébergement* sera précédée de l'indicatif « HEB-ORG-02 ».

- Deux catégories de centres d'hébergement sont distinguées dans cette directive : les centres nationaux et les centres locaux. Pour chaque exigence de sécurité, il est précisé à quelle catégorie de centre d'hébergement elle s'applique.
- Les exigences de sécurité sont différenciées en **Directives** et **Recommandations**.
  - ▶ Une **Directive** est **impérative** et **doit être appliquée conformément à son contenu et aux conditions d'application** sur l'ensemble du périmètre des centres d'hébergement. La non-conformité à une directive doit avoir pour corollaire l'existence d'une dérogation ou d'un plan d'action.

Pour les exigences de sécurité considérées comme des directives, la lettre « D » apparaît dans la case correspondant au type de centre d'hébergement auquel elles s'appliquent.

- Une **Recommandation** s'applique le plus largement possible sur l'ensemble du périmètre des centres d'hébergement. Des contraintes spécifiques peuvent nécessiter d'y déroger. Dans ce cas, les conséquences techniques sont pleinement assumées par l'entité responsable de sa non-application. L'entité sera néanmoins amenée, dans le cadre des opérations de contrôle, à rendre compte de la raison pour laquelle elle n'applique pas une recommandation.

Pour les exigences de sécurité considérées comme des Recommandations, la lettre « R » apparaît dans la case correspondant au type de centre d'hébergement auquel elles s'appliquent.

Dans le cas ci-dessous, l'exigence s'applique aux centres d'hébergement nationaux et locaux. Cependant, le niveau d'exigence n'est pas le même selon le type de centre : il s'agit d'une directive pour les centres d'hébergement nationaux et d'une recommandation pour les centres d'hébergement locaux.

La référence N/A est considérée comme Non Applicable pour les centres d'hébergement locaux.

Exemple d'une exigence :

HEB-PHY-18 Redondance du système de climatisation	Local	National
La continuité du service de refroidissement des salles d'hébergement <b>doit</b> être assurée en cas d'un incident unique (panne d'électricité, panne d'un système de climatisation) ou d'une opération de maintenance.	<b>R</b>	<b>D</b>

- Les principaux termes utilisés dans le document figurent au glossaire en annexe 1.

## 2 - Enjeux relatifs à la sécurité de l'hébergement

### 2.1 - Enjeux relatifs aux centres d'hébergement informatiques

L'offre d'hébergement informatique est un ensemble de services délivrés par un centre d'hébergement du ministère et souscrits par un maître d'ouvrage (MOA).

Les centres d'hébergement hébergent les ressources<sup>1</sup> et les applications Métier nécessaires aux entités du ministère pour assurer leurs missions. Les centres doivent donc répondre aux enjeux de sécurité du ministère, notamment :

- **« des enjeux de sûreté nationale et de santé publique**, par exemple lors de la manipulation d'informations relatives à la sûreté de la navigation, à la sécurité industrielle, à l'environnement ;
- **des enjeux financiers et sociaux**, par exemple lors de la gestion des subventions pour le logement et l'habitat ;
- **des enjeux politiques et d'image du ministère**, par exemple en cas de fuite d'information ou de sanction prononcée par l'Union européenne, etc.
- **des enjeux d'organisation interne**, par exemple lors de la gestion des Ressources Humaines, de la comptabilité, du système d'information local, etc. »

<sup>1</sup> Ressource : cf. glossaire.

## 2.2 - Objectifs de sécurité des centres d'hébergement informatiques

L'offre d'hébergement informatique est le socle commun à tous les systèmes d'information du ministère, elle doit donc répondre globalement aux objectifs de sécurité définis dans de la PGSSI V2 en réponse aux exigences de la PSSI, notamment :

- «assurer la continuité des activités du ministère» ;
- «prévenir la fuite d'informations sensibles» ;
- «renforcer la confiance des citoyens et des entreprises dans les téléprocédures.»

Ces objectifs de sécurité doivent être adaptés :

- **aux contraintes d'exploitation** : le bon fonctionnement des applications étant l'objectif premier des services rendus par un centre d'hébergement ;
- **aux enjeux propres de chaque application** exprimés par la maîtrise d'ouvrage.

Les exigences de sécurité de la présente directive visent à répondre à l'ensemble de ces enjeux et objectifs.

## 3 - Organisation de la sécurité des centres d'hébergement

Cette partie du document résume les dispositions définies dans la PGSSI V2 en terme d'organisation de la sécurité des systèmes d'information au sein du ministère, elle précise certaines exigences à prendre en compte spécifiquement lors de la définition de l'organisation de la sécurité des centres d'hébergement.

La sécurité de l'hébergement informatique implique différentes activités du ministère

- les centres d'hébergement internes (nationaux ou locaux), les centres externes hébergeant les SI du ministère ;
- les instances en charge de la sécurité des systèmes d'information pour l'ensemble du ministère.

Les exigences définies dans cette directive s'appliquent à l'ensemble de ces acteurs, en particulier aux exploitants des centres d'hébergement.

### 3.1 - Direction de l'entité

La direction de l'entité est responsable de la mise en œuvre de la PGSSI V2 au sein de l'entité.

### 3.2 - Responsable sécurité du centre d'hébergement

Le «responsable sécurité du centre d'hébergement» :

- apporte son assistance aux maîtres d'œuvre, aux exploitants et administrateurs de son périmètre pour la mise en œuvre de la directive de sécurité de l'hébergement informatique ;
- s'assure que les informations et la documentation relatives à la sécurité des systèmes d'information sont diffusées et connues des personnes concernées ;
- s'assure que les personnes impliquées dans l'exploitation ou l'administration technique d'un système d'information reçoivent la formation appropriée dans le domaine de la sécurité et lorsque nécessaire propose des actions de sensibilisation ;
- est l'interlocuteur privilégié de l'entité en charge des contrôles/inspections menés sur son périmètre de responsabilité.

HEB-ORG-1 Nomination d'un « responsable sécurité du centre d'hébergement »	Local	National
<p>Un « responsable sécurité du centre d'hébergement » <b>doit</b> être nommé pour chaque centre d'hébergement.</p> <p><i>Plusieurs centres d'hébergement peuvent être sous la responsabilité d'un même responsable sécurité.</i></p>	<b>D</b>	<b>D</b>

Son directeur formalise cette nomination via une **lettre de mission** et en notifie les instances en charge de la sécurité des systèmes d'information au sein du ministère.

HEB-ORG-2 Bilan de conformité annuel à la directive	Local	National
<p>Le « responsable sécurité du centre d'hébergement » <b>doit</b> réaliser annuellement un bilan de conformité afin de contrôler l'application par son centre des exigences de sécurité définies dans ce document.</p> <p>Ce bilan est piloté par le « responsable sécurité du centre d'hébergement »</p> <p>Il <b>doit</b> fournir le bilan annuel aux acteurs en charge de la sécurité des systèmes d'information au sein du ministère, notamment au bureau en charge de la sécurité des SI, de l'hébergement et des référentiels techniques.</p> <p>Les bilans de conformité <b>doivent</b> donner lieu à la formalisation d'un plan d'actions visant à corriger les éventuels manquements détectés.</p>	<b>D</b>	<b>D</b>

Remarque : Le bilan de conformité devrait être détaillé de manière à fournir un état des lieux précis des pratiques sécurité et permettrait d'apporter aux MOA métier une vision précise du niveau de sécurité du centre d'hébergement.

HEB-ORG-3 Évaluation de la sensibilité des centres d'hébergement	Local	National
<p>Le « responsable sécurité du centre d'hébergement » <b>doit</b> régulièrement évaluer la sensibilité de son centre.</p> <p>Cette sensibilité est déterminée en fonction des besoins de sécurité des applications (cf. définition ci-dessous) hébergées et de l'exposition du centre d'hébergement à Internet.</p> <p>L'échelle utilisée pour évaluer la sensibilité est composée de deux niveaux :</p> <ul style="list-style-type: none"> <li>■ <b>Local</b> : correspondant aux centres qui n'ont pas de connexion locale à Internet<sup>2</sup> et qui hébergent exclusivement des applications dont les besoins de sécurité sont de niveau inférieur ou égal à 3 sur le critère Disponibilité, 2 sur le critère Intégrité, 2 sur le critère Confidentialité et 2 sur le critère Traçabilité.</li> <li>■ <b>National</b> : correspondant aux centres qui ont une connexion locale à Internet ou qui hébergent au moins une application dont les besoins de sécurité sont de niveau supérieur ou égal à 4 sur le critère Disponibilité, 3 sur le critère Intégrité, 3 sur le critère Confidentialité ou 3 sur le critère Traçabilité.</li> </ul>	<b>D</b>	<b>D</b>

<sup>2</sup>

Connexion locale à Internet : cf. glossaire

Ainsi, un centre d'hébergement disposant d'une connexion locale à Internet doit nécessairement appliquer les exigences des centres d'hébergement dits «nationaux».

En l'absence de connexion locale à Internet, un centre d'hébergement est «national» si et seulement si au moins une de ses applications a des besoins de sécurité de niveau supérieur ou égal à DICT= 4333.

Dans tous les autres cas, le centre d'hébergement est considéré comme local.

La classification en fonction de la sensibilité des centres d'hébergement est rappelée en annexe 2 du présent document.

HEB-ORG-4 Déclinaison de la directive en documents d'application	Local	National
Le « responsable sécurité du centre d'hébergement » <b>doit</b> décliner pour son centre la présente directive en documents d'application locaux permettant d'en faciliter la mise en œuvre.	<b>D</b>	<b>D</b>

Ces documents d'application peuvent être de différentes formes :

- note de service, note d'organisation de la sécurité sur le centre d'hébergement ;
- modes opératoires (e.g. configuration sécurisée d'un serveur) ;
- procédures opérationnelles, (e.g. traitement des incidents de sécurité, sauvegarde...) ;
- dossier d'exploitation, plan de continuité informatique.

### 3.3 - Exploitants d'un centre d'hébergement informatique

Comme précisé dans l'annexe A de la PGSSI V2, les exploitants d'un centre d'hébergement informatique « assurent le fonctionnement des systèmes d'information hébergés sur leur périmètre. Ils définissent les procédures de gestion et administrent les ressources pour en assurer la cohérence, la qualité et la sécurité ».

Les exploitants :

- « apportent leur compétence au maître d'ouvrage et au maître d'œuvre dans le cadre de la définition des exigences de sécurité de chaque système d'information et des dispositions à prendre pour satisfaire ces exigences ;
- font appliquer ou appliquent les dispositions prises pour satisfaire les exigences de sécurité et, à cette fin, affectent les ressources requises ;
- signalent tout incident de sécurité affectant un système d'information selon les canaux définis à cette fin, en informent le maître d'ouvrage et mettent tout en œuvre pour le résoudre ;
- procèdent, à leur initiative ou sur demande motivée des acteurs de sécurité concernés, aux investigations suite à un incident de sécurité ou nécessaires à prévenir un incident ;
- apportent leur collaboration et toute contribution nécessaire au bon déroulement des contrôles de sécurité ».

L'exploitant « définit et met en œuvre, le cas échéant, les actions correctives de son ressort :

- nécessaires à la correction de non-conformités identifiées lors de contrôles/inspections ;
- identifiées suite à des incidents de sécurité ».

L'exploitant n'effectue, à son initiative ou sur demande hiérarchique, aucune exploitation des systèmes d'information à des fins autres que celles liées au bon fonctionnement et à la sécurité des systèmes d'information.

En particulier, il s'attache à respecter la confidentialité des informations auxquelles il peut accéder dans le cadre de ses missions et notamment aux informations personnelles des utilisateurs ».

HEB-ORG-5 Évaluation des besoins de sécurité des applications	Local	National
<p>Avant toute mise en production d'une application (ou mise en sites pilote, formation, qualification/pré-production), et le plus tôt possible avant le déroulement de l'opération, le « responsable sécurité du centre d'hébergement » et les exploitants du centre d'hébergement <b>doivent</b> obtenir de la Maîtrise d'Ouvrage l'évaluation des besoins de sécurité SI et les objectifs de sécurité y afférant.</p>	<b>D</b>	<b>D</b>

Cette évaluation sera effectuée conformément aux principes mentionnés dans un document de déclinaison méthodologique (e.g. « Méthodologie d'intégration de la sécurité dans les projets de développements d'applications »)

HEB-ORG-6 Évolution des besoins de sécurité des applications	Local	National
<p>Le « responsable sécurité du centre d'hébergement » et les exploitants du centre d'hébergement <b>doivent</b> demander à la Maîtrise d'Ouvrage si les besoins de sécurité de son application évoluent.</p> <p>Une révision des besoins de sécurité doit avoir lieu au minimum tous les 2 ans.</p>	<b>D</b>	<b>D</b>

HEB-ORG-7 Contrôle du respect des exigences de développement et d'intégration	Local	National
<p>Le « responsable sécurité du centre d'hébergement » et les exploitants du centre d'hébergement <b>doivent</b> mettre en place les mesures nécessaires afin de respecter les exigences de développement et d'intégration définies dans un document de déclinaison méthodologique (e.g.« Méthodologie d'intégration de la sécurité dans les projets de développements d'applications »).</p> <p>En particulier, ils doivent collaborer avec la Maîtrise d'Ouvrage lors d'audits de sécurité.</p>	<b>D</b>	<b>D</b>

## 4 - Exigences de sécurité

### 4.1 - Sécurité de l'infrastructure informatique

#### 4.1.1 - Sécurité des réseaux

##### Sécurité des réseaux nationaux

HEB-INF-1 Interconnexions avec des réseaux externes	Local	National
Toute interconnexion télécoms entre les réseaux locaux du ministère et des réseaux externes (Internet, connexions locales avec des tiers) <b>doit</b> être réalisée via les infrastructures nationales proposées par le ministère.		
Par définition, les interconnexions à Internet sans passer par les infrastructures nationales sont interdites pour les centres d'hébergement «locaux ».	D	D
Une demande de dérogation à cette règle dûment motivée et adressée au bureau en charge de la sécurité des SI, de l'hébergement et des référentiels techniques doit être instruite.		

