



Page 1 of 53	Afpa – CCTG-SSI	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

CCTG SSI

Cahier des Clauses Techniques Générales pour la Sécurité des Systèmes d'Information

Mai 2023

Page 2 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

Suivi des versions


Rédacteur / Vérificateur	Date	Version	Statut (Travail / pour validation / applicable)	Objet
Mourad ZIRARI Florence PATENNE	10/01/2022	1.0	Applicable	
Florence PATENNE	10/07/2023	2.0	Applicable	

Suivi des modifications

Version	Date	Objet de l'évolution	Rédacteur	Fonction
1.0	10/01/2022	Création du document	Florence PATENNE Mourad ZIRARI	RSSI DSI/DOP
2.0	11/05/2023	Changements majeurs	Florence PATENNE	RSSI


Vérification / Approbation

	Nom	Fonction	Date
Vérification	Mourad ZIRARI	Responsable DSI/DOP	10/07/2023
	Olivier LHERPINIERE	Responsable DSI/DET	10/07/2023
	Florence PATENNE	RSSI	10/07/2023
Approbation	Mourad ZIRARI	Responsable DSI/DOP	10/07/2023
	Olivier LHERPINIERE	Responsable DSI/DET	10/07/2023
	Florence PATENNE	RSSI	10/07/2023


Page 3 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

Sommaire

Suivi des versions	2
Suivi des modifications.....	2
Vérification / Approbation	2
1. <i>Présentation du document</i>	5
1.1 <i>Objet</i>	5
1.2 Structure du document	6
1.3 Evolution et modification du CCTG-SSI	7
1.4 Discussions, amendements et accords.....	7
1.5 Documents de référence et associés.....	7
1.6 Termes et définitions	8
2. <i>Préambule</i>	10
2.1 Prérequis vis-à-vis de la Maîtrise d'Ouvrage.....	10
2.2 Actions avant la mise en service du système.....	10
2.3 Gestion de la documentation	11
3. <i>Politique de sécurité du système d'informations</i>	12
3.1 Homologation des SI	12
4. Organisation de la sécurité et gouvernance	13
4.1 Appareils mobiles et télétravail	13
5. Gestion des actifs	17
5.1 Protection des informations	17
6. Contrôle d'accès	20
6.1 Gestion des accès logiques via l'authentification	20
7. Chiffrement	24
7.1 Fonctions cryptographiques et chiffrement	24
8. Sécurité physique et environnementale.....	26
8.1 Gestion des accès physiques et matériels de sécurité.....	26
9. Sécurité liée à l'exploitation.....	28
9.1 Protection contre les logiciels malveillants	28
9.2 Sauvegardes	29

Page 4 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

9.3 Journalisation et surveillance	30
9.4 Maitrise des logiciels en exploitation & protection des systèmes	32
9.5 Gestion des vulnérabilités techniques.....	37
9.6 Hébergement de SI à l'extérieur de l'AFPA.....	38
10. Sécurité des communications.....	40
10.1 Management de la sécurité des réseaux	40
10.2 Liaison de télé-opération	43
11. Acquisition, développement et maintenance des systèmes d'information.....	48
11.1 Sécurité des processus de développement, d'assistance technique et traitement des données de tests	48
12. Continuité et reprise d'activité	50
12.1 Plan de secours.....	50
11.2 Architecture, disponibilité et mécanismes de redondance.....	52

Page 5 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

1. Présentation du document

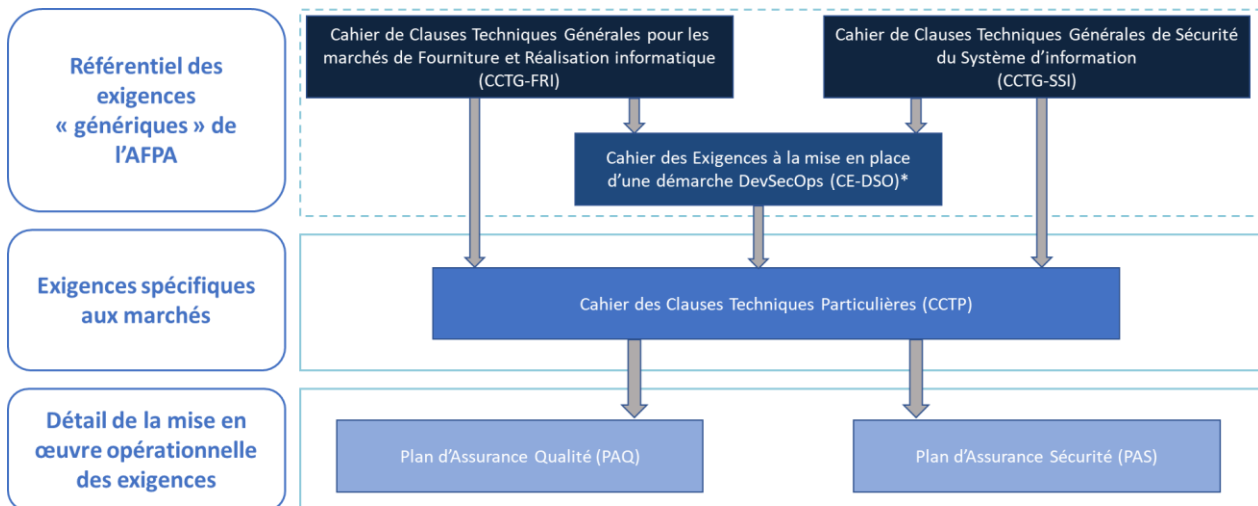
1.1 Objet

Ce document constitue le cahier des clauses techniques générales de sécurité des systèmes d'information utilisables pour l'ensemble des prestations liées aux systèmes d'information de l'Afpa. Il spécifie l'ensemble des règles qui permettent une couverture acceptable des risques auxquels les systèmes conçus sont exposés.

Le présent document est organisé selon la norme ISO/CEI 27002 : 2022, avec un ensemble de dix périmètres couverts, qui sont les suivants :

- Politique de sécurité du système d'information,
- Organisation de la sécurité et gouvernance,
- Gestion des actifs,
- Contrôle d'accès,
- Chiffrement,
- Sécurité physique et environnementale,
- Sécurité liée à l'exploitation,
- Sécurité des communications,
- Acquisition, développement et maintenance des systèmes d'informations,
- Continuité et reprise d'activité.

Le CCTG-SSI est un document contractuel. Il est annexé au marché de réalisation et s'articule avec les autres documents du marché de la manière suivante :



* Uniquement si la démarche DevSecOps est applicable

1.2 Structure du document

Ce document est organisé selon la norme ISO/CEI 27002 : 2022. Chaque périmètre décrit dans le présent document sera présenté selon la structure suivante :

Objectif
Description de l'objectif du périmètre

Risques
Les risques que présente le périmètre

Exigence	Titre	Description	Application
Identifiant de l'exigence (EX-XXX)	Titre de l'exigence	Description de l'exigence	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

1.3 Evolution et modification du CCTG-SSI

Un historique des modifications est disponible au début de ce document et doit être mis à jour à chaque validation d'un changement du CCTG-SSI. Chaque changement du présent document doit être revu et approuvé suivant le RACI ci-dessous.

- R : Responsable. C'est la ressource qui est garante de l'activité.
- A : Acteur. C'est la ressource qui réalise l'activité. Il peut y avoir plusieurs A.
- C : Consulté. Ressource consultée (par R) pour obtenir des informations nécessaires à la réalisation de la tâche. La communication est aussi bidirectionnelle.
- I : Informé. Ressource uniquement informée des travaux sur la tâche.

Action	RSSI	DOP	DET	Prestataire
Ajout d'un élément au CCTG-SSI	R, A	A, C, I	A, C, I	I
Modification d'un élément du CCTG-SSI	R, A	A, C, I	A, C, I	I
Suppression d'un élément du CCTG-SSI	R, A	A, C, I	A, C, I	I

1.4 Discussions, amendements et accords


Les discussions, amendements et accords se font :

- Sous forme de questions-réponses dans le cas d'un appel d'offres,
- Lors d'un comité ad-hoc organisé avec le prestataire titulaire.

NB: Lors d'une réponse à un appel d'Offres, lorsque le prestataire marque qu'il est « conforme », cette conformité devra être respectée au cours du contrat

1.5 Documents de référence et associés


Document	Description
PSSI-E	La Politique de Sécurité des Systèmes d'Information de l'Etat.
PSSI AFPA	La Politique de Sécurité des Systèmes d'Information de l'AFPA, qui est une déclinaison de la PSSI-E.
ISO27001:2022	Une norme internationale de sécurité des systèmes d'information de l'ISO et de la CEI.

Page 8 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information


ISO27002:2022	Une norme internationale de sécurité des systèmes d'information de l'ISO et de la CEI.
Politique de gestion des mots de passe	La politique de gestion des mots de passe de l'AFPA.
PAS AFPA	Plan d'assurance sécurité de l'AFPA
CCTG-FRI V1.1	Le cahier des clauses techniques générales de l'AFPA pour les Fournisseurs de Ressources informatiques
CE-DSO	Le cahier des exigences de mise en œuvre d'une démarche DevSecOps.
Processus de mise en œuvre d'une opération de patching de sécurité	Le processus à suivre lors de la demande, la validation, puis l'application d'une opération de patching.
Procédures de gestion des comptes	Les procédures de création, modification, désactivation et suppression des comptes de l'AFPA (compte utilisateur, compte prestataire, compte administrateur etc.)
Processus d'alerte en cas de crise	Le processus interne AFPA à suivre afin d'activer les cellules de crise.

