

**Maintenance préventive et corrective des
installations de sûreté dans les établissements du
ressort de la Direction Interrégionale des Services
Pénitentiaires Grand-Ouest**

C.C.T.P. - ANNEXE 06 – PSSI Sûreté
(Politiques de sécurité des systèmes d'information)

Fiche de contrôle du document

Caractéristiques du document

Identification :	RI.01 - PSSI_Surete-2.1.docx
Objet :	PSSI Sûreté
Version :	Version 2.1 du 29/11/2024

Contributeurs

NOM Prénom (trigramme)	Fonction
David DU SERRE-TELMON (DST)	Consultant SSI du pôle SSI DAP
Bernard CASSOU-MOUNAT (BCM)	RCSSI DAP
Franck PERREAU (FPE)	RCSSI Adjoint DAP
Olivier SIEROCKI (OSI)	RSSI Systèmes Industriels
SDSP et SDPS (EXP)	Experts métier (DSP)
RISSI	Chaîne SSI régionale de la DAP

Suivi des versions

Version	Date	Rédacteur	Relecteur	Modification
1.0	07/06/22	DDST JKR CAU SKH	BCM FPE	Rédaction de la version initiale du document
1.1	13/06/22	SKH	FPE	Ajout références documentaires
1.2	20/06/22	DDST	FPE	Relecture et prise en compte remarques FPE
1.3	26/06/22	DDST	FPE	Revue des chapitres, mise à jour des références documentaire
1.4	25/07/22	DDST	BCM	Relecture et correction.
1.5	23/08/22	DDST	FPE	Relecture et correction.
2.0-RC0	02/09/22	DDST	FPE BCM	Pour diffusion
2.0-RC1	14/03/22	DDST	FPE BCM	Corrections mineures sur les numéros d'annexes
2.1	29/11/2024	FPE OSI	BCM	Alignement avec certaines annexes de la PSSI Préparations des références ISO27002:2022 et GRC, clarifications des renvois aux annexes.

Processus de validation

Émetteur/Rédacteur	Approbateur
Nom : Franck PERREAU Date : 29/11/2024	Nom : Bernard CASSOU-MOUNAT Date : 29/11/2024
Validation finale : Sébastien CAUWEL (DAP) Date :	

Liste de diffusion

Service	Fonction	Objet de la diffusion
SA & SM	Chefs de services	Information
SDSP et SDPS	Sous-directeurs	Information
PDS	CSN	Avis
DISP	RISSI	Information
Agents de l'Administration pénitentiaire et prestataires concernés		Information

Sommaire

Partie 1	Cadre d'emploi	6
	Avant-propos	7
1.1	Objet et champ d'application de la PSSI Sureté	7
1.1.1	Organisation des politiques de sécurité des systèmes d'information de la DAP	7
1.1.2	Périmètre d'application de la PSSI	8
1.1.3	Définition, rôles et responsabilités des acteurs	9
1.2	Entrée en vigueur	9
1.3	Pilotage et évolutions de la PSSI-DAP-SUR	10
1.4	Suivi et contrôle de l'application de la PSSI	10
Partie 2	Enjeux et Objectifs	11
2.1	Contexte et Contraintes	12
2.1.1	Contexte général	12
2.1.2	Personnel concerné par l'application des PSSI	12
2.1.3	Gestion du risque	13
2.1.4	Structure documentaire de la PSSI Sûreté	13
2.1.5	Intégration de la PSSI sûreté dans la méthode « EBIOS Risk Manager » de l'ANSSI... ..	13
2.2	Objectifs de sécurité	14
2.2.1	Mesures de sécurité	14
2.2.2	Métriques utilisées dans les analyses de risques	14
2.2.3	Métriques utilisées dans les analyses d'impact sur la protection des données (AIPD)	14
2.2.4	Nomenclature des exigences de sécurité	15
2.2.5	Déclinaison de la PSSI dans chaque système d'information de sûreté sur chaque site pénitentiaire	16
Partie 3	Règles de sécurité	17
3.1	Gestion des biens	18
3.1.1	Responsabilités relatives aux biens	18
3.1.2	Protection des informations	20
3.1.3	Manipulation des supports	24
3.1.4	Ressources humaines	27
3.2	Sécurité physique et environnementale	34
3.2.1	Zones sécurisées	34
3.2.2	Matériels	41
3.3	Gestion de l'exploitation et de la maintenance	45
3.3.1	Procédures et responsabilités liées à l'exploitation	45
3.3.2	Résilience	53

3.3.3	Sauvegarde	55
3.3.4	Protection contre les logiciels malveillants.....	61
3.3.5	Relations avec les fournisseurs	62
3.3.6	Interconnexion des réseaux	70
3.3.7	Gestion des journaux	75
3.3.8	Revue des droits d'accès utilisateurs	79
3.3.9	Politiques d'utilisation des mesures cryptographiques	80
3.4	Contrôle d'accès	81
3.4.1	Exigences générales en matière de contrôle d'accès	81
3.4.2	Gestion des accès utilisateurs	83
3.4.3	Gestion des accès à privilèges.....	87
3.4.4	Gestion des mots de passe.....	88
3.4.5	Gestion des comptes génériques.....	89
3.5	Acquisition et développement des systèmes d'information.....	91
3.5.1	Standardisation et homogénéisation des solutions techniques	91
3.5.2	Sécurité des développements et logiciels.....	92
3.6	Gestion des incidents	95
3.6.1	Responsabilité et procédures.....	95
3.6.2	Signalement des événements liés à la sécurité de l'information	96
3.6.3	Réponse aux incidents liés à la sécurité de l'information.....	97
3.6.4	Capitalisation des incidents liés à la sécurité de l'information.....	98
3.7	Gestion du plan de continuité et de reprise de l'activité	100
3.7.1	Introduction de la continuité et la reprise d'activité	100
3.7.2	Plan de continuité et reprise informatique.....	101
3.7.3	Plan de continuité et reprise d'activité	104
3.8	Conformité.....	105
3.8.1	Conformité aux obligations légales et réglementaires	105
3.8.2	Audits	106
3.8.3	Reporting.....	108

Partie 1 Cadre d'emploi

Avant-propos

La DAP dispose d'un *Glossaire des sigles et dictionnaire des termes référencés* [MJ-DAP-GLO] [RI.05] ainsi que d'un *Corpus documentaire de référence*, unifié et normalisé, référencé [MJ-DAP-REF] [RI.04].