##### Sécurité des réseaux sans fil

HEB-INF-2 Mise en place de réseaux sans fil	Local	National
Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées par le HFDS, doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio.	D	D
A défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des SI manipulant des données sensibles est proscrit.		

## 4.1.2 - Filtrage et cloisonnement<sup>3</sup>

Le filtrage porte sur :

- le filtrage en entrée du centre d'hébergement visant à protéger les ressources hébergées des réseaux Internet, des connexions locales avec des tiers et des réseaux internes du ministère ;
- le filtrage en sein du centre d'hébergement visant à protéger les ressources hébergées l'une de l'autre, afin notamment d'éviter la propagation d'un incident de sécurité.

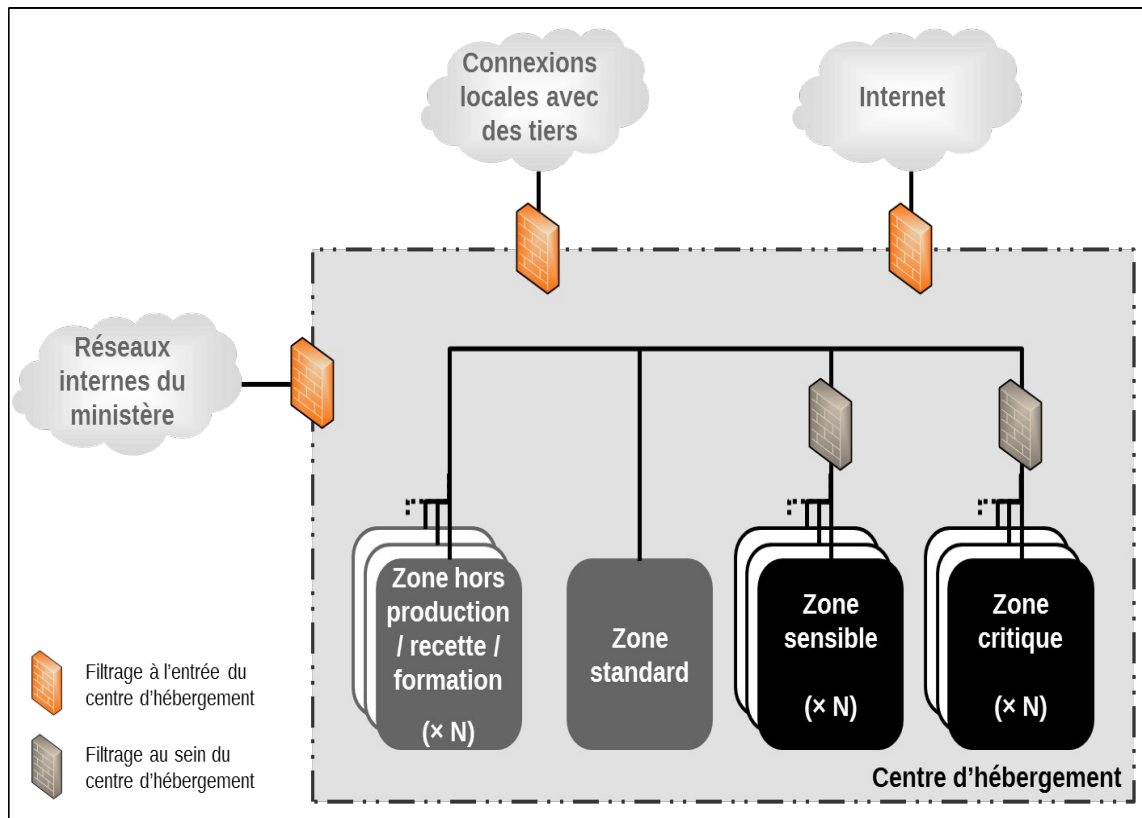


Figure 1 : Filtrage en entrée et au sein d'un centre d'hébergement

HEB-INF-3 Homologation des ouvertures/fermetures de flux	Local	National
Une procédure d'homologation des ouvertures et fermetures de flux <b>doit</b> être formalisée par le « responsable sécurité du centre d'hébergement ».	<b>R</b>	<b>D</b>

*La procédure d'homologation pourra préciser par exemple que : chaque demande d'ouverture de flux doit être tracée, une matrice des flux autorisés doit être formalisée, une analyse de risques spécifique doit être réalisée pour tout flux non autorisé, des revues des règles de filtrage doivent être réalisées chaque année.*

*Elle pourra préciser également*

- *que tous les flux non autorisés sont interdits ;*
- *la stratégie de filtrage utilisée : filtrage par sous réseau ou adresse IP par adresse IP.*

<sup>3</sup> Cloisonnement : cf. glossaire.

#### 4.1.2.1 - Filtrage en entrée du centre d'hébergement

### Filtrage réseau des flux en entrée du centre d'hébergement

Ces exigences visent à réduire au strict nécessaire la visibilité réseau des ressources d'un centre d'hébergement depuis l'externe (Internet, connexions locales avec des tiers) et l'interne (réseaux internes du ministère). La réduction de la surface d'exposition des ressources d'un centre d'hébergement permet de diminuer drastiquement le risque de leur compromission.

**Le filtrage réseau est typiquement réalisé par un pare-feu.**

HEB-INF-4 Filtrage réseau des flux provenant d'Internet	Local	National
<p>Tout flux provenant d'Internet <b>doit</b> être filtré au niveau réseau par deux équipements physiquement distincts et issus de constructeurs différents :</p> <ul style="list-style-type: none"><li>■ le premier équipement permettant de filtrer les accès entre Internet et les zones de sécurité<sup>4</sup> qui hébergent les ressources accessibles directement depuis Internet ;</li><li>■ le deuxième équipement permettant de filtrer les accès entre ces zones de sécurité et le réseau interne du centre d'hébergement qui héberge les applications et les bases de données.</li></ul>	N/A	D
HEB-INF-5 Filtrage des flux provenant d'une connexion locale avec un tiers	Local	National
<p>Tout flux provenant d'une connexion locale avec un tiers <b>doit</b> être filtré au niveau réseau en entrée du centre d'hébergement.</p>	D	D
HEB-INF-6 Filtrage des flux provenant d'un réseau interne du ministère	Local	National
<p>Tout flux provenant d'un réseau interne du ministère <b>doit</b> être filtré au niveau réseau en entrée du centre d'hébergement.</p>	D	D
HEB-INF-7 Non mutualisation des pare-feux	Local	National
<p>Le premier équipement<sup>5</sup> filtrant les flux externes (provenant d'Internet ou des connexions locales avec des tiers) ne <b>doit</b> pas être mutualisé avec l'équipement filtrant les flux internes (flux provenant des réseaux internes du ministère).</p>	D	D

<sup>4</sup> Zone de sécurité : cf. glossaire.

<sup>5</sup> cf. exigence HEB-INF-5

## Relais des flux en entrée du centre d'hébergement

Le relais permet de réaliser la coupure de flux et de retransmettre un flux après y avoir réalisé éventuellement des modifications (exemple : réécriture d'URL).

Cette exigence vise à limiter l'exposition des ressources hébergées aux attaques à travers les couches réseaux ou applicatives par mise en œuvre d'une rupture de flux entre différentes zones de sécurité.

*Exemple d'équipement de relais : reverse-proxy http pour les flux http.*

HEB-INF-8 Relais des flux en provenance d'Internet	Local	National
Tout flux provenant d'Internet <b>doit</b> être relayé en entrée du centre d'hébergement.	N/A	D
HEB-INF-9 Relais des flux en provenance d'une connexion locale avec un tiers	Local	National
Tout flux provenant d'une connexion locale avec un tiers <b>doit</b> être relayé en entrée du centre d'hébergement.	D	D
HEB-INF-10 Non mutualisation des équipements de relais	Local	National
Les équipements de relais des flux provenant d'Internet, de connexions locales avec des tiers et des réseaux internes du ministère ne <b>doivent</b> pas être mutualisés.	D	D

## Filtrage applicatif des flux en entrée du centre d'hébergement

Le filtrage applicatif permet de protéger les composants applicatifs contre certains défauts de conception, erreurs de configuration ou détournement d'usage en réalisant des contrôles sur les flux applicatifs échangés.

Des mécanismes de déchiffrement / chiffrement permettent d'effectuer ce type de contrôles sur les flux chiffrés.

HEB-INF-11 Filtrage applicatif des flux en provenance d'Internet	Local	National
Tout flux provenant d'Internet <b>doit</b> faire l'objet d'un filtrage applicatif en entrée du centre d'hébergement. Le filtrage applicatif <b>doit</b> être adapté aux besoins de sécurité des ressources protégées.	N/A	D
HEB-INF-12 Filtrage applicatif des flux en provenance d'une connexion locale avec un tiers	Local	National
Tout flux provenant d'une connexion locale avec un tiers <b>doit</b> faire l'objet d'un filtrage applicatif en entrée du centre d'hébergement. Le filtrage applicatif <b>doit</b> être adapté aux besoins de sécurité des ressources protégées.	D	D

HEB-INF-13 Non mutualisation des équipements de filtrage applicatif	Local	National
Les équipements de filtrage applicatif des flux provenant d'Internet, de connexions locales avec des tiers et des réseaux internes du ministère ne <b>doivent</b> pas être mutualisés.	<b>D</b>	<b>D</b>

Exemple de filtrage applicatif : contrôle de conformité protocolaire, filtrage sur base de signatures d'attaques applicatives connues, contrôle par liste noire ou liste blanche sur certaines variables utilisées dans les échanges applicatifs...).

Dans le cas des applications Web, la mise en place d'un pare-feu HTTP permet de fiabiliser les échanges en vérifiant la longueur des URL et les paramètres utilisés (en filtrant notamment les séquences Unicode dangereuses, les possibilités d'injection de code SQL...).

## Détection des intrusions en entrée du centre d'hébergement

HEB-INF-14 Détection d'intrusion	Local	National
Un dispositif de détection / prévention d'intrusion <b>doit</b> être mis en place pour protéger les ressources accessibles depuis Internet.	<b>R</b>	<b>D</b>

Exemples de dispositif de détection d'intrusion :

- sonde de détection / prévention d'intrusion permettant de détecter et prévenir les tentatives d'intrusion sur le centre d'hébergement par repérage des activités anormales ou suspectes en écoutant les flux entrants sur le centre d'hébergement. L'écoute est transparente pour les utilisateurs ;
- analyse de journaux permettant de détecter les comportements anormaux par la revue régulière des journaux ou la mise en place d'alertes.

### 4.1.2.2 - Cloisonnement au sein du centre d'hébergement

Le **cloisonnement** consiste à confiner des ressources du système d'information dans des **zones de sécurité** spécifiques (ou segment réseau) et à contrôler les communications entre les ressources situées sur des zones de sécurité distinctes. La qualité du contrôle (e.g. filtrage réseau, relais et filtrage applicatif) est alors adaptée aux besoins de sécurité des communications.

Les ressources positionnées sur une même zone de sécurité peuvent communiquer entre elles sans restriction.

On distingue dans cette directive différents types de zones de sécurité pour héberger les applications en production/sites pilotes ou sur des environnements de formation :

- la zone de sécurité dite « standard » : elle héberge les applications qui ne sont ni identifiées sensibles, ni jugées dangereuses ;
- les zones de sécurité dites « sensibles » : elles hébergent les applications dont les besoins de sécurité sont égaux à 3 ou 4 sur le critère Intégrité ou Confidentialité. Ces zones permettent de mettre en place un niveau de sécurité renforcé sur les applications les plus critiques du ministère.

*Il est possible d'avoir plusieurs zones de sécurité sensibles dans un centre d'hébergement.*

- Les zones de sécurité dites « critiques »: elles hébergent les applications jugées dangereuses par les exploitants du centre d'hébergement. Elles permettent d'éviter la propagation d'un incident de sécurité sur tout le centre d'hébergement en cas de corruption d'une telle application.

*Il est possible d'avoir plusieurs zones de sécurité dites « critiques » dans un centre d'hébergement.*

Une application peut être considérée comme dangereuse notamment dans les cas suivants :

- ▶ application vulnérable à des failles de sécurité référencées ;
- ▶ application dont la technologie n'est pas maîtrisée par les exploitants des centres d'hébergement ;
- ▶ application dont la configuration n'est pas sécurisée ;
- ▶ application qui ne respecte pas la « Méthodologie d'intégration de la sécurité dans les projets de développements d'applications » ;
- ▶ application sur laquelle des connexions à privilège non maîtrisées sont effectuées par des tiers.

Un audit peut éventuellement être réalisé sur une application par le centre d'hébergement pour déterminer son niveau de dangerosité.

Une application est installée sur une zone de sécurité dite « critique » sur proposition des exploitants. Un arbitrage doit avoir lieu entre la MOA et le responsable sécurité du centre d'hébergement. La décision est validée par le responsable sécurité des systèmes d'information de l'entité de la MOA.

Le choix du nombre de zones dites « critiques » et/ou dites « sensibles » revient à chaque centre d'hébergement en fonction de son environnement et de ses contraintes propres.

Les environnements hors production/site pilote/formation (développement, recette, qualification...) sont sauf exception sur des zones de sécurité distinctes de la production/site pilote/formation.