1.6 Termes et définitions

Terme	Définition
Actif ou bien	Élément ayant de la valeur pour l'AFPA
ARP	Address Resolution Protocol (protocole de résolution d'adresse)
Chiffrement	Le chiffrement désigne la conversion de texte brut lisible par les hommes en texte incompréhensible, appelé texte chiffré. Les données chiffrées ne peuvent être lues ou traitées qu'après leur déchiffrement.
CMDB	Configuration Management Database
CVE	Common Vulnerabilities and Exposures ou CVE est un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité.
DAT	Dossier d'Architecture Technique
DHCP	Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes)
DHCP Snooping	DHCP Snooping est une technologie de sécurité qui empêche les serveurs DHCP non autorisés de distribuer des adresses IP aux clients
DOP	Direction des Opérations
DMZ	Une zone démilitarisée, ou DMZ est un sous-réseau séparé du réseau local et isolé de celui-ci par un pare-feu
DPO	Délégué à la Protection des Données
FTP	File Transfer Protocol (protocole de transfert de fichier)
IaaS	Infrastructure as a service

Page 9 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

IPSEC	Ensemble de protocoles permettant d'assurer une communication sécurisée et privée
Load balancing	Le load balancing (en français : répartition de charge) désigne le processus de répartition d'un ensemble de tâches sur un ensemble de ressources, dans le but d'en rendre le traitement global plus efficace.
MPLS	Multiprotocol Label Switching, transport de données basé sur la commutation de label
PaaS	Plateforme as a service
PAS	Plan d'Assurance Sécurité
Patch	Correctif de sécurité
PCA	Plan de continuité d'activité
PRA	Plan de reprise d'activité
PSSI	Politique de Sécurité des Systèmes d'Information
RPO	Recovery Point Objective, le temps maximal admissible d'interruption de l'enregistrement des données
RSSI	Responsable Sécurité du Système d'Information
RTO	Recovery Time Objective, le temps maximal théorique admissible d'interruption de service
SaaS	Software as a service
SI	Système d'Information
Threat Intelligence	La Threat Intelligence est une discipline basée sur des techniques du renseignement, qui a pour but la collecte et l'organisation de toutes les informations liées aux menaces du cyberspace, afin de dresser un portrait des attaquants et des tendances.
VLAN	Réseau local virtuel
VPN	Virtuel Private Network
802.1X	802.1X est un standard lié à la sécurité des réseaux informatiques, mis au point en 2001 par l'IEEE

Page 10 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

2. Préambule

2.1 Prérequis vis-à-vis de la Maîtrise d’Ouvrage

Conformément à la classification des systèmes d'information, l'application des exigences de sécurité formulées dans le présent document doit être modulée en fonction des éléments suivants relatifs au projet et validés par l’Afpa :

- Le contexte du système :
 - L'inventaire des informations et fonctions composant le système ;
 - La classification de l'ensemble des informations, fonctions, sous-fonctions du système.
- L'aspect réglementaire et législatif permettant l'identification de l'ensemble des législations et réglementations applicables aux informations et/ou au SI (RGPD, propriété intellectuelle, PCI-DSS, SecNumCloud, ...) ;
- La spécification des exigences fonctionnelles de sécurité.

2.2 Actions avant la mise en service du système

En informatique, comme dans les autres domaines, le risque zéro n'existe pas.


Conformément à la PSSI-E, tout système d'information doit faire l'objet d'une décision d'homologation avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité d'emploi atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés.

Un audit de sécurité doit être effectué avant la mise en service d'un nouveau système afin de garantir son adéquation avec les exigences SSI issus du présent document et les « bonnes pratiques » appliquées par la DSI de l’Afpa.

La décision d'homologation s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi du système d'information.

Cet audit a pour but de vérifier les principaux points énoncés dans ce document, dont notamment :

- La résilience et la performance,
- La disponibilité, l'intégrité et la confidentialité des données,
- La sécurité physique,
- Les moyens d'authentification,

Page 11 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

- Le respect des principes de sécurité concernant les installations et les configurations des systèmes,
- Le respect des principes de traçabilité,
- La sécurité d'accès aux équipements (physique, logique, etc.),
- Les conditions de cloisonnement du système cible.

2.3 Gestion de la documentation

L'ensemble des acteurs du projet doit veiller à la réalisation des actions suivantes :

- La traçabilité et la justification des solutions envisagées et retenues,
- L'intégration de la sécurité à l'ensemble de la documentation,
- Dossier de conception générale et détaillée,
- Dossier d'installation et de configuration,
- Dossier d'exploitation et de maintenance,
- Manuel d'utilisation et d'administration.

L'ensemble de ces documents doit être mis à jour durant tout le cycle de vie du système, et vérifié périodiquement au minimum une fois par an.

La formalisation de cette exigence devra figurer dans le PAS du SI concerné à l'initialisation d'un nouveau projet.


3. Politique de sécurité du système d'informations

3.1 Homologation des SI

Objectif :
<p>La spécification d'exigences de sécurité de l'Afpa et la mise en place de mesures techniques/organisationnelles pour satisfaire ces exigences, la bonne adéquation des solutions techniques des prestataires avec le besoin nécessitent avant toute mise en service d'un système d'information la réalisation d'un audit, appelé homologation de sécurité, qui garantit que les objectifs de sécurité sont atteints.</p> <p>Il s'agit, lors de cet audit, de vérifier la bonne prise en compte de la sécurité dans la solution mise en œuvre, avant sa mise en production. Elle doit notamment permettre de déterminer les risques liés aux vulnérabilités résiduelles et de proposer un plan d'actions permettant de les corriger et de statuer sur les risques résiduels.</p>

Risques :
<p>Les principaux risques lors de l'absence d'audit de sécurité :</p> <ul style="list-style-type: none"> • Non-connaissance du niveau de sécurité réel du système ; • Possibilité de non-respect des spécifications du client.

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-001	Homologation d'un SI	<p>Tout SI, qu'il soit vital, sensible, nominatif, doit faire l'objet d'un audit de sécurité avant sa mise en service.</p> <p>Sont également intégrés dans ce périmètre :</p> <ul style="list-style-type: none"> • Les systèmes hébergés ; • Les postes de télé-opérations tels que décrits au chapitre 10 et de façon générale les éléments de la chaîne de communication entre le prestataire externe et le système maintenu et sous responsabilité de l'Afpa ; • Les systèmes nomades. 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 13 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information


4. Organisation de la sécurité et gouvernance

4.1 Appareils mobiles et télétravail


Objectif :
<p>Les salariés de l'Afpa, les prestataires, les stagiaires utilisent dans le cadre de leurs activités des postes informatiques nomades et des supports de grande capacité amovibles (clés USB, disques durs, etc.). On distingue les postes bureautiques du « domaine Gestion » dédiés aux personnels internes, des postes bureautiques du « domaine Pédago » dédiés aux stagiaires.</p> <p>Ces systèmes nomades peuvent héberger des données techniques, des schémas, des identifiants, des mots de passe, des dossiers d'appel d'offres, des réponses à ces appels d'offres, des dossiers RH, etc. ... Il s'agit de définir des exigences concernant le nomadisme et la protection des données hébergées sur ces systèmes, notamment dans le cadre de la prévention du vol ou de la perte du matériel.</p>

Risques :
<p>Les principaux risques associés à la non-protection des données hébergées sur des systèmes nomades sont liés à la confidentialité avec des impacts potentiellement forts en terme :</p> <ul style="list-style-type: none"> • D'atteinte à l'image de marque ; • De perte d'avantage concurrentiel ; • De perte de données critiques relevant du secret industriel ; • De perte de données décrivant des systèmes ou des techniques d'accès à ces systèmes ; • ...


Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-002	Protection physique contre le vol	<p>Les systèmes nomades (poste informatique) doivent être protégés du vol simple et être attachés à un point fixe via un câble d'acier.</p> <p>Concernant les médias amovibles, la protection physique s'appuie sur la protection des données liées au respect de l'exigence EX-004.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 14 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

EX-003	Classification des données stockées	<p>Les données hébergées sur le système nomade (poste informatique, clé USB, etc.) doivent être clairement identifiées et classées au travers d'une analyse de risques.</p> <p>En fonction de la criticité, un processus de protection par chiffrement des données doit être utilisé. Ce processus de protection s'appuie sur un outil logiciel qualifié par l'entreprise. L'utilisateur peut s'appuyer sur les équipes de support informatique pour enregistrer toutes les données critiques dans un catalogue protégé par chiffrement.</p> <p>Cette exigence s'applique notamment :</p> <ul style="list-style-type: none"> • Aux chefs de projets ; • au responsable achat ; • au responsable RH ; • aux directeurs d'entité ; • et à toute personne détenant des informations confidentielles sur des systèmes nomades ; • Tout logiciel non nécessaire à la fonction du poste nomade est interdit. <p>L'Afpa se réserve le droit de pouvoir auditer le système nomade (poste).</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-004	Sauvegarde des données nomades	<p>Conformément à la charte informatique, l'utilisateur doit veiller à effectuer des sauvegardes régulières de données afin d'assurer une perte minimale en cas de vol, de destruction, ou d'immobilisation (via un ransomware par exemple) du système nomade. Pour ce faire, l'utilisateur s'appuiera sur l'offre de sauvegarde proposée par la DSI.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-005	Niveau de sécurité	<p>La connexion d'un poste nomade non matricé sur les réseaux informatiques de l'Afpa (hors Wi-Fi externe tel que Invité, village, etc...) n'est pas autorisée. L'obtention d'une dérogation est possible auprès du RSSI si le niveau de sécurité du poste est au moins équivalent au niveau de sécurité d'un poste matricé Afpa.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 15 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

EX-006	MCS	Les postes nomades doivent être maintenus à jour en termes de sécurité (patches de sécurité, anti-virus). Les données qu'ils contiennent doivent être protégées (chiffrement de disques durs, etc.). Il n'est pas autorisé l'activation des connexions réseaux simultanées (Wi-Fi, 4G/5G).	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-007	Protection des données nomades	L'utilisation des médias de stockage nomades (clé USB, disque externe, carte SD, etc.) est strictement interdite au sein de l'Afpa, ainsi il est obligatoire de désactiver les pilotes de masse pour les différents ports (port USB, type C, lecteur de carte SD, etc.) afin de bloquer tout transfert de données entre les machines et les médias amovibles. Dans le cas d'une nécessité d'utiliser ce type de support, une demande justifiée devra être adressée à la RSSI de l'Afpa, afin de décider d'accorder ou non une dérogation exceptionnelle et temporaire.	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-008	Connexion d'équipements nomades non identifiés	La connexion d'équipements nomades non identifiés (PC portable personnel, smartphone, etc.) ou non référencés susceptibles d'être porteurs de virus, est interdite sur le réseau de l'entreprise.	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-009	Connexion d'équipements nomades identifiés	<p>La connexion d'équipements nomades (PC portable professionnel, smartphone, clé USB, disque dur, etc.) clairement identifiés et référencés dans les équipements du système d'information est autorisée sous les conditions suivantes :</p> <ul style="list-style-type: none"> • La politique anti-virale doit être appliquée et suivie ; • L'ensemble du poste doit être scanné par un anti-virus avant la connexion au réseau privé ; • Seule l'interface de connexion vers le réseau privé doit être active. Tout autre moyen de liaison vers d'autres médias 	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 16 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		<p>de transmission (Bluetooth, WIFI, etc.) doit être désactivé.</p> <p>Dans le cas de médias de stockage (clé USB, disque externe, etc.), l'ensemble du média doit être scanné par un anti-virus avant la connexion sur un équipement connecté au réseau privé.</p>	
--	--	---	--


5. Gestion des actifs

5.1 Protection des informations


Objectif :
Afin d'assurer la confidentialité, l'intégrité d'une donnée à caractère personnel ou confidentiel, il est important de s'assurer de l'adéquation des risques aux mécanismes de protections mis en œuvre.

Risques :
Les risques qui portent sur les données sont des risques qui menacent la confidentialité, l'intégrité et la disponibilité des données.
- Confidentialité : Les données confidentielles peuvent être compromises par des attaquants qui exploitent d'éventuelles faiblesses du système (vulnérabilités, la non-utilisation du chiffrement, etc.)
- Intégrité : Les données peuvent être modifiées ou corrompues par des utilisateurs malveillants ou par des erreurs humaines. Par exemple, en modifiant les informations répertoriées dans une base de données.
- Disponibilité : Les données peuvent être rendues indisponibles par des attaques informatiques ou par des défaillances système. Par exemple, en utilisant une attaque DDOS.


Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-010	Confidentialité des données	<p>Toute donnée classée confidentielle et transmise dans le cadre d'un projet par l'entreprise doit faire l'objet d'un engagement de confidentialité du titulaire.</p> <p>Le titulaire doit :</p> <ul style="list-style-type: none"> Faire respecter cet engagement par son personnel ; Veiller à ne pas divulguer les informations ; <p>Restituer les données à la fin du projet et les détruire de tout support ayant pu les contenir</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 18 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

EX-011	Chiffrement des données	<p>Lorsqu'il est nécessaire de protéger la confidentialité des données hébergées sur le SI, des techniques de chiffrement des données peuvent être utilisées.</p> <p>Les données suivantes doivent obligatoirement être chiffrées :</p> <ul style="list-style-type: none"> • Les flux d'authentification et d'administration ; • Le stockage des authentifiants utilisés, sous forme de hash avec Salt (chiffrement irréversible) <p>La mise en place d'un système de chiffrement de données impose la rédaction d'une politique ou de procédures précises qui garantissent la protection des clés et le recouvrement.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-012	Cas de données nominatives	<p>Les données informatiques classées « confidentielles » ou « personnelles » doivent répondre aux exigences suivantes :</p> <ul style="list-style-type: none"> • Disposer d'une liste d'accès ou de diffusion précisant le nom, la fonction et l'organisation de chaque destinataire. Ces listes sont elles aussi classées « confidentielles » ou « personnelles » et doivent disposer des mêmes mécanismes de protection ; • N'être accessibles qu'à des tiers ayant signés un engagement de confidentialité et ayant le « besoin d'en connaître » ; • Être transportées ou stockées sur un support chiffré, notamment lors des sorties en dehors du périmètre de l'entreprise ; • Disposer de mécanismes techniques ou organisationnels (ex : double vérification) permettant de valider qu'elles n'ont pas été modifiées après toute action sur ces dernières. 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 19 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

EX-013	Intégrité des données	<p>Lorsque l'intégrité des données hébergées sur le SI est nécessaire, des techniques de contrôle doivent être mises en œuvre.</p> <ul style="list-style-type: none"> • Au niveau du réseau, via une authentification des émetteurs et un contrôle des paquets échangés ; • Au niveau du système, via des applications en charge de surveiller la non-altération des paquets. <p>De plus des techniques de chiffrement doivent garantir l'intégrité des informations transmises, y compris l'authentification mutuelle des deux entités.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-014	Mise au rebut	<p>Il convient de garantir :</p> <ul style="list-style-type: none"> • L'absence de données classifiées internes / confidentielles ou secrètes sur l'ensemble des matériels ou supports mis au rebut ; • L'absence de logiciel sous licence sur l'ensemble des matériels ou supports mis au rebut. <p>L'emploi d'outils appropriés de suppression sécurisée est nécessaire.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 20 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information


6. Contrôle d'accès

6.1 Gestion des accès logiques via l'authentification


Objectif :
<p>L'authentification sur un SI couvre 2 objectifs :</p> <ul style="list-style-type: none"> • Être la première protection du SI ; • D'engager ou de dégager la responsabilité de l'utilisateur, via des authentifiants personnels. <p>Les présentes règles ne sont pas exclusives d'autres modes d'authentification utilisés dans de futurs contrôles d'accès aux systèmes d'information.</p>

Risques :
<p>Les risques découlant d'une authentification et traçabilité insuffisantes sont :</p> <ul style="list-style-type: none"> • Intrusion dans un système par une personne non habilitée ; • Impossibilité d'identifier la source à l'origine d'un incident ou d'une fraude sur les équipements. <p>Les impacts d'intrusions sur des systèmes peuvent être :</p> <ul style="list-style-type: none"> • Atteinte à la confidentialité ou à l'intégrité de certaines ressources ; • Atteinte à la disponibilité d'équipements.


Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-015	Règles minimales	<p>Tout SI (système d'exploitation, application, etc.) doit respecter les points suivants :</p> <ul style="list-style-type: none"> • Authentifier, avant tout autre action sur le système, l'utilisateur ou processus ou matériels ; • Stocker les informations d'authentification de façon qu'elles soient seulement accessibles pour consultation ou modification par des 	<p>☒ On-Prem</p> <p>☒ SaaS</p> <p>☒ IaaS/PaaS</p>

Page 21 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		<p>utilisateurs autorisés et protégées de tout intrus ;</p> <ul style="list-style-type: none"> • Traiter l'authentification au travers d'un chemin de confiance entre l'utilisateur et le système (exemple : chiffrement du couple login / mot de passe transitant au travers du réseau). <p>D'un point de vue technique, le système d'authentification doit au minimum disposer d'un élément de preuve (ou facteur d'authentification) pour authentifier l'entité demandant un accès. Enfin, les comptes génériques à privilèges sont strictement interdits. Dans le cas où l'utilisation d'un tel compte est nécessaire, une demande justifiée devra être adressée à la RSSI de l'Afpa, afin d'attribuer ou non une dérogation.</p>	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-016	Contrôles d'accès	<p>Tout système d'information doit être configuré pour limiter l'accès aux seuls utilisateurs strictement autorisés, ou processus et matériels agissant comme tel.</p> <p>Ces derniers ne doivent pouvoir accéder qu'aux seules informations et fonctions strictement nécessaires à leur activité et pour lesquelles ils ont reçu une autorisation.</p> <p>Conformément à la politique de gestion des mots de passe de l'Afpa, un mécanisme de limitation d'essais d'authentification doit être implémenté afin de bloquer les tentatives de connexion par force brute. Le nombre de tentatives d'authentifications est fixé de manière inversement proportionnelle au niveau de privilèges de l'utilisateur.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-017	Utilisation du login / mot de passe	<p>Les SI mettant en œuvre une authentification par login et mot de passe doivent être conformes à la politique des mots de passe de l'Afpa.</p> <p>De plus, l'authentification applicative des utilisateurs par mot de passe doit se faire au travers du référentiel unique Active Directory.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 22 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