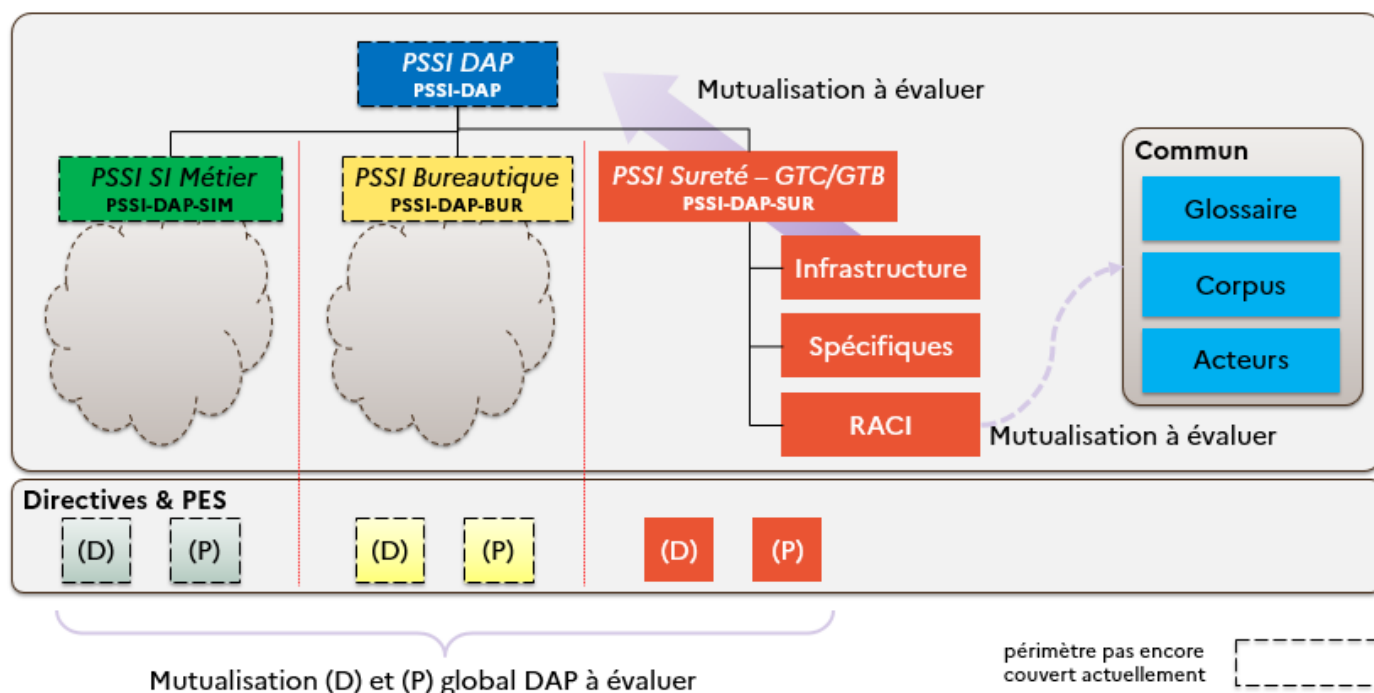
Les références entre crochet [REF] figurant dans le présent document renvoient à ce corpus documentaire (références avec numéros) d'une part, tout en permettant d'autre part une interprétation naturelle des notions abordées dans les documents référencés du corpus (références nomenclaturées et sans numéro).

Sauf mention contraire, ce document ainsi que les documents de référence qui y sont recensés sont librement consultables et peuvent être obtenus sur simple demande auprès du Responsable Central de la Sécurité des Systèmes d'Information (RCSSI) de la DAP.

1.1 Objet et champ d'application de la PSSI Sureté

1.1.1 Organisation des politiques de sécurité des systèmes d'information de la DAP

Une PSSI fixe les principes, règles et conditions de mise en œuvre composant la politique de sécurité des systèmes d'information d'une entité.



La *Politique de Sécurité des Systèmes d'Information (PSSI)* de la direction de l'administration pénitentiaire (DAP) [MJ-DAP-PSSI-GEN] [RI.00], constitue le document maître du référentiel de sécurité des systèmes d'information de la DAP, construite sur la structure de la PSSI de l'Etat [PSSI-E] [RRG.11] et complète la *Politique Ministérielle de Sécurité Numérique* (PMSN) du ministère de la justice [MJ-PMSN] [RRS.05], afin de formaliser les exigences de sécurité spécifiques à la DAP. La PMSN reste cependant le socle de base commun à l'ensemble du ministère de la justice et aucune exigence de la présente politique ne pourra être de niveau inférieur à celles de la PMSN.

La présente *Politique de Sécurité des Systèmes d'Information de Sûreté, de la gestion technique bâtiminaire (GTB) et de la Gestion technique centralisée (GTC)* de la direction de l'administration pénitentiaire (DAP) [MJ-DAP-PSSI-SUR] [RI.01], constitue le document maître du référentiel de sécurité de ces systèmes.

La *PSSI des SI métier de la DAP* [MJ-DAP-PSSI-SIM] [RI.19], constitue le document maître du référentiel de sécurité de ces systèmes d'information métiers.

La *PSSI de la bureautique de la DAP* [MJ-DAP-PSSI-BUR] [RI.18], constitue le document maître du référentiel de sécurité de ces systèmes d'information bureautiques.

La présente politique [MJ-DAP-PSSI-SUR] est déclinée de la [MJ-DAP-PSSI-GEN] et l'objectif de ses exigences est triple :

- Elle constitue un cadre de référence et de cohérence qui sert à informer, mobiliser, conseiller, éclairer, conduire à la mise en œuvre de dispositifs, procédures, moyens de sécurité garantissant un niveau de protection approprié au regard des activités de sûreté de la direction de l'administration pénitentiaire et adaptées à chaque structure et systèmes ;
- Elle sert de base à la construction d'un référentiel d'audit permettant de s'assurer dans les faits et les procédures en place, de la conformité et de la bonne application de cette PSSI au sein de la direction de l'administration pénitentiaire ;
- Elle est incluse dans les documents de marché et doivent être respectées durant tout le cycle de vie des équipements numériques à chaque fois que cela est applicable.

Les PSSI issues de la présente politique [MJ-DAP-PSSI-SUR] permettent de contextualiser les exigences soit :

- En remplacement des exigences globales de la présente politique [MJ-DAP-PSSI-SUR] ;
- En intégrant des exigences restreintes supplémentaires lié au contexte particulier du système concerné.

Le SI de sûreté regroupe en particulier :

- les services support des activités de contrôle d'accès et de détection d'intrusion ;
- les services support des activités de vidéoprotection.

Le SI GTC/GTB regroupe en particulier :

- les services support de la gestion technique et centralisé des bâtiments ;
- les services support de la sécurité incendie.

1.1.2 Périmètre d'application de la PSSI

La présente politique [MJ-DAP-PSSI-SUR] s'applique à tout l'écosystème du système d'information de Sûreté de la DAP, ce dernier étant décrit en détail dans le document *Écosystème de la DAP* [MJ-DAP-ECO] [RI.08].

Elle doit être observée et mise en œuvre par l'ensemble des personnes physiques ou morales intervenant dans ce SI, qu'il s'agisse des administrations de l'État et de leurs agents ou bien de tiers (partenaires, prestataires ou sous-traitants) et de leurs employés.

Dans le cadre de l'utilisation du système d'information de Sûreté de la DAP par des prestataires externes, il est entendu que les règles imposées par leur propre PSSI devront être cohérentes (donc *a minima* au même niveau) que les règles édictées par la présente politique [MJ-DAP-PSSI-SUR].