Les couches « base de données » et « application / présentation » des applications sensibles peuvent être cloisonnées sur des zones de sécurité différentes.

Cette séparation n'est pas imposée dans cette directive : elle est à réaliser au cas par cas suivant les conclusions de l'analyse de risques effectuée lors de la phase projet.

<b>HEB-INF-15 Cloisonnement par filtrage entre les zones de sécurité du centre d'hébergement</b>	Local	National
Chaque zone de sécurité du centre d'hébergement <b>doit</b> être cloisonnée du reste du centre d'hébergement par du filtrage	<b>R</b>	<b>D</b>

Exemple : une zone de sécurité dite « critique » doit être cloisonnée d'une zone de sécurité dite « standard ».

<b>HEB-INF-16 Cloisonnement des applications sensibles</b>	Local	National
Une application dont les besoins de sécurité sont égaux à 3 ou 4 sur le critère intégrité ou confidentialité <b>doit</b> être hébergée sur une zone de sécurité dite « sensible ».	<b>R</b>	<b>D</b>

Deux applications sensibles peuvent être positionnées soit sur une même zone de sécurité dite « sensible », soit sur plusieurs zones de sécurité « sensibles » distinctes. Ce choix doit être réalisé au cas par cas en fonction des conclusions des analyses de risques.

<b>HEB-INF-17 Cloisonnement des ressources dangereuses</b>	Local	National
Une application jugée dangereuse <b>doit</b> être hébergée sur une zone de sécurité dite « critique ».	<b>D</b>	<b>D</b>

Deux applications dangereuses peuvent être positionnées soit sur une même zone de sécurité dite « critique », soit sur plusieurs zones de sécurité dites « critiques » distinctes. Ce choix doit être réalisé au cas par cas en fonction des conclusions des analyses de risques.

<b>HEB-INF-18 Cloisonnement des ressources hors production / site pilote / formation</b>	Local	National
Les applications hors production / site pilote / formation (développement, recette, pré-production...) <b>doivent</b> être hébergées sur des zones de sécurité distinctes de celles de production /site pilote / formation, sauf si celles-ci sont aussi « sensibles » que la production/site pilote/formation.	<b>R</b>	<b>D</b>

<b>HEB-INF-19 Interconnexion des sites géographiques locaux d'une entité</b>	Local	National
L'interconnexion au niveau local de réseaux locaux d'une entité n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet, et de passerelles sécurisées et validées par le HFDS.	<b>D</b>	<b>D</b>

<b>HEB-INF-20 Cloisonnement des ressources en cas de partage des locaux</b>	Local	National
Dans le cas où une entité partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées par le HFDS.	<b>D</b>	<b>D</b>

<b>HEB-INF-21 Accès réseau en zone d'accueil du public</b>	Local	National
Tout accès réseau installé dans une zone d'accueil du public doit être filtré ou isolé du reste du réseau informatique de l'entité.	<b>D</b>	<b>D</b>

### 4.1.3 - Sécurité de l'exploitation

La sécurité de l'exploitation des ressources hébergées dans les centres d'hébergement repose sur les sous-thématiques suivantes :

- filtrage des équipes d'exploitation, des outils, et des services réseaux d'exploitation ;
- traçabilité des opérations réalisées par les exploitants ;
- gestion des habilitations délivrées aux exploitants ;
- gestion des comptes de service utilisés par les systèmes et les applications ;
- protocoles d'exploitation utilisés ;
- sécurité de l'exploitation à distance (astreinte).

On entend par exploitation toutes les opérations permettant le maintien en conditions opérationnelles des ressources (e.g. administration, supervision, sauvegarde).

HEB-INF-22 Centralisation de la gestion du système d'information	Local	National
Afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements réseau, les administrateurs doivent utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information.	R	D

#### Filtrage des équipes d'exploitation, des outils et des services réseaux d'exploitation

HEB-INF-23 Réseau dédié à l'exploitation	Local	National
Les exploitants <b>devraient</b> être positionnés sur un réseau dédié à l'exploitation et cloisonné des autres réseaux afin de protéger les postes de travail des exploitants.	R	R

Le cloisonnement des outils d'exploitation (serveur de rebond, console d'administration pare-feu, robot de sauvegarde...) sur une ou plusieurs zones de sécurité dédiées à l'exploitation permet de protéger ces équipements critiques contre des actes malveillants.

HEB-INF-24 Flux d'administration	Local	National
D'une manière générale, il convient de différencier deux type de flux d'administration : <ul style="list-style-type: none"><li>■ les flux d'administration de l'infrastructure (réservés aux agents du centre informatique) d'une part ;</li><li>■ les flux d'administration des applications métier (réservés à la direction métier) d'autre part.</li></ul> L'attribution des droits d'administration doit respecter cette différenciation, et les 2 types de flux d'administration devraient être cloisonnés.	R	R

HEB-INF-25 Cloisonnement des outils d'exploitation	Local	National
<p>Les outils d'exploitation <b>doivent</b> être cloisonnés dans des zones de sécurité dédiées aux outils d'exploitation.</p> <p>Les robots de sauvegarde peuvent être placés directement sur les zones de production/site pilote/formation pour des raisons de performance.</p> <p>Pour les outils d'exploitation critiques, un cloisonnement plus fin <b>devrait</b> être mis en place.</p>	<b>R</b>	<b>D</b>

HEB-INF-26 Architecture de stockage et de sauvegarde	Local	National
<p>Le réseau de stockage/sauvegarde pour les besoins des centres d'hébergement informatiques repose sur une architecture dédiée à cet effet.</p>	<b>R</b>	<b>D</b>

Cette architecture peut reposer sur des équipements physiques dédiés au stockage et à la sauvegarde ou être virtualisée.

HEB-INF-27 Cloisonnement des services d'exploitation	Local	National
<p>Seules les équipes d'exploitation ou les outils d'exploitations <b>doivent</b> être autorisés par les équipements de filtrage à accéder aux services ouverts sur les ressources réseau utilisés dans le cadre de l'exploitation.</p>	<b>D</b>	<b>D</b>

A titre d'exemple, l'architecture suivante répond aux exigences de sécurité liées au cloisonnement.

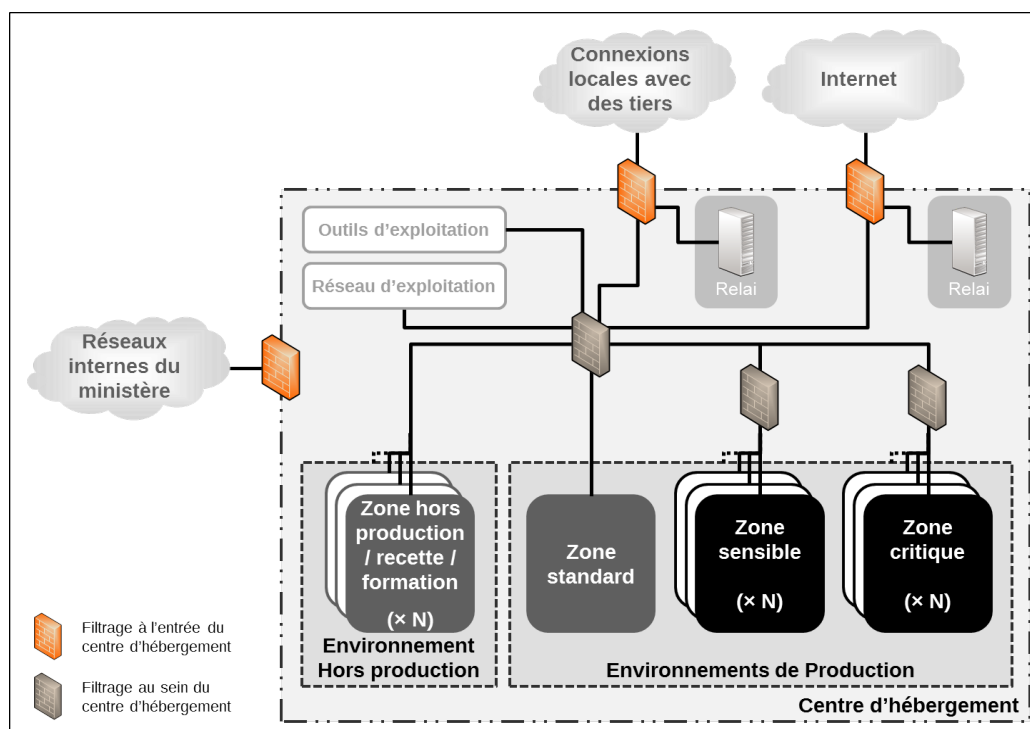


Figure 2 : Exemple d'implémentation des exigences de sécurité liées au cloisonnement

HEB-INF-28 Cloisonnement des flux de supervision et d'administration	Local	National
Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place.	R	R

## Traçabilité des opérations réalisées par les exploitants

La **traçabilité des opérations réalisées par les exploitants** permet de dissuader tout acte malveillant de la part d'un exploitant.

Ces exigences de journalisation des opérations d'exploitation relèvent plus généralement de la mise en œuvre d'un système de journalisation efficace et sécurisé, détaillée dans la note technique de l'ANSSI intitulée « *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation* (No DAT-NT-012/ANSSI/SDE/NP) »).

HEB-INF-29 Journalisation des opérations d'exploitation	Local	National
Une journalisation des opérations d'exploitation <b>doit</b> être mise en place.		
Les journaux <b>doivent</b> comporter <i>a minima</i> la date, l'heure et le type d'opération effectuée.	R	D
Les ressources <b>doivent</b> être synchronisées sur les serveurs de temps du ministère.		

La référence de temps commune (service Network Time Protocol – NTP) permet d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité.

HEB-INF-30 Gestion de la journalisation	Local	National
Toute modification des journaux par les administrateurs <b>devrait</b> être empêchée.		
Les journaux <b>devraient</b> être régulièrement analysés et faire l'objet d'une procédure de remontée d'incident.		
Les journaux <b>doivent</b> être régulièrement sauvegardés voire archivés en fonction des besoins de traçabilité exigés et en conformité avec les contraintes réglementaires.	R	D
De manière plus large, les événements applicatifs <b>doivent</b> être « journalisés », protégés et archivés conformément aux besoins exprimés par les maîtrises d'ouvrage.		

La centralisation des journaux et la sécurisation du serveur central de journalisation est un moyen de limiter les modifications.

L'historisation des traces permet une analyse a posteriori des incidents de sécurité.

HEB-INF-31 Serveur de rebond	Local	National
Un serveur de rebond <b>devrait</b> être utilisé pour toute action d'administration.		
Un serveur de rebond permet de centraliser l'ensemble des actions réalisées par les administrateurs : il authentifie les administrateurs, leur attribue des accès aux ressources et trace leurs actions.	<b>R</b>	<b>D</b>

## Gestion des habilitations délivrées aux exploitants

Un compte d'exploitation permet à un exploitant de réaliser des opérations (administration, supervision, sauvegarde...) sur les ressources de son périmètre de responsabilité.

HEB-INF-32 Restriction des accès exploitant	Local	National
L'accès aux outils et interfaces d'exploitation <b>doit</b> être strictement limité aux personnes habilitées et fourni sur la base du besoin d'en connaître <sup>6</sup> .	<b>D</b>	<b>D</b>

HEB-INF-33 Comptes d'exploitation personnels	Local	National
Les exploitants <b>doivent</b> être identifiés par un compte d'exploitation nominatif.	<b>D</b>	<b>D</b>

Exemples d'implémentation de l'exigence :

- configuration sur chaque ressource de comptes nominatifs pour chaque exploitant ;
- centralisation des comptes nominatifs sur un serveur de rebond.

HEB-INF-34 Profils d'exploitation	Local	National
Les droits d'accès attribués à un compte d'exploitation <b>doivent</b> correspondre à un profil d'exploitation prédéfini.	<b>R</b>	<b>D</b>

HEB-INF-35 Accréditation des habilitations	Local	National
Toute habilitation <b>doit</b> être effectuée via un processus formalisé qui permet d'assurer la traçabilité des demandes et des validations.	<b>D</b>	<b>D</b>

HEB-INF-36 Politique de mot de passe relative aux comptes d'exploitation	Local	National
Une politique de mot de passe <b>doit</b> être formalisée et appliquée pour les comptes d'exploitation.	<b>D</b>	<b>D</b>

<sup>6</sup> Besoin d'en connaître : chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès.

HEB-INF-37 Authentification forte pour l'administration des serveurs sensibles	Local	National
Des mécanismes d'authentification forte <b>doivent</b> être utilisés pour l'administration des serveurs dont les besoins de sécurité sont de niveaux 3 ou 4 sur un des critères Intégrité, Confidentialité, Traçabilité.	<b>R</b>	<b>D</b>

Exemple de mécanisme d'authentification forte : token, cartes à puces, clés privées...

*Remarque : pour homogénéiser les pratiques d'exploitation, les centres d'hébergement ont la possibilité d'appliquer sur tous les serveurs les exigences de sécurité initialement exigées sur les serveurs les plus critiques.*

HEB-INF-38 Génération d'alertes en cas de tentative d'intrusion sur un compte d'exploitation	Local	National
Une série d'échecs d'authentification successifs sur un compte d'exploitation <b>doit</b> générer une alerte automatique auprès des exploitants du centre d'hébergement et verrouiller le compte.	<b>R</b>	<b>D</b>

Les seuils d'alerte et de blocage du compte sont à définir en fonction des besoins de sécurité de la ressource impactée. Ces seuils peuvent être différents mais ne doivent pas excéder cinq tentatives infructueuses.