EX-018	Droits d'accès	<p>Tout système d'information doit permettre la spécification et le contrôle de droits d'accès accordés aux utilisateurs ou groupes d'utilisateurs. Ces droits d'accès doivent suivre le principe suivant : « tout est interdit sauf ce qui a été explicitement autorisé ».</p> <p>La solution doit appliquer les autorisations adéquates pour chacune des tentatives d'accès et ce, jusqu'à la granularité de l'utilisateur individuel. Pour les comptes à privilèges, la mise en place d'une revue est nécessaire. La fréquence de cette revue est au minimum deux fois par an.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-019	Contrôle des droits d'accès	<p>Il convient également de procéder, une à deux fois par an, à un réexamen complet des droits d'accès (revue de compte) et de supprimer les comptes ou les autorisations d'accès qui ne sont plus nécessaires.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-020	Gestion des sessions	<p>L'accès doit être soumis à une procédure d'ouverture et de maintien de session sécurisée (écoute, rejeu...).</p> <p>La solution technique retenue doit systématiquement offrir un mécanisme de déconnexion mettant fin à la session.</p> <p>Elle doit permettre de verrouiller ou mettre fin à la session de l'utilisateur au terme d'une période d'inactivité paramétrable (par défaut 30 minutes). En cas d'impossibilité technique, un temps maximal de connexion paramétrable doit être implémenté.</p> <p>La solution doit permettre de contrôler le nombre de sessions concourantes. Par défaut, aucune session concourante n'est autorisée.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-021	Cas d'un système critique	<p>Les systèmes critiques doivent respecter les règles supplémentaires suivantes :</p> <ul style="list-style-type: none"> Avant l'établissement d'une connexion ou avant l'échange de données de l'utilisateur, l'entité homologue (ordinateur, processus ou utilisateur) 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 23 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		<p>doit être identifiée et authentifiée de façon unique ;</p> <ul style="list-style-type: none"> • Les données de l'utilisateur ne doivent être échangées qu'après le succès de l'identification et de l'authentification ; • A la réception de données, il doit être possible d'identifier et d'authentifier de façon unique leur émetteur. <p>D'un point de vue technique, le système peut disposer d'une authentification forte, à savoir ayant à minima deux éléments de preuve (ou facteurs d'authentification) pour authentifier l'entité demandant un accès.</p>	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
--	--	---	---

7. Chiffrement

7.1 Fonctions cryptographiques et chiffrement

Objectif :

Le chiffrement et le hachage sont des techniques importantes en matière de sécurité informatique. Le chiffrement permet de protéger les données en les rendant illisibles pour toute personne qui n'a pas la clé de déchiffrement appropriée. Cela est particulièrement utile pour protéger les informations sensibles telles que les mots de passe, et les informations personnelles.

Le hachage, quant à lui, permet de créer une empreinte numérique unique d'un fichier ou d'un message, qui peut être utilisée pour vérifier l'intégrité des données. Cela permet de s'assurer que les données n'ont pas été modifiées ou altérées de manière malveillante.


Risques :

L'utilisation d'algorithmes de chiffrement et fonctions de hachages obsolètes présente un risque important de sécurité. Les pirates peuvent utiliser des techniques telles que la cryptanalyse ou des attaques par force brute pour déchiffrer des messages qui sont chiffrés avec des algorithmes faibles. De plus, ce type d'algorithmes peut également :

- Être vulnérable à des attaques de type man-in-the-middle,
- Permettre de Modifier des messages chiffrés et les envoyer à la place des messages originaux,

A titre d'exemple, les algorithmes et fonctions tels que **DES, 3DES, MD5 et SHA1** sont considérés comme obsolètes et ne sont plus recommandés.

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-022	Utilisation d'algorithmes de chiffrement recommandés par l'ANSSI	<p>A date (janvier 2023), l'ANSSI et la CNIL recommandent les algorithmes suivants :</p> <ul style="list-style-type: none"> • SHA-256, SHA-512 ou SHA-3 comme fonction de hachage ; • HMAC utilisant SHA-256, bcrypt, scrypt ou PBKDF2 pour stocker les mots de passe ; • AES ou AES-CBC pour le chiffrement symétrique ; 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 25 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

	<ul style="list-style-type: none"> • RSA-OAEP comme défini dans PKCS#1 v2.1 pour le chiffrement asymétrique ; • Enfin, pour les signatures, RSA-SSA-PSS comme spécifié dans PKCS#1 v2.1. <p>Il est également important d'utiliser des tailles de clés suffisantes, pour AES il est recommandé d'utiliser des clés de 128 bits et, pour les algorithmes basés sur RSA, des modules et exposants secrets d'au moins 2048 bits ou 3072 bits, avec des exposants publics, pour le chiffrement, supérieurs à 65536.</p> <p>A noter que ces recommandations évoluent dans le temps, ainsi les références restent les recommandations de l'ANSSI et la CNIL.</p>	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
--	---	--


8. Sécurité physique et environnementale

8.1 Gestion des accès physiques et matériels de sécurité


Objectif :
La protection de l'information nécessite en tout premier lieu de se prémunir de tout incident ou attaque des supports matériels physiques contenant des données sensibles : supports amovibles, disques, serveurs, etc.

Risques :
L'absence de mesures de protection et de prévention physique entraîne un risque d'incident, accidentel ou volontaire portant sur des zones, équipements et données sensibles dont les conséquences peuvent être des atteintes : <ul style="list-style-type: none"> • Au patrimoine SI de l'entreprise ; • A la disponibilité des activités métiers.

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-023	Contrôles d'accès physique aux locaux	L'accès aux locaux techniques, armoires et aux équipements informatiques (serveurs, commutateurs, etc.) ne doit être autorisé qu'aux personnes dûment habilitées. Les ouvertures restantes doivent être sécurisées (fenêtres à barreau, etc.).	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-024	Traçabilité des accès physiques aux locaux	Une liste d'utilisateurs disposant des accès doit être établie et contrôlée régulièrement. Le prêt des clés ou badges est interdit. Les entrées et sorties doivent être tracées. Dans le cas de projets critiques, l'utilisation de moyens d'accès (clé, badge) spécifiques doit être envisagée.	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-025	Accès physiques aux équipements informatiques	Tous les équipements informatiques (serveurs, routeurs, commutateurs, etc.) doivent être mis dans des baies fermées à clé.	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 27 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-026	Typologie des locaux	<p>Il convient de s'assurer que tout local informatique, soit à minima conforme aux règles de l'art en termes de sécurité physique et environnementale :</p> <ul style="list-style-type: none"> • Climatisation ; • Détection et extinction incendie ; • Secours électriques ; • Protection contre le dégât des eaux, • ... 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-027	Accessibilité des prises réseaux	<p>Les prises réseaux ne doivent pas être en libre accès.</p> <p>En cohérence avec les exigences précédentes, en particulier la fermeture des armoires et la désactivation des ports inutilisés des commutateurs/routeurs réseaux, il ne doit pas être possible de connecter un système tiers sur le réseau.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-028	Connexion d'équipements tiers	<p>Par principe, il est formellement interdit de connecter sur un SI des équipements qui contourneraient les exigences de sécurité explicitées ci-dessus. Pour exemple, il est formellement interdit d'ajouter des équipements de communication (mini-hubs, commutateurs, routeurs) qui ne seraient pas décrits dans les documents de réalisation et qui permettraient notamment de contourner l'EX-027.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 28 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

9. Sécurité liée à l'exploitation

9.1 Protection contre les logiciels malveillants

Objectif :

Les virus représentent une menace réelle et sont une des préoccupations majeures de l'Afpa. Ils sont synonymes de risques d'attaques logiques dont la potentialité est particulièrement élevée dans un contexte de systèmes d'informations fortement communicants.

Risques :

Les conséquences sur des équipements insuffisamment protégés sont notamment :

- L'indisponibilité temporaire de ressources ou de services informatiques, conséquente à l'infection et/ou aux actions de désinfection ;
- La perte de données provoquée par la charge destructrice de certains codes malveillants ;
- L'intrusion logique sur les réseaux et systèmes de l'entreprise ;
- La diffusion de codes malveillants vers des partenaires de l'entreprise ou à des systèmes tiers de l'Afpa (via la messagerie électronique ou un support amovible infecté).

Dans ce contexte, il importe de mettre en place l'ensemble des moyens indispensables à une protection efficace des SI contre la menace d'infection informatique.

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-029	Logiciels anti-virus	<p>Le déploiement de logiciels anti-virus est obligatoire sur les systèmes d'information situés en réseau privé.</p> <p>Ces anti-virus doivent être installés sur tous les serveurs et postes clients. En parallèle du déploiement d'anti-virus, une politique de mise à jour de ces logiciels et des bases de signatures virales doit être rédigée et mise en place.</p> <p>Dans le cadre de SI, notamment orientés métiers, il est strictement nécessaire de mettre en œuvre et déployer des solutions anti-virales en ayant au préalable étudié l'impact, à la fois sur la disponibilité (dysfonctionnement anti-virus, etc.) et sur la sécurité du système (processus de mise à jour des bases antivirales, etc.).</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

9.2 Sauvegardes

Objectif :
Toute solution informatique est à considérer comme faillible du fait de la possibilité de panne matérielle, de suppression ou modification accidentelle de données, voire d'attaques logicielles (virus) pouvant porter atteinte à sa disponibilité et son intégrité.