La présente politique [MJ-DAP-PSSI-SUR] s'applique à toutes les ressources matérielles, logicielles ou humaines, propres au SI de Sûreté de la DAP ou appartenant aux différents acteurs, qui :

- permettent de rendre les services fournis par le SI de Sûreté de la DAP ou y contribuent,
- permettent d'exploiter le SI de Sûreté de la DAP ou contribuent à son exploitation,
- manipulent des informations relatives au SI de Sûreté de la DAP, notamment d'exploitation, ou issues de la DAP.

La présente politique [MJ-DAP-PSSI-SUR] doit être diffusée à l'ensemble des personnes concernées ou devant ou souhaitant être informées de son contenu et de ses éventuelles évolutions.

1.1.3 Définition, rôles et responsabilités des acteurs

Le rôle et les missions des acteurs intervenant dans l'écosystème de la DAP sont précisément définis dans le *Référentiel des acteurs* [MJ-DAP-ACT] [RI.07]

En complément, l'organisation mise en place en matière de sécurité des systèmes d'information pour couvrir les objectifs de sécurité identifiés pour la DAP sont formalisés et détaillés dans la *note organisationnelle en matière de SSI* [MJ-DAP-ORG-SSI] [RI.20].

La formalisation de cette organisation est indispensable pour que chaque acteur puisse mettre en œuvre ses responsabilités face aux enjeux de sécurité.

L'ensemble des acteurs est tenu d'appliquer et faire appliquer la présente PSSI sur son périmètre de responsabilité.

1.2 Entrée en vigueur

Cette nouvelle version de PSSI sûreté annule et remplace les versions précédentes des PSSI de 2016 ainsi que les LDSSI de 2010.

La présente politique entre en vigueur le jour de sa publication. Les entités internes de la DAP et les prestataires partie prenante du SI de Sûreté doivent s'y conformer.

Les prestataires disposent d'un délai maximum de 3 mois pour mettre à jour leurs déclarations de conformité visant l'application des règles nouvellement introduites ou mises à jour. Ce délai court à compter de la date de transmission du présent document vers eux.

En application de l'arrêté sectoriel portant application a Loi de programmation militaire de 2013, les prestataires se rapprochent du RCSSI de la DAP pour connaître le délai maximum de mise en conformité avec la présente politique.

La mise en conformité des prestataires et fournisseurs avec les règles nouvellement introduites ou mises à jour par la présente politique sera intégrée au pilotage de chacun des marchés concernés dans un délai maximum de 6 mois à compter de la date de transmission du présent document vers eux.

Un comité de suivi sera mis en place avec le RCSSI de la DAP, dont le but sera notamment de :

- Identifier les écarts majeurs entre les PSSI du bénéficiaire concerné et de la DAP ;
- Arbitrer les choix d'alignement considérés en tenant compte des impacts sur les activités ainsi que des moyens financiers et humains à mettre en œuvre ;
- Établir un calendrier de mise en conformité indiquant les mesures à prendre dans l'immédiat puis à moyen et à long terme ;
- Assurer le suivi du plan d'actions co-construit.

La présente PSSI-DAP-SUR doit être diffusée par le RCSSI de la DAP à l'ensemble des personnes concernées devant ou souhaitant être informées de son contenu et de ses éventuelles évolutions.

1.3 Pilotage et évolutions de la présente politique [PSSI-DAP-SUR]

La présente politique [MJ-DAP-PSSI-SUR] est amenée à évoluer dans le temps. Elle pourra notamment être revue afin de prendre en compte :

- les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'inspections ;
- les évolutions de la *Politique Ministérielle de Sécurité Numérique (PMSN)* [MJ-PMSN] [RRS.05] ;
- les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

Toute révision de l'analyse de risques ou de l'état de la menace, conduite par le RCSSI de la DAP, à son initiative ou sur décision de l'autorité d'homologation, entraîne automatiquement la révision de la présente PSSI. À cette fin, le RCSSI de la DAP anime les groupes de travail SSI de consultation puis de validation, sous responsabilité de l'AQSSI de la DAP.

Afin de garantir le traitement de la SSI et dans un cycle cohérent d'amélioration et de contrôle permanents, la DAP applique la norme ISO/IEC 27002:2022 relative aux mesures de sécurité de l'information [ISO27002:2022] [RD.10] qui fournit un modèle visant à définir, mettre en œuvre, exploiter, surveiller, mettre à jour et assurer le maintien en condition opérationnelle d'un système de gestion de la sécurité des systèmes d'information, ainsi que la norme [ISO27002:2022] [RD.10] qui décrit les bonnes pratiques en matière de SSI.

1.4 Suivi et contrôle de l'application de la PSSI

Le RCSSI de la DAP est garant de la bonne application de la présente PSSI sur l'ensemble du périmètre considéré, en s'appuyant sur les RSSI des prestataires externes pour leurs périmètres de responsabilité respectifs, ainsi que sur la chaîne des RISSI pour le périmètre interne de la DAP. En cas de non-respect de la présente PSSI, le RCSSI de la DAP peut prendre, ou faire prendre, en concertation avec les tiers concernés, toute mesure visant à garantir la sécurité de l'ensemble du réseau de la DAP.

Les RSSI des prestataires externes contrôlent et garantissent la bonne application de la présente PSSI-DAP-SUR sur le périmètre dont ils ont la charge par tous les moyens techniques ou humains à leur disposition. Ils contrôlent et garantissent également la bonne application de la présente PSSI-DAP-SUR sur leurs sous-traitants. Le RCSSI de la DAP, sur son initiative ou sur demande du GT SSI, peut demander aux RSSI des prestataires externes concernés de justifier de la bonne application de la présente PSSI-DAP-SUR sur tout leur périmètre.

Partie 2 Enjeux et Objectifs

2.1 Contexte et Contraintes

2.1.1 Contexte général

La Direction de l'Administration Pénitentiaire (DAP) utilise des locaux et bâtiments très différenciés, depuis les établissements pénitentiaires (EP) et les services pénitentiaires d'insertion et de probation (SPIP), jusqu'aux établissements ouverts accueillant du public : locaux SPIP, bâtiments administratifs de l'AC et des DISP et leurs satellites (ERIS, ARPEJ, PREJ, base cynophile, DAI externalisé, ENAP).

Ces bâtiments peuvent lui appartenir en propre, comme la majorité des établissements pénitentiaires, ou être loués, comme certains bâtiments administratifs et SPIP, être mis à disposition comme les UHSI, les UHSA, ou bien même relever de la gestion déléguée (GD) ou d'un Partenariat Public Privé (PPP) comme les nouveaux établissements livrés. En cas de GD, celle-ci assure des prestations d'entretien et de maintenance des locaux et des équipements (incluant le cas échéant les SI de sûreté) ainsi que la fourniture des fluides et des énergies.

La DAP délègue la gestion de tout ou partie de son SI de sûreté (en tant que MOE), à un ou plusieurs prestataires, dont les systèmes et services ont été préalablement homologués, conformément au cadre de l'*Arrêté du 23 décembre 2021 fixant les règles de sécurité et modalités de déclaration des SIIV et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Activités judiciaires »* [Arr-SAIVAJ] [RL.01].

L'ensemble des exigences applicables sont détaillées dans le présent document.