HEB-INF-39 Protection des moyens d'authentification des exploitants	Local	National
Le caractère personnel des <b>moyens d'authentification des exploitants doit</b> être protégé à tout moment.	<b>D</b>	<b>D</b>

Exemple de moyens d'authentification : mots de passe, tokens, mots de passe administrateurs de secours (stockés dans un coffre sécurisé).

HEB-INF-40 Modification / suppression des habilitations	Local	National
En cas de mutation/départ d'un exploitant, ses habilitations <b>doivent</b> être ajustées ou supprimées en fonction des besoins de sa nouvelle fonction.	<b>D</b>	<b>D</b>

HEB-INF-41 Revues des habilitations logiques des exploitants	Local	National
Une liste des comptes d'exploitation activés et des profils d'accès associés <b>doit</b> être tenue à jour.		
Des contrôles <b>doivent</b> être effectués tous les 6 mois sur l'ensemble des systèmes afin de revoir les habilitations des exploitants.	<b>D</b>	<b>D</b>

Les opérations de contrôle devront notamment pouvoir détecter et supprimer :

- les comptes redondants ;
- la présence de comptes avec des privilèges inadéquats ;
- les comptes inactifs ou obsolètes.

## Gestion des comptes de service

Les comptes de service sont utilisés :

- En local sur un système pour exécuter un service.  
*Exemple : compte système « tomcat » utilisé pour exécuter le service tomcat.*
- Par les systèmes ou les applicatifs pour se connecter sur un autre système ou une autre brique applicative.  
*Exemple : compte « FTP-appli1 » utilisé par une application pour s'authentifier sur un service FTP hébergé dans le centre d'hébergement.*

HEB-INF-42 Comptes de service non partagés	Local	National
Les comptes de service ne <b>doivent</b> pas être partagés entre plusieurs serveurs et ne <b>doivent</b> pas être utilisés par un exploitant.	<b>D</b>	<b>D</b>

HEB-INF-43 Droits d'accès limités	Local	National
Les droits d'accès attribués à un compte de service <b>doivent</b> être fournis sur la base du besoin d'en connaître.	<b>D</b>	<b>D</b>

HEB-INF-44 Authentification par certificat aux comptes de service	Local	National
Une authentification par certificat doit être privilégiée pour l'accès aux comptes de services.	<b>D</b>	<b>D</b>

HEB-INF-45 Politique de mot de passe relative aux comptes de service	Local	National
Une politique de mot de passe <b>doit</b> être formalisée et appliquée pour les comptes de service.	<b>D</b>	<b>D</b>

La politique de mot de passe doit être adaptée aux problématiques liées aux comptes de service : la complexité à modifier régulièrement les mots de passe des comptes de service doit être compensée par la mise en place de mots de passe très robustes.

HEB-INF-46 Génération d'alertes en cas de tentative d'intrusion sur un compte de service	Local	National
Une série d'échecs d'authentification successifs sur un compte de service <b>doit</b> générer une alerte automatique auprès des exploitants du centre d'hébergement Le seuil de l'alerte est à définir en fonction des besoins de sécurité de la ressource impactée.	<b>R</b>	<b>D</b>

HEB-INF-47 Protection des mots de passe	Local	National
La confidentialité des mots de passe des comptes de service <b>doit</b> être protégée à tout moment.	<b>D</b>	<b>D</b>

HEB-INF-48 Revues des habilitations logiques des comptes de service	Local	National
Des contrôles <b>doivent</b> être effectués régulièrement sur l'ensemble des ressources afin de revoir les comptes de service existants.	<b>D</b>	<b>D</b>

HEB-INF-49 Messagerie technique	Local	National
Pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, une messagerie dite technique peut être déployée en zone de Back-office du centre d'hébergement informatique. Cette messagerie technique doit être réservée aux exploitants et ne doit pas être interconnectée avec l'extérieur.	<b>R</b>	<b>R</b>

## Protocoles d'exploitation

HEB-INF-50 Protocoles d'exploitation	Local	National
Les protocoles d'exploitation utilisés <b>doivent</b> protéger en confidentialité toute donnée sensible échangée.	<b>D</b>	<b>D</b>
Les éléments d'authentification et les actions d'administration sont considérés comme sensibles.		

Exemple : les protocoles SSH et HTTPS doivent être **préférés** aux protocoles telnet et HTTP.

## Sécurité de l'exploitation à distance

HEB-INF-51 Accès distant des exploitants internes	Local	National
Tout accès d'un exploitant interne en situation de nomadisme <b>doit</b> faire l'objet des mesures de protection suivantes :		
<ul style="list-style-type: none"> <li>■ authentification forte sur l'infrastructure d'accès nomade basée sur une technologie VPN (SSL ou IPSec) ;</li> <li>■ restriction des services accédés : seuls les services nécessaires aux administrateurs doivent être autorisés ;</li> <li>■ journalisation des accès sur l'ensemble de la chaîne de liaison.</li> </ul>	<b>D</b>	<b>D</b>

HEB-INF-52 Accès distant des exploitants externes	Local	National
<p>Tout accès distant d'un tiers (ex : télémaintenance) à une ressource du ministère <b>doit</b> faire l'objet des mesures de protection suivantes :</p> <ul style="list-style-type: none"> <li>■ authentification forte sur l'infrastructure dédiée aux accès distants des tiers ;</li> <li>■ restriction des services accédés : seuls les services nécessaires au tiers dans le cadre de sa mission doivent être autorisés ;</li> <li>■ restriction des possibilités de rebond depuis l'accès en télémaintenance vers le reste des systèmes d'information du ministère ;</li> <li>■ journalisation des accès sur l'ensemble de la chaîne de liaison ;</li> <li>■ intégration de clauses liées à la sécurité des systèmes d'information dans les contrats impliquant un accès par des tiers à des ressources du ministère.</li> </ul>	D	D

Le « responsable sécurité du centre serveur » devra être informé de tout manquement à ces règles.

#### 4.1.4 - Gestion de la mutualisation et de la virtualisation

Mutualiser des ressources dont les besoins de sécurité sont différents présente le risque de dégrader l'efficacité des mesures de sécurité mises en œuvre spécifiquement pour les ressources les plus sensibles ou jugées les plus dangereuses.

La possibilité de mutualiser ou non des ressources dépend donc de leurs besoins de sécurité, c'est-à-dire de la zone de sécurité à laquelle elles appartiennent.

Un équipement réseau (commutateur) peut être mutualisé entre des zones de sécurité différentes, à condition de mettre en place du cloisonnement logique (VLAN) entre chaque zone de sécurité.

Une seule exigence concerne les commutateurs.

HEB-INF-53 Mutualisation des équipements réseaux	Local	National
Un commutateur ne <b>doit</b> pas être relié à la fois au réseau interne du centre d'hébergement et à un réseau externe (Internet, connexion locale avec un tiers).	D	D

HEB-INF-54 Mutualisation des serveurs	Local	National
<p>Un serveur applicatif est un serveur qui intervient dans le fonctionnement d'une application : e.g. , serveur web, serveur d'application, serveur de base de données, serveur cartographique...</p> <p>Un serveur applicatif ne <b>doit</b> pas être mutualisé entre des zones de sécurité de natures différentes.</p> <p>La mutualisation d'un serveur web entre une zone standard et une zone sensible est donc interdite.</p>	D	D

HEB-INF-55 Mutualisation du stockage	Local	National
Les serveurs de stockage ne <b>doivent</b> pas être mutualisés sur des zones de sécurité de nature différentes, à moins qu'un cloisonnement adapté soit mis en place.	<b>D</b>	<b>D</b>

A titre d'exemple, le cloisonnement adapté peut être obtenu par la création de VLAN, la gestion « d'access list » ou un cloisonnement logique entre les volumes de stockage affectés aux différentes zones de sécurité (e.g. zoning).

## Virtualisation

HEB-INF-56 Mutualisation des hyperviseurs	Local	National
Un hyperviseur ne doit pas être mutualisé pour héberger des machines virtuelles de sécurité et des machines virtuelles applicatives. Lorsque l'hyperviseur héberge des machines virtuelles applicatives, celles-ci peuvent appartenir à des zones de sécurité différentes à condition que les fonctions de filtrage soient réalisées par un autre équipement dédié à la sécurité.	<b>D</b>	<b>D</b>

Nota :

- Une machine virtuelle de sécurité héberge des services d'infrastructure destinés à assurer la sécurité de la plate-forme : serveurs de relais, pare-feux pour assurer le cloisonnement du stockage entre VLAN,
- Une machine virtuelle applicative héberge un serveur applicatif tel que défini dans la règle **HEB-INF-45-D**.

### 4.1.5 - Sécurisation des mécanismes de commutation et de routage

HEB-INF-57 Configuration du protocole IGP de manière sécurisée	Local	National
Le protocole de routage dynamique de type IGP doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.	<b>D</b>	<b>D</b>

HEB-INF-58 Configuration du protocole EGP de manière sécurisée	Local	National
Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, cette session doit s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.	D	D

#### 4.1.6 - Sécurisation des ressources

On entend par ressource tout composant matériel, logiciel, système d'exploitation sous la responsabilité des centres d'hébergement. Les équipements de réseaux, et en particulier les routeurs, en tant que ressources, sont concernés par les exigences suivantes.

HEB-INF-59 Guides de durcissement	Local	National
Des guides de durcissement <b>devraient</b> être formalisés pour tous les systèmes d'exploitations et logiciels sous la responsabilité des centres d'hébergement (Windows, Linux, AIX...).	R	R
Les systèmes <b>devraient</b> être durcis conformément à ces guides de sécurisation.		

HEB-INF-60 Systèmes d'exploitation	Local	National
Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque.	D	D

HEB-INF-61 Modification systématique des éléments d'authentification par défaut des équipements et services	Local	National
Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.	D	D

HEB-INF-62 Gestion des correctifs de sécurité	Local	National
Un processus de gestion des correctifs de sécurité <b>doit</b> être défini pour chaque type de ressource hébergée.		
<ul style="list-style-type: none"> <li>Les systèmes d'exploitation et les applications doivent être protégés contre les vulnérabilités critiques au plus tôt après leur publication.</li> <li>Il est de la responsabilité des exploitants d'appliquer les correctifs de sécurité disponibles pour les technologies de leur périmètre.</li> <li>Une réflexion doit être menée par les exploitants et validée par les Maîtrises d'Ouvrage afin de minimiser les impacts sur la production lors du déploiement des correctifs de sécurité.</li> <li>Toute installation de correctif de sécurité doit être tracée et faire l'objet si nécessaire d'une mise à jour de la documentation existante.</li> </ul>	N/A	D

Le processus de gestion des correctifs de sécurité doit prendre en compte :

- le type de ressource (systèmes Windows, Linux, AIX, pare-feu,...) et les besoins de sécurité de la ressource ;
- l'exposition de la ressource (accessible depuis les réseaux des exploitants, du ministère, d'Internet....).

Plus la ressource est critique et exposée (e.g. besoin de disponibilité élevé, accessibilité depuis Internet) plus les correctifs de sécurité doivent être déployés rapidement.

A défaut d'une qualification/validation des correctifs de sécurité (e.g. sur une base de données, sur le noyau d'un système Linux,...), fortement préconisée, dans un environnement de qualification / pré-production, il est envisageable de déployer les correctifs de sécurité directement dans l'environnement de production sous réserve que le centre d'hébergement ait la possibilité d'effectuer un retour arrière de manière simple (e.g. bascule d'un serveur principal vers un serveur de secours).

Cette procédure doit être partagée et expliquée aux **Maîtrises d'Ouvrage**.

Le centre d'hébergement doit alerter les maîtrises d'ouvrage sur l'obsolescence des versions et les risques encourus. En particulier, si les risques le justifient, une application pourra être isolée dans une zone de sécurité dite « critique ».

## Protection contre les codes malicieux

HEB-INF-63 Protection des flux contre les codes malicieux	Local	National
Tout flux entrant sur le centre d'hébergement (provenant d'Internet, d'une connexion locale avec un tiers ou d'un réseau interne du ministère) <b>doit</b> faire l'objet d'une analyse antivirus si celui-ci est considéré comme vecteur potentiel de code malicieux.	<b>D</b>	<b>D</b>

Exemple de flux entrant à risque : flux mail ou Web contenant des pièces jointes.

Cette exigence vise à intégrer à l'architecture un mécanisme d'analyse des flux pour les flux entrants sur le centre d'hébergement permettant de détecter, bloquer et éliminer les codes malicieux (virus, chevaux de Troie, vers réseau...).

Des mécanismes de déchiffrement / chiffrement permettent d'effectuer ce type de contrôles sur les flux chiffrés.

HEB-INF-64 Protection des systèmes contre les codes malicieux	Local	National
Tout système hébergé dans le centre d'hébergement <b>doit</b> disposer d'un outil de protection contre les codes malicieux. Les outils de protection contre les codes malicieux <b>doivent</b> être mis à jour régulièrement sur l'ensemble des serveurs et disposer d'une base de signature à jour.	<b>D</b>	<b>D</b>

On entend par code malicieux : virus, cheval de Troie, vers réseau...

Les outils de protection contre les codes malicieux installés sur les serveurs, sur les postes de travail ou sur les passerelles de sécurité **doivent** provenir de trois constructeurs différents.

#### 4.1.7 - Gestion des serveurs de fichiers

Les serveurs de fichiers (autrement appelés serveurs bureautiques) sont utilisés par les utilisateurs pour stocker leurs données afin de travailler de manière collaborative. La gestion des serveurs de fichiers (mise à disposition, sauvegarde, nettoyage) doit par conséquent être réglementée afin de garantir le service mis à disposition des utilisateurs.