Risques :
Lors d'un incident, l'absence de sauvegardes des systèmes fait porter les risques suivants : <ul style="list-style-type: none"> • Impossibilité de redémarrer les systèmes • Perte définitive de données • Etc


Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-030	Obligation de sauvegarde	Les sauvegardes ont pour vocation de restaurer un système dans un mode de fonctionnement nominal suite à un incident (perte partielle ou totale d'un disque, effacement malencontreux de fichiers, etc.), afin d'assurer la perte minimale de données et de disponibilité du service. La mise en place de sauvegarde est obligatoire dans tout projet, et sa conception doit être prévue dès la phase d'ingénierie du projet. Note : La DSI doit prendre en compte les exigences de la MOA en termes de temps de rétention (durée de conservation d'une sauvegarde avant sa suppression) et par conséquent le nombre de jours en arrière d'activité qu'implique la restauration d'une sauvegarde sur un système.	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-031	Données sauvegardées	La sauvegarde doit être exhaustive (les données, les applications, les systèmes, ...). Exception faite pour les solutions SaaS qui doivent permettre une sauvegarde des données exportable et réutilisable.	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

EX-032	Procédures de sauvegarde	<p>Les sauvegardes doivent être réalisées à date régulière et de façon le plus automatique possible. Des tests de restauration doivent être faits régulièrement dans le but de valider :</p> <ul style="list-style-type: none"> • La qualité du support de sauvegarde ; • La cohérence des sauvegardes ; • L'absence de perte de données ; • La qualité des procédures. <p>Ces tests doivent être effectués dès la conception de l'architecture de sauvegarde.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-033	Localisation des sauvegardes	<p>Les sauvegardes ne doivent en aucun cas être stockées dans le même local, ou le même site que les serveurs dont elles sont issues.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

9.3 Journalisation et surveillance

Objectif :
Créer, tenir à jour et vérifier régulièrement des journaux d'évènements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information. C'est un élément primordial pour assurer la sécurité des traitements, obligation posée à l'article 5 du RGPD.

Risques :
<ul style="list-style-type: none"> • Perte de données : sans journalisation, il est impossible de retracer les actions et les modifications effectuées sur les données. • Faible sécurité : sans journalisation, il est difficile de détecter les tentatives d'intrusion ou les activités malveillantes. • Faible conformité : sans journalisation, il est difficile de respecter les normes et les réglementations en matière de sécurité et de confidentialité des données. • Faible fiabilité : sans journalisation, il est difficile de diagnostiquer et de résoudre les problèmes techniques. • Faible auditabilité : sans journalisation, il est difficile de prouver les actions effectuées sur le système et de les justifier en cas de besoin.

Page 31 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-034	Traitement des traces - alertes	<p>Tout système informatique doit créer, protéger et archiver une journalisation des événements système et applicatifs permettant par analyse fine de :</p> <ul style="list-style-type: none"> • Vérifier les connexions (réussite ou échec) au système ou à l'application et détecter les tentatives d'intrusions non autorisées ; • Vérifier l'état du système (cpu, mémoire, etc), disques (taux de remplissage, etc.), de l'application (nombre de licences atteint) ou détecter toute anomalie ou activité non autorisée concernant le système ou une application : <ul style="list-style-type: none"> ○ Changement de droits sur un fichier ; ○ Modification des privilèges d'un utilisateur ou groupe ; ○ Ouverture de fichier sensible, activation d'une fonction spécifique ; ○ ... <p>L'ensemble de ces événements tracés doit :</p> <ul style="list-style-type: none"> • Être horodatés ; • Décrits comme échec ou succès ; • Associés à l'utilisateur / processus qui l'a commis. <p>Toute modification ou lecture des fonctions et informations d'audit doit être aussi tracée.</p> <p>En fonction des exigences de sécurité du RSSI le traitement des fichiers de traces pourra être réalisé au moyen d'un serveur logiciel de type syslog.</p> <p>Dans le cas où le SI est installé sur un réseau équipé d'une sonde de détection d'intrusion, les alertes sont transmises directement vers cette sonde de détection qui concentre et diffuse aux équipes</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

		<p>d'administration concernées les anomalies rencontrées.</p> <p>Enfin, par application du principe de moindre privilège, chaque journal doit être protégé et accessible uniquement à partir de comptes pour lesquels il existe des justifications opérationnelles (validées par l'Afpa) à l'octroi de ces privilèges.</p>	
--	--	--	--

9.4 Maitrise des logiciels en exploitation & protection des systèmes

Objectif :

Les systèmes d'exploitation sont devenus au fil des années d'une complexité suffisante pour nécessiter une analyse de sécurité spécifique avant de déployer des applications sur ces derniers. La non-maîtrise de ces systèmes risque d'engendrer des vulnérabilités dont l'exploitation pourrait porter au bon fonctionnement des SI.

De plus, une installation et une configuration d'un système adaptées au juste besoin est vecteur de fiabilité, performance et disponibilité.

Risques :

Les systèmes actuels disposent encore de nombreux comptes et services réseaux par défaut vulnérables à des attaques logicielles qui, s'ils ne sont pas désactivés, rendent aisée la compromission du système.


L'utilisation frauduleuse de ces services et comptes permet, par exemple, à des attaquants de :

- S'introduire de façon illicite sur les équipements ;
- De récupérer / modifier des informations sensibles ou d'interrompre le fonctionnement des applications métiers installées.


De même un défaut de sécurisation des équipements de commutations et routage permet :

- La capture illicite de flux sensibles par des intrus connectés au réseau de l'Afpa (mots de passe de connexions, fichiers, etc.) ;
- La propagation de virus au travers de l'ensemble du réseau informatique ;
- La saturation des ports de serveurs connectés via des attaques cibles ;
- ...


Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-035	Installation minimale	<p>Toute opération d'installation doit commencer par l'étude précise des besoins et l'identification des fonctions à remplir par l'équipement informatique. Toute installation dite « par défaut » est interdite. Une installation système optimisée doit satisfaire les critères suivants :</p> <ul style="list-style-type: none"> • Ne doivent être installés sur le système que les logiciels systèmes utiles et seulement ceux-ci ; • Ne doivent être installés sur le système que les applicatifs utiles identifiés dans la spécification de besoin. 	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-036	Installation standardisée	<p>Les systèmes doivent faire l'objet d'une installation soignée. Les éléments suivants doivent être respectés :</p> <ul style="list-style-type: none"> • Les disques doivent être partitionnés de façon à séparer le système d'exploitation des données et des applications ; • Les enregistrements et traces doivent être stockés sur des partitions ou ressources ne provoquant pas l'arrêt du système en cas de saturation de ces espaces. <p>Dans le cas des systèmes critiques, des actions de durcissement (hardening) devront être réalisées, conformément aux recommandations de l'ANSSI, notamment les principes de minimisation, moindre privilège, défense en profondeur, Secure Boot, configuration statique et dynamique sécurisée, etc.</p>	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 34 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

EX-037	Services réseaux	<p>Le système installé doit être correctement paramétré. Il doit disposer uniquement des services nécessaires aux applications, à l'exploitation, l'administration, la maintenance et la supervision. L'ensemble de ces services réseaux (http, smtp, ssh,...), doit faire l'objet d'une installation et d'une configuration conforme aux règles de l'art.</p> <p>Toute configuration dite « par défaut » est bannie.</p> <p>Ainsi :</p> <ul style="list-style-type: none"> • Tous les services réseaux non utilisés ne doivent pas être démarrés ; • Les services réseaux en écoute, notamment ceux utilisés pour les travaux d'administration, doivent être correctement paramétrés afin de n'autoriser que des utilisateurs dûment authentifiés ; • Les services réseaux, connus pour leur vulnérabilité (telnet, ftp, rpc com/dcom microsoft, séries des ports tcp 135, 137, 139 et 445 etc.) sont interdits. 	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-038	Cas de systèmes critiques	<p>Pour les équipements informatiques situés dans des zones à risques (locaux techniques ou datacenter), leur sécurité physique sera renforcée par la fermeture des ports de commutateurs non utilisés. Ces exigences peuvent être complétées par une sécurisation des équipements réseaux :</p> <ul style="list-style-type: none"> • Activation du « Storm Control » : limitation des bandes passantes sur chaque port ; • Activation de « Port Security » : limitation du nombre d'adresses MAC autorisées sur chaque port, pour 	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 35 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		<p>contrer des attaques d'épuisement de pools d'IP de serveurs DHCP ;</p> <ul style="list-style-type: none"> • Activation du « DHCP Snopping » : interdiction de réponses DHCP venant de serveurs pirates ; • Activation de « l'ARP Inspection » : interdiction de modification des tables ARP par des pirates, dans le but de réaliser des attaques Man in the Middle ; • Filtrage par adresse MAC pour les ports utilisés • Fermeture de port de management • Mise en service de 802.1x 	<input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-039	Accès aux médias amovibles	<p>Une attention particulière doit être portée sur les vecteurs d'entrée des vers, virus et programmes pouvant conduire à une baisse de la fiabilité, disponibilité et confidentialité des systèmes en production.</p> <p>Un des moyens à privilégier est la condamnation des équipements de type périphériques identifiés ci-dessous :</p> <ul style="list-style-type: none"> • Port USB (clé USB) ; • Eventuellement carte type média (smart card, etc). <p>Il est recommandé que les accès à ces périphériques soient contrôlés et que seules les personnes accréditées à intervenir sur les machines puissent en obtenir l'accès.</p> <p>La solution optimale est de désactiver de façon logicielle (non-installation des drivers) l'ensemble des périphériques, comme mentionné dans l'EX-007.</p>	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 36 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information