Enfin, concernant le cadre particulier des systèmes de Placement sous Surveillance Électronique (PSE) fixe ou mobile, la MOE de la solution technique (bracelets, bornes, systèmes de supervision) est totalement externalisée auprès de prestataires externes.

2.1.2 Personnel concerné par l'application des PSSI

Les exigences des PSSI s'adressent à tout acteur, interne ou externe à la DAP, qui intervient sur les SI de la DAP (action d'administration, d'exploitation ou simple utilisation des ressources mises à disposition).

Les conventions de services au sein de l'administration, les contrats passés avec les tiers, précisent les obligations des parties en la matière et sont soumises au programme d'audit de sécurité de la DAP.

L'organisation des délégations au sein de la chaîne SSI est soumis à l'arbitrage du Directeur de l'Administration Pénitentiaire.

L'ensemble des exigences applicables sont détaillées dans le présent document.

2.1.3 Gestion du risque

Sous l'autorité du RCSSI de la direction de l'administration pénitentiaire, les services de la DAP évaluent et traitent les risques qui pèsent sur les activités (missions, fonction, image, réputation, processus métiers, financier) et les actifs (matériel, systèmes logiciels, informations importantes pour l'organisation) qui leur sont confiés.

Une analyse des risques est réalisée ou actualisée a minima tous les 3 ans sous l'autorité du RCSSI de la direction de l'administration pénitentiaire. La méthode EBIOS Risk Manager est utilisée.

L'acceptation des risques se fait au travers de l'acceptation des risques résiduels par l'AQSSI.

2.1.4 Structure documentaire de la présente politique

La présente politique **[MJ-DAP-PSSI-SUR] [RI.01]** décline l'organisation de la sécurité au travers d'exigences de sécurité, claires et précises sur un ensemble de thèmes de sécurité structuré en conformité avec la norme **[ISO27002:2022] [RD.10]**. Ces exigences sont détaillées dans les chapitres qui suivent.

La présente politique constitue le document maître du référentiel sécurité composée de 6 types de documents :

- le présent document **[MJ-DAP-PSSI-SUR] [RI.01]** ;
- la *PSSI infrastructure liés aux systèmes de sûreté* (ex : cœur de réseau, commutateurs d'accès, système de virtualisation, etc.) **[MJ-DAP-PSSI-INF] [RI.02]**;
- la *PSSI spécifique liés aux systèmes de sûreté* (infrastructure, vidéo-surveillance, contrôle d'accès, etc.) **[MJ-DAP-PSSI-SPC] [RI.03]**;
- un *Corpus documentaire* **[MJ-DAP-REF] [RI.04]** contenant les textes de références associés aux PSSI. Les textes de références internes en vigueur correspondent aux dernières versions publiées pour les référentiels externes et aux dernières versions validées par la DAP pour les référentiels internes ;
- un *Glossaire* **[MJ-DAP-GLO] [RI.05]** ;
- un *RACI* précisant les rôles de chaque acteur présent dans les exigences **[MJ-DAP-RACI] [RI.06]** ;
- un document *Acteurs* **[MJ-DAP-ACT] [RI.07]**, précisant les rôles et responsabilités de chaque entité dans la sécurité du SI ;
- les documents de spécification et de conception des systèmes d'information, non spécifiquement dédiés à la SSI.

Cette politique est complétée par des « documents d'application » opérationnels : d'architecture, d'exploitation et de maintenance des systèmes d'information.

Ces documents comprennent des procédures d'exploitation sécurisées.

2.1.5 Intégration de la présente politique dans EBIOS RM

La présente PSSI **[MJ-DAP-PSSI-SUR] [RI.01]** s'inscrit également dans la démarche « *EBIOS Risk Manager* » **[EBIOS-RM] [RD.03]** portée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Dans ce cadre, elle alimente plus particulièrement l'**Atelier 1 : Cadrage et socle de sécurité**, car elles constituent la composante principale du socle de sécurité des systèmes d'information applicable à la DAP.

2.2 Objectifs de sécurité

2.2.1 Mesures de sécurité

Les mesures de sécurité définies sont issues de l'analyse de risques réalisée sur le périmètre de la direction de l'administration pénitentiaire et de ses activités essentielles.

2.2.2 Métriques utilisées dans les analyses de risques

Les métriques applicables aux analyses de risques des systèmes d'information de la DAP sont décrites dans le *Référentiel applicable à la DAP dans le cadre de la détermination des risques* **[MJ-DAP-RSK] [RI.58]**.

2.2.3 Métriques utilisées dans les analyses d'impact sur la protection des données (AIPD)

Les métriques applicables aux études d'impacts sur la vie privée des traitements de la DAP sont décrites dans le *Référentiel applicable à la DAP dans le cadre de la détermination des risques* **[MJ-DAP-RSK] [RI.58]**.

2.2.4 Nomenclature des exigences de sécurité

Les exigences de sécurité sont basées sur les 114 mesures de la version (2013) de la norme ISO27002 [ISO27002:2013] et ont ainsi été réparties selon les 14 domaines de celle-ci. Une nouvelle version de cette norme a été publiée en 2022 [ISO27002:2022] [RD.10]

Chacune des exigences de sécurité définies est construite de manière à être unique, et afin la lecture de sa référence permette une compréhension naturelle sans obligation de se reporter systématiquement à la description littérale. La nomenclature respecte le modèle suivant :

[trigramme domaine]-[quadrigramme de la notion]-[trigramme optionnel de précision]

p.ex. :

- GDA-RESP-SIS : pour la responsabilité des SI de sûreté
- GDA-INVT : pour l'obligation concernant les inventaires des biens

Domaine	Trigramme	Nomenclature
Sécurité des ressources humaines	SRH	SRH-xxxx
Gestion des actifs	GDA	GDA-xxxx
Contrôle d'accès	CAC	CAC-xxxx
Cryptographie	CRY	CRY-xxxx
Sécurité physique et environnementale	PHY	PHY-xxxx
Sécurité liée à l'exploitation	EXP	EXP-xxxx
Sécurité des communications	RSX	RSX-xxxx
Acquisition	ACQ	ACQ-xxxx
Développement et entretien des systèmes d'information	DEV	DEV-xxxx
Relations avec les fournisseurs	FOU	FOU-xxxx
Gestion des incidents de sécurité de l'information	GDI	GDI-xxxx
Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	GCA	GCA-xxxx
Conformité	CNF	CNF-xxxx




Il est à noter que « XXX » représente la numérotation de l'exigence, symbolisée par une série de trois chiffres. La numérotation peut inclure volontairement des « trous » afin de pouvoir insérer de nouvelles exigences sans avoir à renuméroter les anciennes.

2.2.5 Déclinaison de la PSSI Générale dans chaque système d'information de sûreté sur chaque site pénitentiaire

La plupart des exigences décrites dans la PSSI générale **[MJ-DAP-PSSI-GEN]** sont directement applicables dans chaque projet et système d'information de sûreté. Elles constituent ainsi le cahier des charges SSI général destiné à assurer un socle minimal en matière de sécurité numérique. En fonction des besoins de sécurité du SI qui sera à homologuer, il pourra être nécessaire de rédiger une PSSI spécifique si les besoins de sécurité sont plus contraignants sur ce périmètre.