HEB-INF-65 Répertoires sur les serveurs	Local	National
<p>Des répertoires adéquats doivent être mis à disposition des utilisateurs sur les serveurs de fichiers afin qu'ils puissent déposer les fichiers professionnels qu'ils gèrent et échanger des informations avec d'autres agents ou services.</p> <p>Chaque utilisateur doit également disposer d'un espace individuel sur les serveurs de fichiers (par exemple pour y sauvegarder ses archives de messagerie).</p> <p>L'équipe support chargée des systèmes d'Information est responsable de la disponibilité des informations stockées sur les espaces réseau partagés qu'elle met à disposition des utilisateurs.</p>	D	D

HEB-INF-66 Sauvegarde des informations chiffrées	Local	National
<p>Lors des opérations de stockage de fichiers chiffrés sur des espaces réseau ou pour les sauvegardes et les archivages, la confidentialité des données doit être assurée par des dispositifs de robustesse équivalente à ceux qui protègent les données stockées sur les postes de travail.</p>	D	D

La solution de chiffrement est déterminée au niveau central et incluse au référentiel national. Dans la mesure du possible, cette solution doit être transparente pour l'utilisateur. En particulier, dans le cas où des données sont chiffrées sur un poste de travail, les sauvegardes de ces données sont elles aussi chiffrées ; par conséquent un administrateur réseau ne peut avoir accès à ces informations.

HEB-INF-67 Recouvrement des données chiffrées	Local	National
<p>La solution de chiffrement sur espace partagé préconisée par le niveau national définit une organisation et des droits de recouvrement propres.</p> <p>En dehors de cette solution, l'équipe chargée des Systèmes d'Information doit formaliser son niveau d'engagement vis-à-vis du recouvrement des informations chiffrées en cas de perte ou d'indisponibilité des secrets assurant le chiffrement (mots de passe, certificats, etc.).</p> <p>Elle doit ensuite mettre en place et contrôler régulièrement les procédures nécessaires au recouvrement des informations chiffrées en cohérence avec son engagement.</p>	D	D

## 4.2 - Sécurité physique

La sécurité physique vise à protéger le système d'information du ministère contre :

- **les menaces environnementales et les sinistres** : catastrophes environnementales (explosion, séisme...), sinistres (incendie, dégât des eaux, panne électrique, panne de la climatisation) ;
- **les menaces d'intrusions physiques sur les centres d'hébergement** : accès en salle d'une personne non habilitée, coupure de l'alimentation électrique, vol de disques durs contenant des informations sensibles...

Les exigences de sécurité physique doivent être appliquées non seulement aux **salles d'hébergement** dans lesquelles est stocké le matériel informatique et télécoms, mais également aux **locaux techniques** hébergeant le matériel utilisé pour alimenter/protéger le centre d'hébergement (électricité, climatisation, protection incendie...).

La mise en place des exigences de sécurité doit s'accompagner de la production par le centre d'hébergement des documents d'application associés (cf. exigence HEB-ORG-04).

### 4.2.1 - Protection contre les menaces environnementales et les sinistres

HEB-PHY-1 Recensement des menaces environnementales et traitement des risques	Local	National
Une liste des menaces environnementales liées à la localisation du centre d'hébergement <b>doit</b> être formalisée et mise à jour <i>a minima</i> tous les ans. Les risques associés à ces menaces environnementales <b>doivent</b> être traités ou acceptés par la direction de l'entité dont dépend le centre d'hébergement.	<b>R</b>	<b>D</b>

Exemples de menaces environnementales : séisme, explosion, incendie, inondation, accident aérien...

L'existence ou non de certaines menaces environnementales (SEVESO, séisme...) peut être obtenue par exemple auprès des préfectures, des DREAL (Directions régionales de l'environnement, de l'aménagement et du logement)...

HEB-PHY-2 Prévention des comportements à risques	Local	National
Des directives <b>doivent</b> être formalisées et communiquées concernant les comportements prohibés ou à risques au sein des salles informatiques.	<b>D</b>	<b>D</b>

Exemples de comportements à risque :

- manipulation de liquides (boissons, liquides inflammables, etc.) ;
- câbles électriques non rangés ;
- faux planchers et châssis des baies non reliés à la terre ;
- branchements électriques non-conformes comme l'utilisation de prises multiples sur prises multiples.

## Protection contre les incendies

Les événements suivants peuvent être à l'origine d'un incendie dans une salle d'hébergement : comportement humain (malveillant ou non), court-circuit électrique, surchauffe d'un équipement, ou feu provenant de l'extérieur de la salle (feu de poubelle, incendie sur le site).

HEB-PHY-3 Étanchéité des salles d'hébergement	Local	National
Les salles d'hébergement <b>devraient</b> être étanches vis-à-vis de l'extérieur afin d'éviter la propagation du feu.	<b>R</b>	<b>D</b>

Par exemple, les enceintes des salles d'hébergement peuvent être isolées par des murs et des portes coupe-feu.

Cette bonne pratique peut être remplacée par des mesures équivalentes, la problématique de lutte contre les incendies étant un enjeu global à traiter au niveau du bâtiment.

HEB-PHY-4 Stockage des matières inflammables	Local	National
Aucune matière inflammable ne <b>doit</b> être stockée dans les salles d'hébergement. <i>Prévoir a minima des actions périodiques de rangement afin d'évacuer les matières inflammables comme les cartons.</i>	<b>D</b>	<b>D</b>

HEB-PHY-5 Systèmes de détection incendie	Local	National
Les systèmes de détection d'incendie <b>doivent</b> couvrir toute la surface des salles d'hébergement et leurs abords.	<b>D</b>	<b>D</b>

HEB-PHY-6 Systèmes d'extinction incendie	Local	National
Des extincteurs manuels adaptés au matériel informatique et télécoms <b>doivent</b> être installés en quantité suffisante dans et aux abords des salles d'hébergement.	<b>D</b>	<b>D</b>

HEB-PHY-7 Capacité d'intervention en cas d'incendie	Local	National
Les centres d'hébergement <b>doivent</b> être en capacité d'intervenir immédiatement et à tout moment (24/7) en cas d'incendie.	<b>R</b>	<b>D</b>

Exemple de dispositif permettant de couvrir cette exigence :

- système d'extinction automatique adapté au matériel informatique et télécoms et d'une capacité suffisante, devant être supervisé et débrayable (en cas de fausse alerte). Il devrait être basé sur du gaz non toxique et non polluant type gaz inerte.

L'agent extincteur devrait être stocké hors des salles d'hébergement à protéger.

- personnel habilité à entrer en salle machine et à intervenir sur des incendies, et présent en permanence (24/7) sur le site.

HEB-PHY-8 Maintenance des dispositifs anti-incendie	Local	National
L'ensemble des dispositifs anti-incendie <b>doit</b> être maintenu opérationnel et contrôlé régulièrement.	<b>D</b>	<b>D</b>

La fréquence des contrôles doit *a minima* être conforme à la réglementation en vigueur.

HEB-PHY-9 Détection de dysfonctionnement des dispositifs anti-incendie	Local	National
Des systèmes de détection de dysfonctionnement au niveau des détecteurs incendies et des systèmes d'extinction automatique <b>doivent</b> être mis en place et supervisés.	<b>R</b>	<b>D</b>

## Protection contre le dégât des eaux

Les événements suivants peuvent provoquer un dégât des eaux dans une salle d'hébergement : intempéries, fuite des extincteurs automatiques, travaux pouvant entraîner des ruptures de canalisation, défaut du système d'évacuation des eaux, et action humaine, volontaire ou involontaire.

HEB-PHY-10 Prise en compte de la menace de dégât des eaux	Local	National
Une réflexion <b>doit</b> être menée afin de protéger le matériel informatique et télécoms contre les dégâts des eaux.	<b>D</b>	<b>D</b>

HEB-PHY-11 Bonnes pratiques liées au dégât des eaux	Local	National
<p>Les bonnes pratiques suivantes <b>devraient</b> être respectées :</p> <ul style="list-style-type: none"> <li>■ Les salles d'hébergement <b>devraient</b> être localisées dans des zones non inondables.</li> <li>■ Le matériel informatique et télécoms <b>devrait</b> être surélevé par rapport au niveau du sol.</li> <li>■ Le matériel informatique et télécoms ne <b>devrait</b> pas être positionné à proximité des installations en eau (plomberie, climatiseur, radiateur, etc.).</li> <li>■ Un dispositif de détection de dégâts des eaux <b>devrait</b> être mis en place dans les salles d'hébergement. Les alertes générées par ce dispositif <b>devraient</b> être supervisées.</li> </ul>	<b>R</b>	<b>R</b>

Exemple de zones inondables : sous-sol, terrains vulnérables à des crues...  
Le matériel peut être surélevé (e.g. installation de faux planchers).

## Continuité de l'alimentation électrique

Les événements suivants peuvent menacer la continuité de l'alimentation électrique d'une salle d'hébergement : chute de tension, coupure d'électricité, rupture d'un câble du distributeur d'électricité, rupture d'un câble électrique au sein du centre d'hébergement, orage et court-circuit électrique.

HEB-PHY-12 Identification des points individuels de défaillance électrique	Local	National
Les points individuels de défaillance (ou Single Point Of Failure – SPOF) électriques <b>doivent</b> être identifiés.		
Les risques associés à ces points individuels de défaillance électriques <b>doivent</b> être traités et/ou acceptés par la direction de l'entité.	<b>D</b>	<b>D</b>

Exemples de points individuels de défaillance : adduction électrique simple, simple raccordement du matériel informatique et télécoms ...

Les dispositifs classiques permettant de fiabiliser l'alimentation en électricité du matériel informatique et télécoms d'un centre d'hébergement sont les suivants :

- **onduleur** protégeant le matériel informatique et télécoms contre les variations de tension et les courtes coupures d'alimentation électrique. La **redondance des onduleurs** permet de se prémunir contre la panne de l'un d'entre eux.
- **doublement de l'adduction et de la pénétration électrique** consistant à mettre en place deux parcours électriques distincts entre le central du distributeur d'électricité et la salle d'hébergement.
- **double raccordement électrique du matériel informatique et télécoms** permettant de raccorder le matériel informatique et télécoms à deux sources d'alimentation électriques. Les ressources informatiques et télécoms doivent alors être équipées de deux dispositifs d'alimentation.
- **générateur électrique** produisant en tant que dispositif de secours de l'énergie électrique à partir d'un carburant stocké à distance de sécurité du centre d'hébergement.

HEB-PHY-13 Dispositifs de continuité électrique	Local	National
Les dispositifs de continuité électriques d'un centre d'hébergement <b>doivent</b> être adaptés aux besoins de disponibilité des applications hébergées.	<b>R</b>	<b>D</b>

Le tableau ci-dessous illustre **à titre d'exemple** les dispositifs de continuité électrique à mettre en place en fonction des besoins de disponibilité des applications (cf. échelle en annexe 2) :

Dispositifs de continuité électrique	Disponibilité 1	Disponibilité 2	Disponibilité 3	Disponibilité 4
Onduleur	✓	✓	✓	✓
Onduleurs redondés	-	✓	✓	✓
Doublement de l'adduction et de la pénétration électrique	-	✓	✓	✓
Générateur	-	-	✓	✓
Double raccordement électrique du matériel informatique et télécoms	-	-	-	✓

HEB-PHY-14 Supervision des alertes des onduleurs	Local	National
Des alertes <b>doivent</b> être générées en cas de coupure électrique. Ces alertes <b>doivent</b> être supervisées.	<b>R</b>	<b>D</b>

Ces alertes peuvent être générées par exemple par les onduleurs.

HEB-PHY-15 Protection contre la foudre	Local	National
Une réflexion <b>doit</b> être menée afin de protéger les ressources du centre d'hébergement contre la foudre.	<b>R</b>	<b>D</b>

Exemple d'équipement de protection : parafoudre en armoire divisionnaire.

HEB-PHY-16 Maintenance et contrôle de l'installation électrique	Local	National
Le bon fonctionnement des installations électriques <b>doit</b> être maintenu opérationnel et contrôlé régulièrement par une société spécialisée.	<b>D</b>	<b>D</b>

## Continuité de la climatisation

Les centres d'hébergement renferment un grand nombre d'équipements informatiques et télécoms qui dégagent une chaleur importante.

Les exigences exprimées dans cette sous-partie visent à réguler la température des salles d'hébergement et à prévenir ainsi les risques liés à une élévation de la température, à savoir :

- la réduction de la durée de vie des équipements informatiques et télécoms ;
- l'arrêt brutal de serveurs ;
- l'incendie au sein de la salle d'hébergement...

HEB-PHY-17 Présence d'un système de climatisation	Local	National
Un système de climatisation <b>doit</b> être mis en place dans la salle d'hébergement.	<b>D</b>	<b>D</b>

La température d'une salle d'hébergement devrait se situer entre 20° et 25°C. De plus, les conditions d'hygrométrie doivent être surveillées afin d'éviter notamment les phénomènes hydrostatiques.

Les serveurs et les baies devraient être disposés de manière à améliorer les échanges de chaleur (exemple : urbanisation de la salle en allée chaude et allée froide, câbles rangés pour faciliter la ventilation, nettoyage régulier des locaux et des équipements...).

HEB-PHY-18 Redondance du système de climatisation	Local	National
La continuité du service de refroidissement des salles d'hébergement <b>doit</b> être assurée en cas d'un incident unique (panne d'électricité, panne d'un système de climatisation) ou d'une opération de maintenance.	<b>R</b>	<b>D</b>

Recommandation : redondance des systèmes de climatisation, rattachement des systèmes de climatisation sur deux arrivées électriques indépendantes.