EX-040	Accessibilité au système	<p>Les moyens de connexions en local et de façon distante doivent être passés en revue :</p> <ul style="list-style-type: none"> • Protection du système d'exploitation et du bios par mot de passe ; • Impossibilité de prendre le contrôle au moyen d'un média amovible ; • Tout service utilisé pour la télémaintenance doit être conforme aux exigences du chapitre « <u>Liaison de télé-opération</u> ». <p>Les systèmes d'information doivent présenter une bannière d'accueil mettant en garde toute personne qui se connecte sur le système considéré alors qu'elle n'y est pas dûment autorisée. Cette bannière d'accueil pourra être la suivante : « L'UTILISATION DE CE SYSTEME EST RESERVEE AUX SEULES PERSONNES AUTORISEES. L'activité des personnes qui utiliseraient cet ordinateur sans autorisation, ou par détournement d'autorisation, sera sujette à enregistrement par les administrateurs du système. Le processus d'enregistrement des activités des utilisateurs non autorisés conduit à l'enregistrement des activités des utilisateurs normalement habilités. Par conséquent toute personne utilisant ce système donne son accord à l'enregistrement de son activité et est avisée que si la surveillance faite à partir de ces enregistrements révélait une quelconque activité illégale, les administrateurs du système pourraient fournir les traces de cette activité à la justice. »</p>	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-041	Authentification et droits	<p>Les comptes d'utilisateurs et administrateurs et leurs droits associés doivent être restreints au strict nécessaire. Les comptes par défaut doivent être désactivés ou leur sécurité renforcée.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

9.5 Gestion des vulnérabilités techniques

Objectif :
<p>A l'issue du développement et de l'installation de systèmes et applications, un audit de sécurité est mené. Cependant, une fois le plan d'action sécurité réalisé, l'entreprise se doit de continuer à maintenir un niveau de sécurité constant sur ces solutions mises en service.</p> <p>Le maintien a un bon niveau de sécurité du système impose la prise en compte d'exigences par les exploitants et les mainteneurs.</p>

Risques :
<p>Le risque principal est l'apparition de nouvelles vulnérabilités pouvant avoir un impact sur les critères classiques de confidentialité, d'intégrité et de disponibilité.</p> <p>Elles sont issues :</p> <ul style="list-style-type: none"> • Du cycle de vie d'un système d'information ; • De la mise en service de nouvelles versions ; • De la modification d'un paramétrage de configuration ; • ...

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-042	Gestion opérationnelle de la sécurité	<p>Il s'agit de détecter, analyser, signaler et éradiquer tout incident de sécurité.</p> <p>Ces incidents de sécurité doivent être systématiquement remontés dès qu'ils sont avérés à la RSSI de l'AFPA. Il convient également de surveiller l'apparition de nouvelles vulnérabilités et d'entreprendre en conséquence l'ensemble des mesures nécessaires (application des correctifs de sécurité, mesures conservatoires, ...).</p> <p>Il doit être mené périodiquement des audits de sécurité pour les systèmes critiques afin de contrôler ou vérifier le maintien du niveau de sécurité.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-043	Installation de mises-à-jour de sécurité	Les systèmes d'exploitations et applications doivent supporter l'installation des correctifs de sécurité émis au fil du temps par les éditeurs ou connues par	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS


Page 38 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		le titulaire. Les systèmes doivent être à jour lors de la remise d'ouvrage.	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-044	Gestion des modifications	<p>Il s'agit de contrôler et d'analyser l'impact sur la sécurité de tout changement apporté au SI dans le cadre d'opérations de maintenance évolutive, corrective, adaptative, etc. Il convient également de maintenir à jour l'ensemble de la documentation et les procédures associées.</p> <p>Les interventions directes en environnement de production sont par défaut interdites. Si celles-ci sont absolument nécessaires, alors elles doivent être explicitement autorisées par la MOA, les responsables projets DSI et l'exploitant, tracées et documentées.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

9.6 Hébergement de SI à l'extérieur de l'AFPA

Objectif :
Dans le cadre de l'hébergement de systèmes d'information en dehors de l'entreprise, l'ensemble des recommandations issues des documents de sécurité SI est applicable.

Risques :
<p>Les principaux risques associés, dans le cas d'un hébergement de SI non sécurisé, dépendent des données et du type de SI considéré. Dans ce cadre, tous les risques seront identifiés dans un document les recensant de manière à en assurant le suivi et le partage avec les acteurs concernés :</p> <ul style="list-style-type: none"> • Atteinte à la disponibilité de systèmes ; • Divulcation d'informations ; • Intrusion dans un système d'information de l'entreprise ; • Atteinte à l'image de marque ; • Altération de données ; • Fraude ; • Dénier de services ; • etc.

Page 39 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-045	Exigences obligatoires	Les systèmes d'information hébergés en dehors de l'entreprise doivent satisfaire aux mêmes exigences que les systèmes installés au sein de l'entreprise. Des exigences de sécurité, issues des exigences formulées dans ce document, doivent donc être transmises à l'hébergeur ou au fournisseur Cloud.	<input checked="" type="checkbox"/> On-Prem
			<input checked="" type="checkbox"/> SaaS
			<input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant
			<input checked="" type="checkbox"/> TMA
EX-046	Conformité au niveau de sécurité	Le niveau de sécurité attendu pour les systèmes hébergés dans un datacenter ou dans le Cloud doit être identique au niveau de sécurité des systèmes dont l'exploitation est assurée par la DSI de l'entreprise.	<input checked="" type="checkbox"/> Autre
			<input checked="" type="checkbox"/> On-Prem
			<input checked="" type="checkbox"/> SaaS
			<input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant
EX-047	Non-mutualisation d'un système hébergé	Les systèmes hébergés, en dehors de l'entreprise, ne peuvent pas être mutualisés sur une plate-forme technique avec d'autres entreprises. Une dérogation est possible et doit être adressé au RSSI si les données stockées dans ces systèmes hébergés sont chiffrées.	<input checked="" type="checkbox"/> TMA
			<input checked="" type="checkbox"/> Autre
			<input checked="" type="checkbox"/> On-Prem
			<input type="checkbox"/> SaaS
			<input checked="" type="checkbox"/> IaaS/PaaS
EX-048	Accès à distance pour des opérations d'administration et de supervision	Les opérations d'administration et de supervision doivent respecter l'exigence EX-034. Cette exigence est satisfaite si les accès distants utilisent un bastion intégrant une double authentification.	<input checked="" type="checkbox"/> Infogérant
			<input checked="" type="checkbox"/> TMA
			<input checked="" type="checkbox"/> Autre
			<input checked="" type="checkbox"/> On-Prem
			<input type="checkbox"/> SaaS


10. Sécurité des communications

10.1 Management de la sécurité des réseaux


Objectif :
<p>Depuis plusieurs années, les systèmes d'information doivent répondre à des nouveaux contextes d'échange impliquant l'interconnexion de réseaux de niveaux de sécurité non homogènes.</p> <p>Le cloisonnement, s'il est bien étanche, permet de protéger les systèmes contre toute attaque informatique, intentionnelle (hacking, DDoS) ou non intentionnelle (Virus, Vers, ...). Il faut le considérer comme un principe structurant de la maîtrise et de la sécurité des échanges entre les systèmes et un facteur clé de la disponibilité.</p>

Risques :
<p>Les systèmes informatiques, devenus premiers vecteurs de propagation de l'information au sein d'une entreprise, sont aussi les principaux supports d'attaques et outils de propagation de risques majeurs tels que :</p> <ul style="list-style-type: none"> • Le vol ou la modification de données par intrusion illicite sur les systèmes ou par interception des flux d'informations échangées ; • L'atteinte à la disponibilité des SI par intrusion ou attaques depuis des réseaux de confiances ou tiers.


Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-049	Obligation de cloisonnement	Afin de maîtriser les conditions d'accès aux systèmes, un cloisonnement doit être mis en place. Au sein de ce système cloisonné, il doit être possible de disposer de mécanismes permettant la séparation des flux propres à une application.	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-050	Choix du système de cloisonnement	<p>Le type de cloisonnement doit être choisi en fonction du niveau de criticité du système.</p> <p>Dans le cas d'un système vital pour l'activité de l'entreprise un firewall de type appliance ou FWaaS doit être privilégié. Toute autre solution de</p>	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 41 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		<p>cloisonnement doit garantir un niveau de sécurité adéquat.</p> <p>Dans le cadre de tout système jugé non vital, le cloisonnement peut être logique (le système assure sa propre protection). Ceci impose que le système est maintenu à jour en termes de sécurité et qu'il embarque des dispositifs de protection efficaces.</p>	<input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-051	Configuration du système de cloisonnement	<p>Le cloisonnement des systèmes doit être configuré selon les règles suivantes :</p> <ul style="list-style-type: none"> Les accès aux systèmes et flux d'information cloisonnés doivent être réduits au strict besoin, spécifiés et contrôlés, selon les principes : « tout est interdit sauf ce qui a été explicitement autorisé » et « seuls les flux strictement nécessaires sont autorisés » ; Les services et protocoles vecteurs de vulnérabilités (ex : partage de ressources, rpc com/dcom microsoft, séries des ports tcp 135, 137, 139 et 445, ftp, telnet, r-cmd, etc.) <u>sont interdits</u> et doivent être remplacés par des services ou des protocoles qui implémentent une couche sécurité et avec obtention d'une dérogation: <ul style="list-style-type: none"> HTTPS, ssh, sftp... L'initialisation des connexions est à réaliser de l'interne (zone protégée) vers l'externe (zone non protégée ou DMZ) en vue de ne pas permettre de tentatives de fraude. 	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-052	Isolement des flux	<p>Dans le cadre de systèmes différents reposant sur le même réseau, des systèmes spécifiques pour séparer les flux doivent être mis en œuvre :</p> <ul style="list-style-type: none"> VLAN filtrés pour postes clients, serveurs, administration, ... ; IPSEC ; MPLS ; 	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 42 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		Les flux doivent être routés et filtrés selon la matrice de flux établi, élaborée au strict nécessaire et validée par la RSSI.	
EX-053	Interconnexion avec d'autres systèmes	<p>L'ensemble des accès avec des réseaux externes ou partenaires doit transiter par la plateforme d'accès sécurisé de l'Afpa.</p> <p>Cette plateforme, gérée par l'Afpa, permet d'assurer le cloisonnement, de superviser et de contrôler les accès des tiers externes qui se connectent au SI de l'Afpa.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-54	Supervision des flux	<p>Le système de cloisonnement doit créer, protéger et archiver des journaux d'audits. Ces journaux permettent de superviser, analyser, reporter toute activité inappropriée ou non autorisée, dans le système cloisonné ou à travers la cloison.</p> <p>Toute anomalie doit être remontée en temps réel aux administrateurs des systèmes de cloisonnement.</p> <p>Le protocole recommandé est la dernière version de SNMP (v3 à la date d'écriture du document)</p>	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-55	Sécurité Intrinsèque	<p>Le système de cloisonnement doit en outre disposer de ses propres mécanismes en charge d'assurer sa sécurité (cf. autres chapitres). Il doit répondre aussi à des exigences de performance et de disponibilité suffisantes pour ne pas porter atteinte au fonctionnement du système qu'il est censé protéger (cf. le chapitre "Architecture et Disponibilité").</p>	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-56	Cas des systèmes critiques	<p>Les SI critiques ne doivent pas être visibles depuis le réseau de l'Afpa, voir celui de partenaires, par des personnes non habilitées, ou par des systèmes potentiellement vecteurs d'attaques (ex : attaque virale, etc.). Des dispositifs de cloisonnement doivent les protéger d'attaques internes ou externes.</p> <p>Cette disposition est toujours vraie quand le système est constitué d'un ou plusieurs sous-réseaux ou qu'il est interconnecté avec d'autres systèmes. L'accès au système et à ses réseaux, doit</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 43 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information


		se faire au travers de ce dispositif de cloisonnement.	
--	--	--	--

10.2 Liaison de télé-opération


Objectif :
<p>Dans le cadre d'action de télé-opération (administration à distance) des demandes d'accès à partir de réseaux externes à l'Afpa peuvent être effectuées par la DSI et accordées par le directeur du département concerné et la RSSI.</p> <p>Ces demandes doivent respecter des principes de sécurité stricts qui garantissent que seules les personnes habilitées ont la possibilité de se connecter aux systèmes. Elles doivent donc s'appuyer sur des recommandations d'ordre technique et organisationnel conformément à la politique de sécurité de l'entreprise.</p>

Risques :
<p>Les principaux risques associés, dans le cas d'utilisation d'une liaison de télé-opération non sécurisée, sont les suivants :</p> <ul style="list-style-type: none"> • Visibilité non contrôlée du système à partir d'internet en cas de connexion via ce réseau ; • Visibilité non contrainte du système à partir des locaux du prestataire (infogérant, TMA, etc). <p>Les conséquences peuvent être les suivantes :</p> <ul style="list-style-type: none"> • Dénier de service ; • Utilisation des fonctions du système par une personne non habilitée (arrêt, relance, passage de commandes, etc), voir prise de contrôle totale ; • Atteinte à l'image de marque de l'entreprise.


Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-057	Bastion	La liaison doit respecter la règle suivante concernant toute liaison de transmission vers un réseau ou un SI externe à l'entreprise. Les échanges doivent passer par le bastion sous contrôle centralisé de la DSI. Si des cas de liaisons directes	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 44 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		existent ou sont nécessaires, ils doivent être dûment justifiés pour obtenir une dérogation du RSSI de l'Afpa. Ces cas de liaisons directes doivent garantir un niveau de sécurité égal ou supérieur à celui du bastion. Dans ce cadre, les préconisations de la DSI concernant cette liaison doivent être respectées absolument.	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-058	Interconnexion avec le réseau de l'Afpa	Dans le cas d'une double interconnexion avec un SI externe (TMA, prestataires, etc.) et le réseau d'entreprise, il ne peut être accordée de dérogation.	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-059	Postes et sites de télé-opération	<p>Les postes de télé-opération doivent présenter des caractéristiques strictes de sécurité, tels que :</p> <ul style="list-style-type: none"> • Sécurité logique et réseau (DMZ non publique chez le titulaire, accès contrôlés des locaux, etc.) ; • Pas de mutualisation de ressources avec d'autres clients autres que l'Afpa ; • Conditions d'accès et d'utilisation strictes ; • Installation et configuration sécurisées et au juste besoin ; • Sessions d'administration chiffrées. <p>Le niveau de sécurité du poste distant doit être équivalent au niveau de sécurité du système télé-opéré.</p>	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre

Page 45 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

EX-060	Contrat d'utilisation	<p>Un contrat d'utilisation de cette liaison sera signé par le titulaire (TMA, infogérant, etc.). Il a pour but de fixer les contraintes d'utilisation. Tout non-respect de ce contrat entraîne l'interruption d'utilisation de la liaison de télémaintenance.</p> <p>Exemple de contraintes :</p> <ul style="list-style-type: none"> • Contraintes horaires : de 8h00 à 19h00 jours ouvrés ; • Contraintes réglementaires : utilisation seulement après accord du domaine manager ou du directeur de département ou de toute autre personne ayant autorité pour le faire ; • Contrainte d'accès : la liaison est toujours « down » et est activée à la demande ; • ... <p>Des clauses de confidentialité doivent être incluses dans le contrat, comme :</p> <ul style="list-style-type: none"> • Le prestataire s'engage formellement à effectuer, sur le SI Afpa, les seuls actes prévus dans le cadre strict du contrat de 	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
--------	-----------------------	--	---

Page 46 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		<p>TMA. Tout manquement à cette obligation sera constitutif d'une faute susceptible d'entraîner demande de dommages intérêts pour le préjudice subi par l'Afpa.</p> <ul style="list-style-type: none"> • Le prestataire s'engage à ce que les documents, informations, données ou méthodes de toute nature appartenant à l'Afpa : <ul style="list-style-type: none"> ○ Soient protégés et soient gardés strictement confidentielles ; ○ Ne soient divulgués et utilisés de manière interne qu'aux membres du personnel ayant à en connaître et pour l'objet initialement prévu ; ○ Ne soient ni divulgués, ni susceptibles de l'être, soit directement, soit indirectement, à tout tiers ou à toutes personnes autres que celles mentionnées ci-dessous. ○ Ne soient ni copiés, ni reproduits, ni dupliqués totalement ou partiellement lorsque de telles copies, reproductions ou duplications n'ont pas été autorisées par l'Afpa et ce, de manière spécifique et par écrit. 	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
--	--	--	---

EX-061	Systèmes de rebond	<p>Si le système ayant une liaison de télé-opération est critique en fonction de la classification portée par la RSSI, les exigences suivantes doivent être respectées :</p> <ul style="list-style-type: none"> • La communication doit être sécurisée et chiffrée de bout en bout, du poste distant au système si besoin de confidentialité et intégrité ; • Sur le poste distant, les informations doivent aussi être chiffrées si besoin de confidentialité et intégrité ; • Au-delà des enregistrements de connexions réalisés par le bastion sur les systèmes cibles, un enregistrement des commandes et des actions passées sur le système critique maintenu doit être réalisé ; • La télé-opération directe à partir du poste distant vers le système cible n'est pas autorisée. Un système, appelé poste de rebond et situé dans une zone de confinement doit être mis en place. Ce système de rebond doit être le seul à avoir accès au système cible. Toute dérogation doit être justifiée et obtenue au regard des risques et vulnérabilités identifiés sur le système cible ; • La télé-opération «nomade» n'est pas autorisée depuis un site géographique non maîtrisé et sans adresse IP fixe. 	<input checked="" type="checkbox"/> On-Prem <input type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-062	Protocoles interdits	<p>Les protocoles vecteurs de vulnérabilités (rpc com/dcom microsoft, séries des ports tcp 135, 137, 139 et 445) sont interdits.</p> <p>Cette liste pourra évoluer en fonction des contextes et de l'obsolescence des protocoles.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre


11. Acquisition, développement et maintenance des systèmes d'information

11.1 Sécurité des processus de développement, d'assistance technique et traitement des données de tests

Objectif :
De même que pour l'installation des systèmes, dont la complexité nécessite des compétences spécifiques pour retirer toute vulnérabilité, les nouvelles applications développées, ne peuvent être considérées par défaut comme dignes de confiance.