Dans l'attente de la transposition des exigences de **[ISO27002:2013]** vers **[ISO27002:2022]** et de l'acquisition d'un outil de Gouvernance des Risques et de la Conformité (GRC), deux emplacements pour les références correspondantes ont été aménagées dans la cartouche de chaque exigence.

Ces exigences sont formalisées dans des cartouches au modèle suivant :

XXX-XXXX : Titre de l'exigence	
Réf. GRC :	ISO27002:2022 :
  	Descriptif de l'exigence globale applicable à tout système d'information de sûreté de la DAP.

DAP 

Prestataire 

DAP et Prestataire 

Les exigences applicables au prestataire portent sur son SI ainsi que sur celui de la DAP pour lequel il est missionné.

Dans les cas où aucun outil de Gouvernance, Risque et Conformité (GRC) n'est mis en œuvre ou que l'outil de GRC, mentionner « non implémenté », et si l'outil ne comporte pas de référence correspondante mentionner « non référencé ».

Le RACI annexé à cette PSSI précise de façon détaillée toutes les parties prenantes de la DAP concernées par l'exigence ainsi que leur niveau de participation (réalise, approuve, contribue, informé).

Le terme Prestataire désigne tous les acteurs hors DAP internes ou externes au ministère (fournisseur, SNUM, DIT, APIJ...), quel que soit leur rang de sous-traitance.

Certaines exigences peuvent faire mention d'un niveau de sécurité exigible dans un ou plusieurs des critères DICT, respectant la nomenclature suivante :

- **Disponibilité** : D1 (Arrêtable), D2 (Prioritaire), D3 (Urgent) et D4 (Immédiat) ;
- **Intégrité** : I1 (Altérable), I2 (Délectable), I3 (Corrignible) et I4 (Inaltérable) ;
- **Confidentialité** : C1 (Publique), C2 (Interne), C3 (Sensible) et C4 (Confidentiel) ;
- **Traçabilité** : T1 (Minimale), T2 (Structurée), T3 (Authentifiée) et T4 (Probante).

L'explicitation des niveaux de sécurité associés à ces mentions est décrite dans le *Référentiel* **[MJ-DAP-RSK] [RI.58]**.

Partie 3 Règles de sécurité

3.1 Gestion des biens

3.1.1 Responsabilités relatives aux biens




3.1.1.1 Règles générales




GDA001 : Responsable de la cybersécurité des systèmes d'information de sûreté		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> La cybersécurité de tout système d'information de sûreté est placée sous la responsabilité du RCSSI.

GDA002 : Responsable de la cybersécurité du réseau national de sûreté		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> La cybersécurité du réseau d'interconnexion de sûreté (RIS) est placée sous la responsabilité du RCSSI.

3.1.1.2 Inventaire des actifs

GDA011 : Cartographie des SI de sûreté	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <div></div> <div></div> <div></div> </div>	<p>Chaque SI de sûreté, qu'il apporte un service métier ou d'infrastructure, doit faire l'objet d'une cartographie, à sa conception, et à chaque mise à jour ultérieure, se conformant aux bonnes pratiques du <i>Guide de la cartographie du SI de l'ANSSI</i> [ANSSI-G-CARTO] [RD.04].</p> <p>Elle est soumise à validation de la DAP et est formalisée pour tout ou partie dans un dossier d'architecture technique (DAT).</p> <p>Les éléments de cartographie à fournir au RCSSI sont <i>a minima</i> les suivants :</p> <ul style="list-style-type: none"> • la liste des ressources matérielles ou virtualisées ; • les noms et les fonctions des applications, supportant les activités de l'opérateur, installées sur le SI ; • pour les systèmes, les équipements et les applicatifs utilisés au sein de l'administration pénitentiaire, un inventaire doit être tenu par l'exploitant qui doit préciser au minimum : Les versions des documents, des actifs systèmes, des logiciels et des Progiciels ; • le cas échéant, les plages d'adresses IP de sortie du SI vers internet ou un réseau tiers, ou accessibles depuis ces réseaux ; • le cas échéant, les plages d'adresses IP associées aux différents sous-réseaux composant le SI ; • la description fonctionnelle et les lieux d'installation du SI et de ses différents sous-réseaux ; • la description fonctionnelle des points d'interconnexion du SI et de ses différents sous-réseaux avec des réseaux tiers, notamment la description des équipements et des fonctions de filtrage et de protection mis en œuvre au niveau de ces interconnexions ; • la matrice des flux réseau autorisés en précisant : <ul style="list-style-type: none"> - leur description technique (sources, destinations, services, protocoles et ports) ; - la justification métier ou d'infrastructure ; - le cas échéant, lorsque des services, protocoles ou ports réputés non sûrs sont utilisés, les mesures compensatoires mises en place, dans la logique de défense en profondeur. • l'inventaire et l'architecture des dispositifs d'administration du SI permettant de réaliser notamment les opérations d'installation à distance, de mise à jour, de supervision, de gestion des configurations, d'authentification ainsi que de gestion des comptes et des droits d'accès ; • la liste des comptes disposant de droits d'accès privilégiés (appelés « comptes privilégiés ») au SI. Cette liste précise pour chaque compte le niveau et le périmètre des droits d'accès associés, notamment les comptes sur lesquels portent ces droits (comptes d'utilisateurs, comptes de processus, etc.) ; • l'inventaire, l'architecture et le positionnement des services de résolution de noms d'hôte, de relais internet et d'accès distant mis en œuvre par le SI ; • la prise en compte des recommandations de la DAP au travers des exigences et objectifs de sécurité de l'application ; • les procédures d'exploitation, décrites plus en détail dans le chapitre « Gestion de l'exploitation et de la maintenance ».


GDA012 : Revue de la cartographie des SI de sûreté	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	Un contrôle annuel de l'inventaire des actifs doit être réalisé pour chacun des SI afin de s'assurer de la complétude de la cartographie.

GDA013 : Capitalisation et gestion documentaire	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Un processus de gestion documentaire conforme à la norme [ISO27002:2022] [RD.10] doit être mis en place permettant la remontée des documents et bonnes pratiques déployées au niveau local.</p> <p>Cette gestion centralisée doit consolider les remontées et réintégrer les bonnes pratiques dans les processus opérationnels à l'échelle nationale.</p> <p>La mission de contrôle interne (MCI) de la DAP doit récupérer les différents documents et bonnes pratiques a minima tous les trois ans à des fins d'évaluation par la chaine SSI.</p>