HEB-PHY-19 Supervision de la température des salles d'hébergement et du matériel informatique et télécoms	Local	National
La température de la salle et du matériel informatique et télécoms <b>doit</b> être supervisée et faire l'objet de différents niveaux d'alertes en fonction de seuils prédéfinis.	<b>R</b>	<b>D</b>

HEB-PHY-20 Anticipation des actions à mettre en œuvre en cas de température élevée	Local	National
Une procédure en cas de température élevée <b>doit</b> être définie.	<b>D</b>	<b>D</b>

Cette procédure peut être intégrée à une procédure d'arrêt du centre (cf. partie Continuité et secours).

HEB-PHY-21 Maintenance des systèmes de climatisation	Local	National
Les systèmes de climatisation <b>doivent</b> être maintenus opérationnels et être contrôlés régulièrement.	<b>D</b>	<b>D</b>

## Continuité des interconnexions télécoms

L'interconnexion télécoms des centres d'hébergement est primordiale car elle permet les échanges entre le centre d'hébergement et les réseaux Internet, les connexions locales avec des tiers et les réseaux internes du ministère.

HEB-PHY-22 Identification des points individuels de défaillance télécoms	Local	National
Les points individuels de défaillance (ou Single Point Of Failure – SPOF) télécoms <b>doivent</b> être identifiés. Les risques associés à ces points individuels de défaillance télécoms <b>doivent</b> être traités ou acceptés par la direction de l'entité.	<b>D</b>	<b>D</b>

Exemples de point individuel de défaillance télécoms : raccordement à un seul opérateur, raccordement à un seul central opérateur, adduction télécoms simple...

Les dispositifs classiques permettant de fiabiliser les interconnexions télécoms sont les suivants :

- double adduction et double pénétration télécoms (deux parcours distincts des arrivées télécoms entre le central de l'opérateur et la salle d'hébergement) ;
- double raccordement (rattachement sur deux centraux distincts de l'opérateur télécoms) permettant de se prémunir contre la panne d'un central ;
- stratégie « multi-opérateur » permettant de se prémunir d'un panne globale chez un opérateur télécoms.

HEB-PHY-23 Continuité de l'interconnexion télécoms	Local	National
Des garanties de temps de rétablissement (GTR) et/ou liaisons de secours adaptées aux besoins de disponibilité des applications hébergées <b>doivent</b> avoir été mises en place avec les opérateurs télécoms pour chaque interconnexion télécoms du centre d'hébergement (Internet, réseaux internes du ministère...).	<b>R</b>	<b>D</b>

Le tableau ci-dessous illustre **à titre d'exemple** les dispositifs de continuité télécoms à mettre en place en fonction des besoins de disponibilité des applications (cf. échelle en annexe 2) :

Dispositifs de continuité télécoms	Disponibilité 1	Disponibilité 2	Disponibilité 3	Disponibilité 4
Double adduction et double pénétration télécoms	-	✓	✓	✓
Double raccordement	-	-	✓	✓
Stratégie « multi-opérateur »	-	-	-	✓

## Étiquetage du matériel informatique et télécoms

L'étiquetage des équipements informatiques et des câbles permet leur identification et limite ainsi les risques d'erreur de manipulation.

HEB-PHY-24 Étiquetage	Local	National
Les câbles réseau et le matériel informatique et télécoms <b>doivent</b> être étiquetés.	<b>D</b>	<b>D</b>

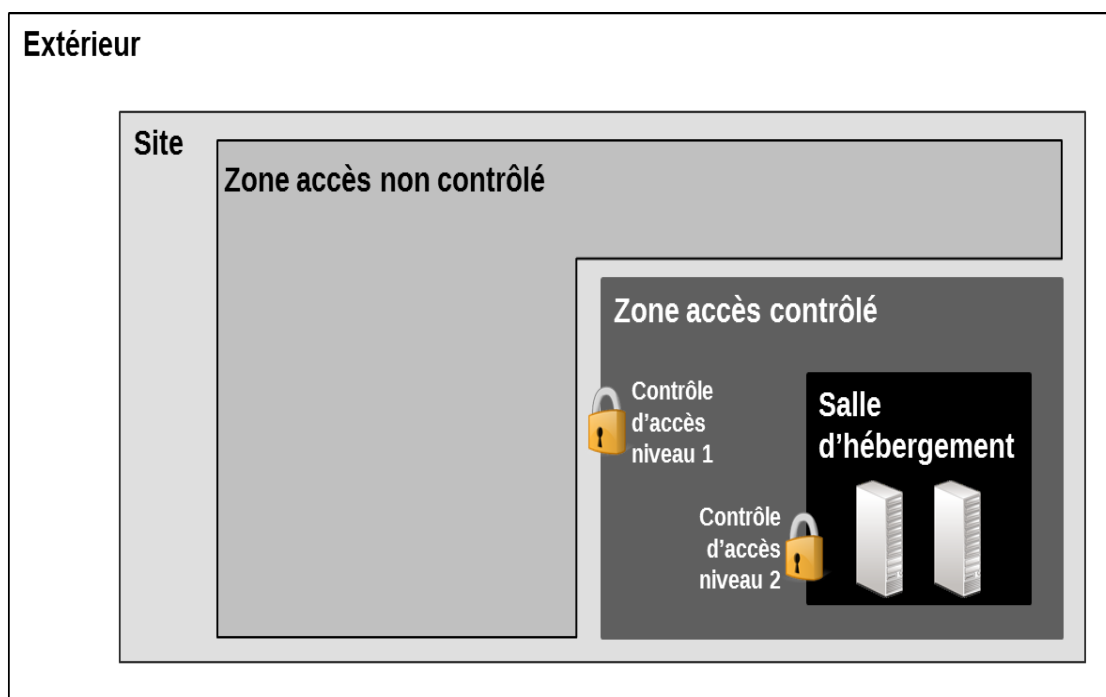
## 4.2.2 - Protection contre les intrusions physiques

Cette partie précise les dispositifs et procédures de contrôle d'accès à mettre en place afin de prévenir et de réagir à toute intrusion physique sur le centre d'hébergement.

On distingue dans ce document trois types de zones au sein des centres d'hébergement du ministère :

- les **zones « accès non contrôlé »** permettant de recevoir du public (hall, salle de réunion...) ou des zones interdites au public mais sans dispositif de contrôle suffisant ;
- les **zones « accès contrôlé »** protégées par du contrôle d'accès ;
- les **salles d'hébergement** protégées par du contrôle d'accès au sein d'une zone « accès contrôlé ». Un double niveau de contrôle d'accès est ainsi nécessaire pour accéder à la salle d'hébergement.

La mise en place d'une zone « d'accès contrôlé » est optionnelle pour les centres d'hébergement « Locaux ». Pour les centres « nationaux », cette zone permet de prévenir et de détecter en amont les intrusions sur le centre d'hébergement.



### Contrôle d'accès au sein de la zone « accès contrôlé »

HEB-PHY-25 Mise en place d'une zone « accès contrôlé » autour de la salle d'hébergement	Local	National
	R	D
Une zone « accès contrôlé » <b>doit</b> être définie autour de la salle d'hébergement.		

HEB-PHY-26 Enceintes sécurisées de la zone « accès contrôlé »	Local	National
	R	D
Les enceintes de la zone « accès contrôlé » <b>doivent</b> être sécurisées de manière à prévenir toute intrusion.		

HEB-PHY-27 Contrôle d'accès au sein de la zone « accès contrôlé »	Local	National
<p>La zone « accès contrôlé » <b>doit</b> être protégée par du contrôle d'accès.</p> <p>Les accès à la zone « accès contrôlé » <b>doivent</b> être restreints aux seules personnes habilitées.</p>	<b>R</b>	<b>D</b>

Exemple de moyens de contrôle d'accès pour la zone « accès contrôlé » : clé, badge, sas, tourniquet...

HEB-PHY-28 Accompagnement des visiteurs au sein de la zone « accès contrôlé »	Local	National
<p>Les visiteurs <b>doivent</b> être accompagnés en permanence au sein de la zone « accès contrôlé ».</p> <p>Les accès ainsi que leurs interventions doivent être tracés (par une main courante par exemple)</p>	<b>R</b>	<b>D</b>

HEB-PHY-29 Port du badge au sein de la zone « accès contrôlé »	Local	National
<p>Le port du badge apparent <b>doit</b> être obligatoire au sein de la zone « accès contrôlé ».</p>	<b>R</b>	<b>D</b>

## Contrôle d'accès au sein des salles d'hébergement

HEB-PHY-30 Contrôle d'accès au sein des salles d'hébergement	Local	National
<p>Les salles d'hébergement <b>doivent</b> être protégées par du contrôle d'accès par badge nominatif (pour les centres « Locaux », un autre moyen de contrôle d'accès peut être mis en place).</p> <p>Les accès aux salles d'hébergement <b>doivent</b> être restreints aux seules personnes habilitées.</p>	<b>D</b>	<b>D</b>

HEB-PHY-31 Accompagnement des visiteurs au sein des salles d'hébergement	Local	National
<p>Les visiteurs <b>doivent</b> être accompagnés en permanence au sein des salles d'hébergement.</p> <p>Les accès ainsi que leurs interventions doivent être tracés (par une main courante par exemple).</p>	<b>D</b>	<b>D</b>

HEB-PHY-32 Définition de profils d'accès aux salles d'hébergement	Local	National
<p>Les habilitations aux salles d'hébergement <b>doivent</b> être attribuées selon des profils d'accès prédéfinis.</p> <p>Les profils d'accès <b>doivent</b> distinguer les heures ouvrées et les heures non ouvrées.</p>	<b>R</b>	<b>D</b>

HEB-PHY-33 Habilitation des prestataires aux salles d'hébergement	Local	National
Les habilitations aux salles d'hébergement fournies aux prestataires <b>doivent</b> être valides moins d'un an. <i>Les droits d'accès du prestataire pourront être renouvelés tous les ans tant que le prestataire aura besoin de ces accès.</i>	<b>D</b>	<b>D</b>

HEB-PHY-34 Revues régulières des habilitations aux salles d'hébergement	Local	National
Les habilitations aux salles d'hébergement <b>doivent</b> être revues tous les 6 mois selon une procédure formalisée. Les habilitations non justifiées <b>doivent</b> être révoquées.	<b>D</b>	<b>D</b>

HEB-PHY-35 Conservation des traces d'accès aux salles d'hébergement	Local	National
Les traces des accès aux salles d'hébergement <b>doivent</b> être conservées pendant un an.	<b>R</b>	<b>D</b>

HEB-PHY-36 Enceintes sécurisées des salles d'hébergement	Local	National
Les enceintes des salles d'hébergement <b>doivent</b> être sécurisées de manière à prévenir toute intrusion.	<b>D</b>	<b>D</b>

Exemples pour les centres nationaux : protection des ouvrants (fenêtres, portes...), robustesse des murs...

HEB-PHY-37 Détection des intrusions	Local	National
Les salles d'hébergement <b>doivent</b> être protégées par des systèmes de détection d'intrusion.	<b>R</b>	<b>D</b>

En complément, les abords des salles d'hébergement devraient être dotés également de systèmes de détection d'intrusion afin de détecter au plus tôt les intrusions.

HEB-PHY-38 Surveillance des abords et/ou de l'intérieur des salles d'hébergement	Local	National
Les abords ou l'intérieur des salles d'hébergement <b>doivent</b> être surveillés en permanence.	<b>R</b>	<b>D</b>

Par exemple : supervision par les exploitants pendant les heures ouvrées, vidéosurveillance supervisées pendant les heures non ouvrées, système d'alarme couplé à une solution de télésurveillance pendant les heures non ouvrées (gestion des alertes par une société de gardiennage).

HEB-PHY-39 Gestion des accès ponctuels et des accès en périodes exceptionnelles	Local	National
<p>Une procédure de gestion des habilitations ponctuelles et en périodes exceptionnelles <b>doit</b> être formalisée. Elle <b>doit</b> préciser le processus de validation des accès ponctuels, et les moyens de tracer les accès et sortie des invités.</p> <p>Elle doit prendre en compte les mesures de sécurité complémentaires à mettre en place pendant les périodes exceptionnelles (travaux, déménagement, installations de matériel informatique).</p>	<b>R</b>	<b>D</b>

Les moyens à mettre en œuvre pour tracer les accès ponctuels et ceux en périodes exceptionnelles peuvent être par exemple des badges d'accès temporaires, une main courante/cahier de bord.

### Protection des postes d'exploitation du centre d'hébergement

HEB-PHY-40 Protection des postes d'exploitation du centre d'hébergement	Local	National
<p>Les postes d'exploitation du centre d'hébergement <b>doivent</b> être situés dans une zone « accès contrôlé ».</p>	<b>R</b>	<b>D</b>

## 4.3 - Continuité et secours de l'hébergement informatique

La capacité d'un centre d'hébergement à assurer la continuité et le secours des ressources dont elle a la charge repose sur :

- son **plan de continuité informatique (PCI)**, qui se focalise sur la protection et la disponibilité des données et des ressources informatiques ;
- son **plan de repli exploitant**, qui assure aux exploitants la possibilité de gérer les systèmes d'information sous leur responsabilité depuis un autre emplacement que leur lieu de travail habituel.

L'objectif de cette directive n'est pas de définir le plan de continuité informatique ou le plan de repli exploitant de chaque centre, lesquels doivent faire l'objet d'une étude au cas par cas, mais de définir les mesures organisationnelles et techniques minimales à mettre en place.