Risques :
Le recours dans les développements à des langages complexes ayant souvent une faible maturité en termes de sécurité engendre des vulnérabilités de plus en plus nombreuses. Une non-maîtrise des applications développées en interne ou par des prestataires laisse la porte ouverte à des vulnérabilités permettant, par exemple, des intrusions.

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-063	Spécifications détaillées	L'intégration et la déclinaison des exigences de sécurité exprimées au sein du CCTP dans les dossiers de spécifications détaillées doivent être réalisées. A cette occasion, il est souvent nécessaire d'affiner le processus d'appréciation et de traitement des risques.	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-064	Règles de développement	Les applications doivent être conformes aux référentiels de l'Afpa et à l'état de l'art de la sécurité. Dans ce cadre, les titulaires s'engagent à ce que leurs bibliothèques binaires soient exemptées de failles, et assurent une protection adéquate contre les :	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 49 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

		<ul style="list-style-type: none"> • Backdoor ; • Code malveillant (virus, cheval de Troie, rootkit...) ; • Vulnérabilité connue et répertoriée (CVE/CAN, CERT-A...). <p>Les développeurs doivent être sensibilisés aux règles de développement sécurisé. Enfin, afin de limiter les risques de sécurité lors du développement, l'utilisation d'outils de vérification de code tels que SonarQube est obligatoire.</p>	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-065	Environnement	Lorsqu'un titulaire a en responsabilité plusieurs type d'environnements (développement, recette, production...), il s'engage à ce que les différents environnements soient cloisonnés afin de réduire les risques d'accès ou de changements non autorisés dans le SI.	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-066	Données d'essai	Toutes données classifiées « confidentielles » ou « personnelles » doivent être modifiées ou rendues anonymes sur les environnements de développement, de recette et de préparation au fonctionnement opérationnel.	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-067	Gestion des évolutions	Dans le cadre d'évolution de versions ou configurations, il faut attribuer un numéro unique et séquentiel à chaque nouvelle version ou modification de l'application. Les évolutions et modifications doivent être documentées.	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS <input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre


12. Continuité et reprise d'activité

12.1 Plan de secours


Objectif :
Un plan de secours informatique permet un retour à un fonctionnement nominal d'une architecture informatique suite à un incident majeur (incendie, inondation, etc.), dans des délais raisonnables.

Risques :
Sans plan de secours informatique, la reprise d'activité en cas d'incident peut s'avérer plus longue et difficile. En effet une interruption partielle ou complète du système d'information peut avoir des incidences fortes sur l'activité des entreprises (impact financier, sur l'image, etc.)

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-068	Expression préalable des besoins fonctionnels	<p>La mise en place d'un plan de secours nécessite au préalable la réalisation d'un état de l'existant et d'une analyse de risques par la RSSI :</p> <ul style="list-style-type: none"> Acceptation d'une perte totale du service, de façon momentanée : <ul style="list-style-type: none"> Durée maximale d'interruption admissible (Recovery Time Objective – RTO) ; Perte de donnée maximale admissible (Recovery Point Objective – RPO). Acceptation seulement d'une dégradation du service. 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-069	Moyens utilisés	<p>Les moyens mise en œuvre peuvent être d'ordre techniques, humains ou procéduriers.</p> <ul style="list-style-type: none"> Moyens techniques : Des matériels (serveurs, disques, etc), systèmes d'exploitation et applications doivent être prévus en secours en complément des sauvegardes des données. Une image système (snapshot) peut être mis en œuvre ; 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 51 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information

		<ul style="list-style-type: none"> • Moyens humains : Selon la criticité du système, il ne pourrait être accepté de retard de remise en service du fait d'un manque de ressources humaines. Les équipes de maintenance s'assureront donc de la bonne connaissance par leurs équipes des plans de reprises techniques ; • Moyens procéduriers : Des procédures documentées et mises à jour régulièrement doivent être prévues. Elles se doivent d'être compréhensibles par l'ensemble des membres de l'équipe en charge de l'exploitation et la maintenance des systèmes. 	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-070	Plan de secours informatique	<p>Le maintien en condition opérationnelle des plans de secours informatiques est un processus continu. Il s'agit de s'assurer que les plans restent opérationnels malgré les évolutions de l'entreprise et de son environnement (technique...). Il convient ainsi de tester régulièrement les plans et définir les modalités de leur maintenance :</p> <ul style="list-style-type: none"> • Responsabilités en matière de maintenance ; • Modalités de révision (fréquence...) et de validation ; • Evènements déclencheurs exceptionnels. <p>Ces éléments doivent être définis dans le PAS.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-071	Tests du plan de secours	<p>Des tests du plan, chronométrés, doivent être effectués dans des situations « grandeurs réelle » autant que se peut. Ils doivent permettre notamment de valider :</p> <ul style="list-style-type: none"> • Le bon fonctionnement des médias de secours utilisés ; • Les temps de redémarrage estimés ; • Les taux de perte de données ; 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 52 of 53	<u>Afpa – CCTG-SSI</u>	
Version 2.0	Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information	Direction des Systèmes d'Information


	<ul style="list-style-type: none"> • La pertinence des documentations et procédures ; • La formation des acteurs et de leur familiarisation avec leurs rôles et responsabilités ; • ... <p>Il est nécessaire de définir une stratégie de tests (périmètre, acteurs, nature et ordonnancement des tests, etc.).</p> <p>Tout test réalisé, doit être documenté et les résultats analysés en vue de proposer des actions de correction et d'amélioration.</p>	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
--	---	--

11.2 Architecture, disponibilité et mécanismes de redondance

Objectif :
La mise en place de sécurité dans les architectures a également pour but de renforcer la disponibilité des SI.

Risques :
<p>Au-delà de la perte d'un équipement, dont l'impact peut être fort pour la disponibilité des applications de l'Afpa, les enjeux portent essentiellement sur les temps nécessaires pour permettre le retour à un fonctionnement nominal avec une perte de service minimale.</p> <p>Selon la qualité du travail d'ingénierie réalisé lors de la conception de l'architecture, les efforts pour pallier une perte de service seront minimes ou très consommateurs en temps et coûteux pour les mainteneurs.</p>

Numéro de l'exigence	Titre de l'exigence	Description	Application
EX-072	Redondance des équipements	Dans le cadre de systèmes sensibles, l'architecture matérielle doit être en redondée pour assurer une continuité de service. Au vu de l'analyse des risques réalisée par la RSSI, cette redondance peut se concrétiser par :	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS

Page 53 of 53	<p style="text-align: center;"><u>Afpa – CCTG-SSI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour la Sécurité des systèmes d'Information</p>	
Version 2.0		Direction des Systèmes d'Information

		<ul style="list-style-type: none"> Des équipements de secours sur un site tiers ; Des équipements de secours dans des locaux distincts d'un même site, voire dans le même local : <ul style="list-style-type: none"> (tels un cluster) Des redondances matérielles au sein d'un équipement : double alimentation, double sortie réseau, RAID, etc. 	<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-073	Redondance des connectiques réseaux	<p>Au vu des exigences de sécurité, devront être envisagées les redondances des interconnexions réseaux :</p> <ul style="list-style-type: none"> Au niveau des serveurs ; Au niveau des réseaux d'accès ; Au niveau des réseaux de backbone. <p>Les solutions peuvent être du type :</p> <ul style="list-style-type: none"> Redondance des ports réseaux, Raccordement des serveurs à deux commutateurs d'accès ou deux backbone distincts, etc. 	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre
EX-074	Mécanismes d'aide à la redondance	<p>Des architectures techniques et applicatives, telles des mécanismes de « haute disponibilité » doivent être conçues pour faciliter autant que possible la mise en service d'équipements de secours.</p> <p>Ces solutions peuvent être basées sur l'utilisation :</p> <ul style="list-style-type: none"> de bascule automatique sur une deuxième carte réseau ; d'IP virtuelle pointant sur plusieurs serveurs ; ... <p>Les équipements peuvent être utilisés en « Actif / Passif » ou en « Partage de Charge ».</p> <p>La mise en service d'équipements de secours de façon manuelle peut toutefois être autorisée, mais elle doit satisfaire les exigences du RSSI.</p> <p>De même, des mécanismes de routage devront être mis en place pour faciliter la reprise de nouvelle route en cas de perte de commutateurs, tels Spanning Tree, HSRP.</p>	<input checked="" type="checkbox"/> On-Prem <input checked="" type="checkbox"/> SaaS <input checked="" type="checkbox"/> IaaS/PaaS
			<input checked="" type="checkbox"/> Infogérant <input checked="" type="checkbox"/> TMA <input checked="" type="checkbox"/> Autre