3.1.2 Protection des informations


3.1.2.1 Sensibilité des informations

GDA021 : Sensibilité des données de sûreté de la DAP et moyens de protection associés	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> </div> <p>Les données de l'Administration Pénitentiaire doivent être manipulées en respectant l'instruction IGI1300 [IGI1300] [RRG.02] qui définit les notions de sensibilités des informations.</p> <p>Le niveau de sensibilité est lié aux impacts d'une éventuelle divulgation non autorisée des informations à la cible de la diffusion, il peut être assujéti des mentions suivantes :</p> <ul style="list-style-type: none"> - Diffusion Restreinte (DR) : impose à l'utilisateur d'être discret dans la gestion des informations non classifiées couvertes par cette mention, l'information concernée pouvant porter atteinte au secret de la défense nationale et à la sécurité des systèmes d'information de l'Administration Pénitentiaire - <u>Spécial France (SF)</u> : les informations marquées SF, classifiées ou non, ne peuvent être transmises qu'à des personnes physiques ayant la nationalité française ou à des personnes morales établies en France ayant le besoin d'en connaître <p><u>Donnée sensible</u> : Certaines informations de l'Administration Pénitentiaire (exemple : données à caractère personnel), sans être protégées par la mention de protection Diffusion Restreinte, peuvent néanmoins revêtir un caractère sensible. Une information ou un support sensible est une information ou un support non classifié ou non protégé par la mention de protection Diffusion Restreinte mais qui pourrait nuire à l'image ou aux intérêts des services de l'Administration Pénitentiaire, des organismes placés sous son autorité, sous sa tutelle ou liés par contrat ou convention.</p> <p>Les données de sûreté de l'Administration Pénitentiaire sont à considérer par défaut de niveau <u>Diffusion Restreinte</u>, au regard du <i>Code des relations entre le public et l'administration</i> [RGS] [RRG.01]. À ce titre les outils de protection de leur stockage et de leur diffusion doivent être adaptés à l'utilisation de cette mention. Cette dernière doit par ailleurs être explicitement apposée dans le document ainsi que dans le nom du fichier. Sans mention explicite sur le livrable comportant la donnée, on considèrera ce livrable comme non protégé (NP).</p> <p>Un <i>Catalogue des catégories de données sensibles</i> [DAP-CAT-DATA] [RI.12] doit être créé en fonction du type document (documentation projet, disques durs de stockage, supports de stockage externe, etc.) en précisant pour chaque catégorie le niveau de classification et les éventuelles mentions associées conformément à l'instruction IGI1300 [IGI1300] [RRG.02]. Ce catalogue doit également définir le type de marquage approprié pour chaque information conformément à la <i>Procédure de marquage</i> [DAP-MARQ-DOC] [RI.14]</p> <p>Seul le propriétaire d'une donnée décide du niveau de sensibilité associé. De fait, il est le seul décisionnaire pour changer ce niveau (suppression de la mention DR, ajouter une mention SF...), classer l'information sur la base de son appréciation du risque porté par la divulgation, l'altération ou la destruction de cette donnée. Le catalogue mentionné <i>supra</i> est un guide à l'appréciation du niveau de sensibilité, qui reste <i>in fine</i> une décision du propriétaire de la donnée.</p> <p>En cas de doute sur le niveau de sensibilité de la donnée et/ou du moyen de transmission à lui associer, il doit solliciter l'officier de sécurité SSI de la DAP.</p> <p>Tout agent ou personnel d'un prestataire qui constaterait un défaut dans le respect des exigences de protection ou de diffusion d'une donnée sensible doit sans délai remonter le problème au plus proche représentant de la chaîne de sécurité ou de la chaîne SSI.</p>	

GDA025 : Recensement des besoins de sécurité des données des SI de sûreté	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>La classification DICT permet de mettre en place un niveau de sécurité adapté à la sensibilité de l'information/ressource considérée par rapport aux 4 besoins de sécurité de l'information :</p> <ul style="list-style-type: none"> • Disponibilité ; • Intégrité ; • Confidentialité ; • Traçabilité. <p>L'échelle utilisée est décrite dans la <i>Grille de métrique SSI de la DAP</i> [DAP-METR-SSI] [RI.58].</p> <p>Pour chaque système d'information, un responsable du traitement est désigné par la DAP. Ce dernier doit :</p> <ul style="list-style-type: none"> • énumérer toutes les données et ressources traitées par le SI ; • établir le niveau de sensibilité des données selon les critères DICT ; • définir les durées de conservation et d'archivage. <p>Les éléments définis ci-dessus doivent en particulier être présents dans le dossier d'architecture technique (DAT) du SI.</p>

3.1.2.2 Utilisation des actifs

GDA031 : Provenance des postes de maintenance et d'intervention	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les postes de maintenance et d'intervention des systèmes de sûreté doivent être dédiés et approuvés par la DAP.</p>

GDA032 : Utilisation des moyens et ressources informatiques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les moyens et ressources informatiques (poste de travail, accès, périphériques) mis à disposition des agents ou prestataires ne doivent pas être utilisés à des fins non autorisées.</p> <p>Un poste de travail ne doit jamais être utilisé à d'autres fins que celles pour lesquelles il est prévu comme indiqué dans la <i>Charte informatique</i> [DAP-CHART-INFO] [RI.78].</p>



GDA033 : Usage des postes administrateurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Un poste d'administration ne doit être utilisé qu'à des fins d'administration.

GDA034 : Utilisation des équipements personnels	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	L'utilisation d'équipements personnels (BYOD pour « <i>Bring Your Own Device</i> ») pour traiter des données de la DAP ou exercer des activités au profit de la DAP est interdite.

3.1.2.3 Restitution des actifs

GDA041 : Procédure de restitution des postes d'administration et de maintenance	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>La DAP doit documenter et mettre en œuvre une <i>Procédure de remise et restitution du matériel</i> [DAP-REST-MAT] [RI.43], permettant de s'assurer que chaque personne impliquée dans la fourniture du service restitue l'ensemble des actifs en sa possession à la fin de sa période d'emploi ou de son contrat.</p> <p>Cette procédure devra prendre en compte le cas où les postes sont mutualisés (pas de restitution) et individuels (restitution).</p> <p>Chaque restitution de matériels et d'équipements doit être sanctionnée dans un PV instancié sur la base du modèle [DAP-PVR-ACTIF] [RM.01].</p> <p>Dans tous les cas, la procédure doit inclure une suppression des données personnels (profil, documents) de l'utilisateur.</p>