HEB-CNT-1 Formalisation d'un plan de continuité informatique	Local	National
Tout centre d'hébergement <b>doit</b> disposer d'un plan de continuité informatique (PCI) formalisé et validé par le « responsable sécurité du centre serveur ». <i>Un plan de continuité informatique peut être commun à plusieurs centres d'hébergement.</i>	<b>R</b>	<b>D</b>

Le plan de continuité informatique devrait préciser en fonction des besoins de sécurité de ses applications :

- le type de sinistre contre lequel on souhaite se protéger (sinistre local, sinistre régional...) ;
- la stratégie de secours des données (sauvegardes, restauration, synchronisation multi site) ;
- la stratégie de secours des serveurs (cluster multi site, serveurs dédiés, serveurs loués, ...).

Il devrait également intégrer un plan d'arrêt et de redémarrage du centre (équipements à arrêter ou à redémarrer en priorité) afin d'anticiper les actions à réaliser en cas de défaillance du centre d'hébergement (e.g. panne électrique, panne de climatisation...).

Deux critères essentiels sont utilisés pour l'expression des besoins de continuité et de secours :

### ■ Délai d'Interruption Maximal Admissible (DIMA)

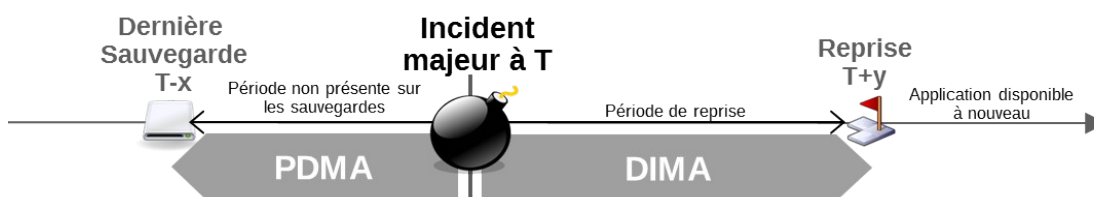
Durée maximale d'interruption d'une ressource que peuvent tolérer les Métiers utilisateurs de la ressource.

*On parle également de Recovery Time Objective (RTO)*

### ■ Perte de Données Maximale Admissible (PDMA)

Durée maximale acceptable entre la dernière sauvegarde et l'incident survenu, quantifiant ainsi les données que les Métiers tolèrent de perdre au maximum

*On parle également de Recovery Point Objective (RPO)*



HEB-CNT-2 Secours de l'infrastructure pour les applications critiques	Local	National
Les applications dont les besoins de disponibilité sont égaux à 3 ou 4 <b>doivent</b> <i>a minima</i> disposer d'une infrastructure redondée dans une salle indépendante de la salle principale.	<b>R</b>	<b>D</b>

HEB-CNT-3 Formalisation d'un plan de repli exploitant	Local	National
Tout centre d'hébergement <b>doit</b> disposer d'un plan de repli exploitant formalisé. <i>Un plan de repli exploitant peut être commun à plusieurs centres d'hébergement.</i>	<b>R</b>	<b>D</b>

Ce plan de repli exploitant peut être intégré au plan de repli utilisateur de l'entité associée au centre d'hébergement..

Le plan de repli exploitant devrait préciser en fonction des besoins de sécurité du centre :

- les locaux de repli utilisés par les exploitants (domicile des exploitants, autre site...) ;
- les outils/documentations mis à leur disposition.

HEB-CNT-4 Test du plan de continuité informatique	Local	National
Le plan de continuité informatique des centres d'hébergement <b>doit</b> être testé tous les ans. Ces tests <b>doivent</b> faire l'objet d'un compte-rendu et, si besoin, aboutir à un plan d'amélioration du plan de continuité informatique.	<b>R</b>	<b>D</b>

HEB-CNT-5 Test du plan de repli exploitant	Local	National
Le plan de repli exploitant des centres d'hébergement <b>doit</b> être testé tous les ans. Ces tests <b>doivent</b> faire l'objet d'un compte-rendu et, si besoin, aboutir à un plan d'amélioration du plan de repli exploitant.	<b>R</b>	<b>D</b>

## Exigences spécifiques concernant les sauvegardes

HEB-CNT-6 Procédures de sauvegardes et de restaurations	Local	National
Chaque ressource hébergée dans le centre d'hébergement <b>doit</b> disposer d'une procédure de sauvegarde et de restauration conforme aux besoins exprimés par les Maîtrises d'Ouvrage.	<b>R</b>	<b>D</b>

Exemple : sauvegardes des ressources applicatives, sauvegardes des éléments d'infrastructures (commutateurs, pare-feu...)

HEB-CNT-7 Réalisation de tests de restauration réguliers	Local	National
Des tests de restaurations <b>doivent</b> être effectués par échantillonnage au minimum tous les ans pour chaque type de ressource.	<b>R</b>	<b>D</b>

Exemple de type de ressource : commutateur, pare-feu, application ACAI, serveur de stockage, serveur de messagerie, serveur DNS, serveur de rebond...

HEB-CNT-8 Stockage des sauvegardes hors de la salle d'hébergement	Local	National
Les sauvegardes <b>doivent</b> être stockées de manière sécurisée hors de la salle d'hébergement.	<b>D</b>	<b>D</b>

Cela consiste à placer les sauvegardes dans un endroit sécurisé et différent de la salle où se trouvent les ressources sauvegardées.

HEB-CNT-9 Protection de la confidentialité des sauvegardes	Local	National
Les sauvegardes doivent être traitées de manière à garantir leur confidentialité.	<b>R</b>	<b>D</b>

## 4.4 - Organisation de l'exploitation

### 4.4.1 - Inventaire des ressources

La sécurité des systèmes d'information d'un centre d'hébergement repose notamment sur la connaissance et le maintien à jour de l'inventaire des ressources informatiques.

HEB-EXP-1 Inventaire des ressources	Local	National
Toutes les ressources sous la responsabilité du centre d'hébergement <b>doivent</b> être identifiées et répertoriées dans un inventaire mis à jour régulièrement. Cet inventaire <b>doit</b> préciser la propriété des ressources.	D	D

### 4.4.2 - Formation et sensibilisation des exploitants

La conduite d'actions d'administration et d'exploitation sur les systèmes d'information implique l'utilisation d'outils spécifiques et de comptes privilégiés. Les exploitants doivent être formés et sensibilisés à la sécurité afin de minimiser les risques d'erreurs lors de leurs opérations d'exploitation.

HEB-EXP-2 Formation et sensibilisation des exploitants	Local	National
Les exploitants du centre d'hébergement <b>doivent</b> être régulièrement formés et sensibilisés à la sécurité des systèmes d'information et aux droits et devoirs liés à leur fonction.	D	D

La mise en œuvre de cette exigence est sous la responsabilité du « responsable sécurité du centre d'hébergement ».

Pour rappel, la sensibilisation des exploitants passe par la connaissance et l'application de la « **Directive d'utilisation des systèmes d'information du ministère** » et du « Mémento sécurité à l'attention des administrateurs informatiques ». Ces documents encadrent notamment les modalités selon lesquelles un exploitant peut accéder à certaines données personnelles d'un agent du ministère.

Si besoin, chaque centre d'hébergement peut formaliser en complément un document plus précis afin d'explicitier les droits et les devoirs des exploitants.

### 4.4.3 - Gestion de la documentation

La formalisation de procédures d'exploitation permet de gérer de manière pérenne et sécurisée les ressources du ministère.

HEB-EXP-3 Formalisation des procédures d'exploitation	Local	National
L'exploitation des ressources <b>doit</b> être réalisée suivant des procédures formalisées intégrant les aspects sécurité. Ces procédures sont sous la responsabilité des centres d'hébergement, à l'exception de celles liées à l'exploitation des applications, lesquelles sont formalisées par les Maîtrises d'Ouvrage.	D	D

Ces exploitants/maîtrises d'ouvrage doivent gérer les versions, diffuser les documents, s'assurer que les acteurs disposent de la bonne version, rendre facilement accessible la version de référence et archiver les versions.

HEB-EXP-4 Élaboration des documents d'architecture technique et fonctionnelle	Local	National
L'architecture réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture, et des configurations, maintenus au fil des évolutions apportées au SI. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée. La cartographie réseau s'insère dans la cartographie globale des SI.	D	D

HEB-EXP-5 Protection de la documentation	Local	National
L'ensemble de la documentation sous la responsabilité du centre d'hébergement <b>doit</b> être protégée conformément à ses besoins de sécurité.	D	D

Exemple de protection : contrôle d'accès, chiffrement, sauvegarde...

HEB-EXP-6 Maintien en conditions opérationnelles de la documentation	Local	National
L'ensemble de la documentation sous la responsabilité du centre d'hébergement <b>doit</b> être gérée grâce à un outil de gestion électronique des documents afin d'assurer son maintien en conditions opérationnelles.	D	D

#### 4.4.4 - Gestion des incidents de sécurité

Les principes de gestion des incidents de sécurité sont précisés dans la directive de gestion des alertes, des incidents de sécurité et des situations d'urgence.

Pour rappel, on appelle incident de sécurité des systèmes d'information tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des systèmes d'information du ministère.

Un incident de sécurité des systèmes d'information peut être :

- d'origine accidentelle, ce qui inclut notamment les sinistres, les événements naturels, les pannes, etc. ;
- dû à une erreur ou une négligence ;
- dû à une malveillance, ce qui inclut notamment la fraude, le vol de matériel ou d'information, le sabotage, les attaques virales, etc.

HEB-EXP-7 Remontée des incidents de sécurité	Local	National
<p>Tout incident de sécurité non mineur<sup>7</sup> sur un centre d'hébergement <b>doit</b> être transmis instantanément aux acteurs en charge de la sécurité des systèmes d'information au sein du ministère (à la direction de l'entité, au bureau en charge de la sécurité des SI, de l'hébergement et des référentiels techniques et aux Maîtrises d'Ouvrage).</p> <p>Le « responsable sécurité du centre d'hébergement » <b>doit</b> prendre toutes les mesures conservatoires si l'urgence l'impose.</p> <p>Le « responsable sécurité du centre d'hébergement » <b>doit</b> recenser les incidents de sécurité survenus sur son centre d'hébergement.</p> <p>Une synthèse de ces incidents non mineurs <b>doit</b> être transmise annuellement aux acteurs en charge de la sécurité des systèmes d'information au sein du ministère (à la direction de l'entité et au bureau en charge de la sécurité des SI, de l'hébergement et des référentiels techniques ).</p>	<b>D</b>	<b>D</b>

<sup>7</sup> Incident de sécurité mineur : un incident de sécurité mineur n'a pas d'impact visible pour les utilisateurs des systèmes d'informations du ministère. Exemple d'incident mineur : panne d'un disque dur redondé, panne électrique maîtrisée grâce à un dispositif de secours...

Cependant, un incident de sécurité, en l'absence d'impact visible sur le SI, peut s'avérer être un incident de sécurité à criticité majeure (e.g exfiltration majeure).

Incident non mineur : indisponibilité d'un centre d'hébergement, le vol de matériel informatique sur un centre d'hébergement, etc...

#### 4.4.5 - Gestion du reconditionnement et de la fin de vie des ressources

Les équipements informatiques du ministère mis au rebut sont susceptibles de contenir des informations sensibles, et doivent donc faire l'objet d'un contrôle avant leur sortie du centre d'hébergement.

HEB-EXP-8 Reconditionnement	Local	National
Le reconditionnement et la réutilisation des ressources du centre d'hébergement <b>doivent</b> être effectués selon une procédure formalisée.		
Cette procédure <b>doit</b> s'assurer qu'aucune donnée confidentielle n'est présente sur les ressources reconditionnées.	D	D
Cette procédure <b>doit</b> identifier les moyens à mettre en place pour effacer/détruire les informations sensibles présentes sur les ressources reconditionnées.		

HEB-EXP-9 Mise au rebut	Local	National
La mise au rebut de ressources du centre d'hébergement, notamment celles contenant un support de stockage, <b>doit</b> être effectuée selon une procédure formalisée.		
Cette procédure <b>doit</b> s'assurer qu'aucune donnée confidentielle n'est présente sur les ressources mises au rebut.	D	D
Cette procédure <b>doit</b> identifier les moyens à mettre en place pour effacer/détruire les informations sensibles présentes sur les ressources mises au rebut.		

\*

*Exemple : destruction physique du matériel, effacement par des outils d'effacement sécurisé... pour tous types de ressources contenant un support de stockage (serveur, imprimante, routeur, commutateur...)*

## 5 - Exigences de sécurité vis-à-vis des hébergeurs externes

L'externalisation de l'hébergement informatique est une **opération complexe** qui impose la mise en place de mesures de sécurité spécifiques afin de **maintenir un niveau de sécurité qui répond aux enjeux de sécurité du ministère** (cf. première et deuxième parties de cette présente directive).

Ces mesures de sécurité s'appliquent à la fois aux prestataires et aux agents du ministère chargés de piloter la prestation d'hébergement.

### Obligation des agents du ministère dans le cadre du pilotage de prestations d'hébergement

L'externalisation de l'hébergement d'une partie des ressources du ministère doit faire l'objet de points d'attention particuliers en termes de sécurité, notamment lors de la phase projet et de la phase d'exploitation.

<b>HEB-EXT-1 Analyse des risques liés à l'externalisation de l'hébergement informatique</b>	Local	National
La Maîtrise d'Ouvrage du projet concernée <b>doit</b> analyser les risques spécifiques liés à l'externalisation de l'hébergement d'une partie de ses systèmes d'information et justifier le caractère essentiel de la prestation.	<b>D</b>	<b>D</b>

L'analyse de risques doit notamment identifier les compétences clés qui devront être maintenues en interne, et consolider les besoins de sécurité de l'ensemble des applications du ministère impactées par l'opération d'externalisation.