3.1.3 Manipulation des supports





GDA051 : Transfert des informations hors de la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Il est interdit de sortir des informations issues des systèmes d'information de la DAP, des matériels ou des logiciels hors de l'administration pénitentiaire sans autorisation préalable et sans justification d'un besoin de service.</p> <p>Cela comprend les informations sous toutes leurs formes (électronique comme papier) et également tout matériel participant ou ayant participé au stockage comme au traitement d'informations au sein des systèmes d'information.</p> <p>Toute sortie d'information (de niveau Diffusion Restreinte ou supérieur) répondant à un besoin métier doit être documentée dans une procédure métier spécifique formalisée et validée par le RCSSI de la DAP. Cette procédure devra intégrer les mesures contre le piégeage durant le transport et le stockage du support.</p> <p>Dans le cas d'un fonctionnement dégradé, un processus dérogatoire doit être mis en place et validé par le RCSSI de la DAP. Les règles de marquage de données doivent être systématiquement respectées en suivant la <i>Procédure de marquage et de manipulation des documents</i> [DAP-MARQ-DOC] [RI.14].</p>
GDA052 : Entrée de matériel informatique sur un site de la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des agents de la DAP ou des prestataires peuvent entrer en établissement avec du matériel informatique en fonction des besoins de la mission qu'ils effectuent.</p> <p>La <i>Demande d'autorisation d'entrée du matériel informatique</i> [DAP-DDE-MAT] [RM.25] dans un établissement doit être transmise conjointement au chef d'établissement et à la chaîne SSI la plus proche, 48h avant l'intervention, sauf cas de force majeure, et validée par le chef d'établissement.</p> <p>La demande [DAP-DDE-MAT] [RM.25] doit permettre d'identifier les différents matériels nécessaires et leur numéro de série. Sauf exception, l'entrée du matériel par ces personnes ne doit pas contrevenir aux principes de sécurité fixés par les mesures de sécurité définies ci-après (désactivation des technologies sans fil, interdiction de pénétrer en zone de détention avec un support de stockage amovible informatique...).</p> <p>Le matériel devra être vérifié et le propriétaire sensibilisé par le CLSI ou à défaut par le responsable infrastructure de l'établissement. Le propriétaire se verra doter d'une autorisation datée du jour qui sera vérifiée par le poste de contrôle avant l'accès en détention.</p>

GDA053 : Sortie d'un support de stockage de la DAP		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Aucun support de stockage contenant des données de production n'est autorisé à quitter les locaux de la DAP sans accord explicite du RCSSI (ex : investigation sécurité), en dehors des cas prévus par la loi (par exemple : réquisition judiciaire).</p> <p>La sortie d'un support devra faire l'objet d'une procédure spécifique adaptée au contexte de la sortie du support.</p>	

GDA054 : Protection des supports de stockage		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Les supports doivent être contrôlés et protégés.</p> <p>L'objectif est d'empêcher la divulgation, la modification, le retrait ou la destruction non autorisée d'information(s) et/ou l'interruption du système d'information.</p>	




GDA055 : Gestion des ACSSI		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>La gestion des articles contrôlés de sécurité des systèmes d'information (ACSSI) doit respecter l'<i>instruction générale interministérielle IGI 1300</i> [IGI1300] [RRG.02].</p>	

GDA056 : Analyse des matériels de stockage amovibles		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Il est obligatoire de mettre en place un jeu de supports amovibles fourni par la DAP et dédié à son système d'information et d'interdire l'emploi d'autres supports non connus du système (principe d'enrôlement matériel).</p> <p>Tout support de stockage amovible doit être analysé par une station blanche maintenue en condition de sécurité avant d'être connecté à un SI de la DAP selon les règles définies par le document « <i>Profil de fonctionnalités et de sécurité - sas et station blanche</i> » de l'ANSSI [ANSSI-PFS-SAS-SB] [RD.05].</p> <p>Ces supports doivent être marqués selon la procédure [DAP-MARQ-SUP] [RI.77].</p>	

GDA057 : Pertes, vols ou perte d'intégrité de données ou de supports amovibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Toute perte ou tout vol d'un support de stockage amovible contenant ou ayant contenu tout ou partie d'informations relatives au système d'information doit être considéré comme un incident de sécurité dont les exigences de traitement sont exprimées dans le chapitre Gestion des incidents de sécurité de l'information.</p> <p>En cas de perte d'intégrité (des informations ou du support de stockage amovible), la <i>Procédure des gestion des éléments compromis</i> [DAP-GEST-COMPRO] [RI.23] devra être respectée.</p>
GDA058 : Effacement sécurisé des données	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Tout décommissionnement de support de stockage doit respecter la <i>Procédure de blanchissement et de destruction du matériel sécurisée</i> [DAP-DSTR-MAT] [RI.10].</p> <p>Il est obligatoire de rendre impossible toute récupération du contenu d'un support recyclable devant être sorti du SI de la DAP.</p>
GDA059 : Stockage physique sécurisé des supports amovibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Il est obligatoire d'assurer le stockage physique des supports amovibles dédiés au système d'information dans un environnement sécurisé (coffre-fort) et conforme aux spécifications du fabricant (pour la conservation optimale des données lors de mise sous séquestre).</p>
GDA060 : Contrôle de la durée de vie du support	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Il est obligatoire de contrôler la durée de vie du support permettant d'assurer la durée légale de conservation de certaines informations.</p> <p>Il est obligatoire de transférer les données d'un support proche de son obsolescence si les données ont une durée de conservation plus longue.</p> <p>La gestion du cycle de vie des supports est formalisée dans le être dans une procédure d'exploitation sécurité (PES).</p>

3.1.4 Ressources humaines

3.1.4.1 Éléments contractuels

SRH001 : Habilitation des candidats	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Toute personne amenée à manipuler des outils – logiciels, matériels – permettant d'obtenir des privilèges élevés aux systèmes d'information de la DAP, ou disposant des codes d'accès permettant d'obtenir ces privilèges, doit faire l'objet d'une procédure de contrôle élémentaire de son aptitude à la manipulation d'informations sensibles incluant les vérifications suivantes :</p> <ul style="list-style-type: none"> • Vérification du feuillet B2 du Casier Judiciaire du candidat pour les candidats de nationalité française ; • Vérification des antécédents concernant les candidats de nationalité étrangère, sous réserve de l'absence de restriction aux seuls nationaux.
SRH002 : Contractualisation des exigences d'habilitation	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Dans le cas de la manipulation ou de l'accès à des informations de niveau de confidentialité « Secret », un niveau d'habilitation « Secret » du candidat est un pré requis à la prise de fonction.</p> <p>Les contrats avec les prestataires externes doivent, en tant que besoin, traduire cette exigence par une clause contractuelle.</p>
SRH003 : Habilitation obligatoire dans les fiches de poste	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les postes proposés par la DAP nécessitant un niveau d'habilitation doivent obligatoirement inclure la mention relative à l'obligation d'être en conformité avec la réglementation sur la protection du secret de la défense nationale dans les fiches de poste.</p> <p>Cette exigence concerne les postes proposés aux agents titulaires (ex : en CAP) et non-titulaires (ex : via la BIEP).</p>










SRH004 : Gestion des habilitations		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>L'officier central de sécurité de la DAP suit la gestion des habilitations de défense du personnel sur la base du <i>Catalogue des emplois</i> [DAP-CAT-EMPL] [RI.39] conformément à la <i>Note organisationnelle de défense et de sécurité</i> [MJ-DAP-ORG-SSI] RI.20].</p> <p>Les officiers de sécurité des entreprises cotraitantes et sous-traitantes sont responsables des demandes et du respect des habilitations des personnels employés par les sous-traitants.</p> <p>Pour chaque prise de poste, ils doivent transmettre à l'officier de sécurité de la DAP un certificat de sécurité attestant de leur habilitation avant leur prise de poste.</p>	




SRH005 : Responsabilité des droits d'accès		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>Le RSSI ou toute personne désignée par le représentant légal des sociétés prestataires de la DAP est responsable du retrait et du réexamen des droits d'accès aux SI et aux locaux ainsi que de la restitution des biens (documents, équipements, supports amovibles, données...) au départ de son personnel ou en cas de changement de poste.</p>	