<b>HEB-EXT-2 Nomination d'un responsable du contrat au sein du ministère</b>	Local	National
Le contrat d'externalisation de l'hébergement <b>doit</b> être placé sous la responsabilité d'un acteur nommé et identifié, appelé dans cette directive « responsable du contrat ».	<b>D</b>	<b>D</b>

Au vu des enjeux liés à l'hébergement des ressources informatiques, les opérations d'externalisation de l'hébergement doivent être réalisées avec l'assistance du bureau en charge de la sécurité des SI, de l'hébergement et des référentiels techniques.

<b>HEB-EXT-3 Avis du bureau en charge de la sécurité des SI, de l'hébergement et des référentiels techniques lors des opérations d'externalisation de l'hébergement</b>	Local	National
<p>Les opérations d'externalisation de l'hébergement <b>doivent</b> être soumises à l'avis du bureau en charge de la sécurité des SI, de l'hébergement et des référentiels techniques</p> <ul style="list-style-type: none"> <li>■ au plus tôt avant le lancement de la consultation de l'opération d'externalisation de l'hébergement ;</li> <li>■ puis avant le choix final du prestataire.</li> </ul>	<b>D</b>	<b>D</b>

<b>HEB-EXT-4 Hébergement sur le territoire national</b>	Local	National
L'hébergement des données sensibles de l'administration sur le territoire national est obligatoire, sauf accord du HFDS et dérogation dûment motivée et précisée dans la décision d'homologation.	<b>D</b>	<b>D</b>

HEB-EXT-5 Insertion de clauses de sécurité dans le contrat d'hébergement garantissant un engagement de résultat	Local	National
<p>Des clauses de sécurité, <u>adaptées aux enjeux et aux besoins de sécurité</u> identifiés lors de l'analyse de risques, <b>doivent</b> être intégrées au contrat proposé au prestataire. Ces clauses <b>doivent</b> être validées au sens juridique par les services compétents.</p> <p>Ces clauses <b>doivent</b> aborder les aspects suivants :</p> <ul style="list-style-type: none"> <li>■ le niveau de service attendu et les niveaux de service inacceptables ;</li> <li>■ l'obligation, pour le prestataire, de faire signer à son personnel affecté sur la prestation une charte d'utilisation des systèmes d'information du ministère. Cette charte doit être préalablement validée par le ministère.</li> <li>■ le respect de la confidentialité ;</li> <li>■ la gestion des accès ;</li> <li>■ la garantie de l'intégrité et de la traçabilité ;</li> <li>■ le respect des lois et de la réglementation ;</li> <li>■ la territorialité de la prestation ;</li> <li>■ la réversibilité de la prestation ;</li> <li>■ la continuité d'activité ;</li> <li>■ la transparence du prestataire vis-à-vis du ministère, notamment lorsqu'il subit un incident de sécurité ;</li> <li>■ la mise en place d'indicateurs de sécurité ;</li> <li>■ la possibilité pour le ministère d'effectuer des audits sur le périmètre du prestataire (clause d'auditabilité) ;</li> <li>■ les pénalités en cas de non-respect des engagements.</li> </ul>	D	D

HEB-EXT-6 Exigences de sécurité minimales à intégrer au cahier des charges	Local	National
<p>Le cahier des charges <b>doit</b> imposer <i>a minima</i> l'ensemble des exigences de sécurité de la présente directive et préciser la catégorie du centre (local ou national). Ces exigences peuvent être renforcées en fonction des conclusions de l'analyse de risques.</p>	D	D

Durant toute la durée de la collaboration, le responsable du contrat doit s'assurer du respect par le tiers de ses engagements contractuels. Il effectue ce suivi notamment :

- par la mise en place et le suivi d'indicateurs de sécurité (cf. règle HEB-EXT-04) ;
- par le contrôle des bilans de conformité annuels réalisés par le centre d'hébergement externe conformément à la règle HEB-ORG-02. Ce bilan est un autocontrôle réalisé de manière déclarative par l'hébergeur externe.
- par le contrôle de la documentation de l'hébergeur (audits internes...) ;
- par l'application de l'exigence suivante :

HEB-EXT-7 Contrôle du respect des clauses de sécurité du contrat	Local	National
<p>Un audit de sécurité <b>doit</b> être effectué par le ministère un an après le début de la prestation, et doit être renouvelé en fonction des conclusions de l'audit. Cet audit permet de contrôler de manière indépendante le respect des engagements contractuels.</p> <p>Le tiers peut être exempté d'audit s'il est en capacité à fournir un rapport indépendant couvrant un périmètre similaire, e.g. certification</p>	<b>D</b>	<b>D</b>

## Annexe 1 : Glossaire

- **Besoin d'en connaître** : consiste à attribuer les habilitations logiques à chaque exploitant de manière stricte ; seuls les droits dont ils ont réellement besoins leur sont attribués.
- **Besoins de sécurité** : cf. annexe 2.
- **Centres d'hébergement** : centres qui assurent le service d'hébergement des systèmes d'informations du ministère.
- **Cloisonnement** : consiste à confiner des ressources du système d'information dans des zones de sécurité spécifiques (ou segment réseau) et à contrôler les communications entre les ressources situées sur des zones de sécurité distinctes.
- **Confidentialité** : propriété permettant de s'assurer que l'information ne soit accessible qu'aux personnes autorisées à y accéder.
- **Connexion locale à Internet** : interconnexion directe entre le centre d'hébergement et Internet, sans passer par les infrastructures nationales.
- **Connexion locale avec un tiers** : interconnexion directe (liaison louée, lien VPN...) entre le centre d'hébergement et un tiers, sans passer par les infrastructures nationales.
- **Directive de sécurité** : la PGSSI implique la définition de documents de références « permettant de faciliter ou de préciser la mise en œuvre de la PGSSI ». La présente directive est un document de référence de la PGSSI V2.
- **Disponibilité** : aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévues.
- **Entité** : définie comme suit dans l'article 2 de la PGSSI V2 :
  - le(s) Cabinet(s) ministériel(s) ;
  - les entités définies dans l'article 1 du décret n°2008-680 du 9 juillet 2008 portant organisation de l'administration centrale du ministère et décret n°2013-872 du 27/09/13 modifiant le décret n°2008-680 du 9 juillet 2008 :
    - le conseil général de l'environnement et du développement durable ;
    - le secrétariat général ;
    - le commissariat général au développement durable ;
    - les directions générales ;
    - les services techniques centraux ;
    - les services déconcentrés du ministère, les centres de formation et les écoles.
- **Incidents de sécurité des systèmes d'information** : tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des systèmes d'information du ministère.
- **Intégrité** : propriété permettant de garantir l'exactitude, la fiabilité et l'exhaustivité des informations et des méthodes de traitement.
- **Maîtrise d'Ouvrage (MOA)** : le maître d'ouvrage d'un système d'information est l'autorité administrative définissant les caractéristiques fonctionnelles de son système d'information.
- **PGSSI** : Politique Générale de Sécurité des Systèmes d'Information du ministère.
- **Ressources** : ensemble des équipements techniques et logiciels sous la responsabilité du centre d'hébergement (équipement physique/hardware, systèmes d'exploitation, applications...).
- **Système d'information** : ensemble organisé de ressources (données, procédures, matériel, logiciel, personnel, etc.) permettant d'acquérir, traiter, stocker, diffuser ou détruire les informations utilisées par les entités dans leurs métiers, et ceci quel que soit le support des informations (numérique, papier, oral, etc.).
- **Traçabilité** : propriété permettant de fournir les moyens de preuve et de contrôle sur les informations et les méthodes de traitement.
- **Zone de sécurité** : définie par un segment réseau pour lequel il n'y a pas de filtrage entre les ressources localisées sur la zone. Chaque ressource de la zone peut communiquer sans restriction avec les autres ressources au sein de la zone

## Annexe 2 : Catégories de centres d'hébergement

Le « responsable sécurité du centre d'hébergement » doit régulièrement évaluer la sensibilité de son centre.

Cette sensibilité est déterminée en fonction des besoins de sécurité des applications (cf. annexe 3) hébergées et de l'exposition du centre à Internet.

L'échelle utilisée pour évaluer la sensibilité est composée de deux niveaux :

- **Local** correspondant aux centres qui n'ont pas de connexion locale à Internet<sup>8</sup> et qui hébergent exclusivement des applications dont les besoins de sécurité sont de niveau inférieur ou égal à : 3 sur le critère Disponibilité, 2 sur le critère Intégrité, 2 sur le critère Confidentialité et 2 sur le critère Traçabilité.
- **National** correspondant aux centres qui ont une connexion locale à Internet ou qui hébergent au moins une application dont les besoins de sécurité sont de niveau supérieur ou égal à 4 sur le critère Disponibilité, 3 sur le critère Intégrité, 3 sur le critère Confidentialité ou 3 sur le critère Traçabilité.

Ainsi, un centre disposant d'une connexion locale à Internet est nécessairement « national ».  
Si un centre ne possède pas de connexion locale à Internet, il est « national » si et seulement si au moins une de ses applications a des besoins de sécurité de niveau supérieur ou égal à DICT= 4333.  
Dans tous les autres cas, le centre est considéré comme local.

	Disponibilité	Intégrité	Confidentialité	Traçabilité
1	Local			
2				
3	National			
4				

<sup>8</sup>

Connexion locale à Internet : cf. glossaire

## Annexe 3 : Critères de sécurité - Échelle d'évaluation des besoins de sécurité des applications

## Critères et évaluation des besoins de sécurité

Les besoins de sécurité des applications sont appréciées selon les critères suivants, dits critères DICT (Disponibilité, Intégrité, Confidentialité, Traçabilité).

Disponibilité	La disponibilité est l'aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévues
Intégrité	L'intégrité est la propriété permettant de garantir l'exactitude, la fiabilité et l'exhaustivité des informations et des méthodes de traitement ainsi que de s'assurer que seuls les collaborateurs habilités interviennent dans la réalisation d'une fonction ou que les fonctions sont réalisées dans les conditions initialement prévues.
Confidentialité	La confidentialité est la propriété permettant de s'assurer que seuls les utilisateurs ayant à en connaître et habilités dans les conditions normales prévues ont accès aux informations.
Traçabilité (parfois appelé <i>Preuve</i> )	La traçabilité est la propriété permettant de fournir les moyens de preuve et de contrôle sur les informations et les méthodes de traitement.

## Échelle d'évaluation des besoins de sécurité

Chaque critère DICT est évalué en fonction de l'échelle ci-dessous :

	Disponibilité	Intégrité	Confidentialité	Traçabilité
1	Supérieur à 2 jours d'interruption tolérable	Besoin d'intégrité faible	Diffusion d'informations publiques	Absence de trace acceptable
2	De 4h à 2 jours d'interruption tolérable	Besoin d'intégrité moyenne Une perte temporaire d'intégrité est acceptée mais la détection et la reconstruction sont obligatoires	Diffusion d'informations internes au personnel du ministère	Besoin d'identification des acteurs des actions
3	De 2h à 4h d'interruption tolérable	Besoin d'intégrité renforcée Une perte temporaire d'intégrité est acceptée mais la détection et la reconstruction sont obligatoires	Diffusion d'informations à un personnel ciblé et authentifié	Besoin d'imputabilité des actions
4	Moins de 2h d'interruption tolérable - besoin immédiat	Aucune altération Aucune perte d'intégrité n'est acceptée	Diffusion d'informations à un personnel ciblé, limité et authentifié	Besoin d'opposabilité légale des actions

**On dit qu'une application est de niveau DICT = 3212 quand ses besoins de sécurité valent 3 pour la disponibilité, 3 pour l'intégrité, 1 pour la confidentialité et 2 pour la traçabilité.**

## Échelle de gravité des impacts

	Politique et image de marque	Désorganisation interne ou externe	Légal et réglementaire	Financier et économique	Atteinte à la vie des personnes
1	Plaintes ou doléances limitées d'utilisateurs ou partenaires	Nécessité d'adaptation limitée du mode de fonctionnement habituel	Sanction interne au ministère	Impact budgétaire limité pour le ministère	Inconfort ou stress élevé des personnes
2	Plaintes ou doléances importantes d'utilisateurs ou partenaires Mentions limitées dans la presse	Augmentation de la charge de travail Doléances ou plaintes des équipes Stress élevé des équipes	Condamnation civile d'un agent du ministère Mention du ministère dans une affaire civile ou pénale	Pertes supérieures à 10 millions d'euros pour le ministère Impact économique ou financier limité pour un partenaire du ministère	Blessure légère d'agents ou de personnes extérieures au ministère
3	Campagnes dans des médias locaux ou campagnes limitées dans des médias nationaux Mouvements de protestations locaux ou limités Perte limitée de pouvoir de négociation	Bouleversements importants de la vie des personnes Mobilisation limitée de moyens ou ressources supplémentaires Perte limitée de productivité Mouvements de protestation limités	Enquête administrative Condamnation ou amende prononcée à l'encontre du ministère	Pertes supérieures à 50 millions d'euros pour le ministère Impact économique ou financier important pour un partenaire du ministère	Blessure lourde d'agents ou de personnes extérieures au ministère
4	Campagnes dans des médias nationaux ou internationaux Mouvements de protestation importants Perte importante de pouvoir de négociation	Mobilisation importante de moyens ou ressources supplémentaires Perte importante de productivité Mouvements de protestation importants	Condamnation pénale d'un agent du ministère ou du ministère	Pertes supérieures à 200 millions d'euros pour le ministère Impact économique ou financier critique pour un partenaire du ministère	Accident grave impliquant un nombre important de personnes Décès de personnes