SRH006 : Responsabilité de la formation du personnel		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>Le RSSI ou toute personne désignée par le représentant légal à cet effet des sociétés prestataires de la DAP est responsable de la mise en place de la formation du personnel aux outils et aux méthodologies à mettre en œuvre pour être conforme aux PSSI de la DAP.</p> <p>La DAP se réserve le droit de réaliser des contrôles sur les formations délivrées en cas d'incident ou d'audit ponctuel.</p>	

SRH007 : Signalement du non-respect des règles SSI		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>Tout responsable est tenu de prendre les mesures nécessaires pour garantir la sécurité et l'intégrité du SI de la DAP.</p> <p>Le non-respect des règles SSI, quelle qu'en soit la cause (impossibilité technique, erreur, malveillance, incompatibilité avec les procédures ou l'organisation en vigueur) doit être signalé à la hiérarchie et au responsable SSI local, avec indication des mesures prises pour limiter les risques associés.</p>	




3.1.4.2 Arrivée du personnel et des prestataires




SRH010 : Sélection des candidats	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Une vérification doit être faite concernant les qualifications, les formations et les références professionnelles des candidats à l'emploi, sous-traitants et tiers utilisateurs, dans le respect de la législation, de la réglementation et de la déontologie et en fonction des besoins professionnels, de la classification des informations auxquelles l'accès doit être donné et des risques perçus.</p>
SRH011 : Procédure d'arrivée d'un agent ou d'un prestataire au sein de la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Il doit exister une <i>procédure RH</i> unique (administration centrale, DISP, établissement pénitentiaire...) orientée <i>système d'information d'arrivée des agents</i> au sein de la DAP [DAP-ARR-PRESTA] [RI.46] et des personnels de l'exploitant.</p> <p>La procédure implique la tenue d'un <i>modèle de dossier administratif</i> [DAP-DOSS-ADM] [RM.05].</p> <p>Chaque remise de matériels et d'équipements doit être sanctionnée dans un PV instancié sur la base du modèle [DAP-PVR-ACTIF] [RM.01].</p>
SRH012 : Création et mise à jour du dossier administratif agent	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Un <i>dossier administratif</i> contenant un volet SSI basé sur le <i>modèle</i> [DAP-DOSS-ADM] [RM.05] doit être mis en place par les services RH pour chaque agent ayant accès au SI de la DAP.</p> <p>Ce modèle doit notamment préciser :</p> <ul style="list-style-type: none"> • les différents SI auxquels la personne aura accès ; • les différents badges lui permettant d'accéder aux locaux nécessaires à sa mission; • les équipements informatiques et de télécommunication ; <p>dont il a besoin pour assurer sa mission.</p> <p>Ce dossier doit être maintenu à jour (changement de poste, départ, ajout d'un périmètre...).</p>




SRH013 : Création et mise à jour du dossier administratif prestataire	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Un <i>dossier administratif</i> dont le <i>modèle</i> est fourni par la DAP [DAP-DOSS-ADM] [RM.05] doit être mis en place par les sous-traitants pour chaque personnel employé ayant accès au SI de la DAP.</p> <p>Ce dossier doit être à jour (changement de poste, départ, ajout d'un périmètre...) et pourra être consulté à la demande par la DAP.</p>




SRH014 : Vérification du dossier administratif	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les services RH de la DAP doivent s'assurer de la conformité du <i>dossier administratif</i> [DAP-DOSS-ADM] [RM.05] pour chaque prise de poste, changement de poste ou départ d'un personnel employé (sous-traitant ou agent de la DAP).</p>




3.1.4.3 Rupture, terme ou modification du contrat de travail




SRH021 : Processus disciplinaire des agents	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Tout agent responsable d'une violation des obligations de sécurité énoncées par les règles SSI encourt un déferrement devant les instances disciplinaires.</p>




SRH022 : Processus disciplinaire de l'exploitant	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Le prestataire doit documenter et mettre en œuvre un processus disciplinaire applicable à l'ensemble des personnes impliquées dans la fourniture du service ayant enfreint la politique de sécurité.</p>

SRH030 : Cessation de l'activité de plus de 6 mois	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Toute personne ayant accès aux systèmes d'information de la DAP, agent ou exploitant, qui cesse son activité plus de 3 mois (congrés longue durée, fin de contrat, mobilité, etc.) se verra suspendre tous ses accès au maximum dans les 5 jours ouvrés suivant son départ.</p> <p>Dans cette hypothèse, l'exploitant a l'obligation d'en informer la DAP sans délai.</p> <p>La demande de réactivation du compte doit survenir dans un délai de prévenance de 5 jours ouvrés avant le retour du personnel.</p>










SRH031 : Suppression des droits d'accès	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les droits d'accès de l'ensemble des utilisateurs au SI doivent être supprimés par la DAP sans délais à la fin de leur période d'emploi ou modifiés en cas de changement de contrat/fonction.</p>

SRH032 : Désactivation des comptes	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les comptes systèmes et applicatifs doivent être désactivés dès le départ ou la suspension d'un administrateur/utilisateur des systèmes d'information ; puis ces comptes doivent être supprimés sous un délai de 6 mois.</p> <p>Dans le cas de la connaissance de mots de passe partagés, ces codes doivent impérativement être renouvelés sans délai.</p>

SRH033 : Procédure RH de départ d'un agent de la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Tout départ d'un agent à la DAP doit se faire conformément à la procédure [DAP-ARR-PRESTA] [RI.46], permettant de s'assurer de la restitution effective des biens et équipements appartenant à la DAP (badge, téléphone portable, ordinateur, PDA, supports de stockage, etc.).</p> <p>Chaque restitution de matériels et d'équipements doit être sanctionnée dans un PV instancié sur la base du modèle [DAP-PVR-ACTIF] [RM.01] et doit être conservée pour une durée de 5 ans.</p>

SRH034 : Procédure RH de départ d'un prestataire	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Tout départ d'un personnel d'un prestataire doit se faire conformément à la procédure [DAP-ARR-PRESTA] [RI.46], permettant de s'assurer de la restitution effective des biens et équipements appartenant à la DAP (badge, téléphone portable, ordinateur, PDA, supports de stockage, etc.).</p> <p>Chaque restitution de matériels et d'équipements doit être sanctionnée dans un PV instancié sur la base du modèle [DAP-PVR-ACTIF] [RM.01]. Une copie est remise au chef d'établissement et une autre à la DISP qui devront la conserver pour une durée de 5 ans.</p>

3.1.4.4 Sensibilisation et formation

SRH041 : Contenus des plans de sensibilisation et formation des agents	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	Le <i>plan de formation et de sensibilisation des agents</i> de la DAP est formalisé dans le livrable [DAP-FORM-SENSI] [RI.75] et son annexe [DAP-CAL-SENSI] [RI.75.1]
SRH042 : Contenus des plans de sensibilisation et formation des prestataires	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Le RCSSI de la DAP partage au RSSI du prestataire ses plans internes pour qu'il puisse l'enrichir.</p> <p>Le RCSSI du prestataire doit valider formellement les plans et les présenter à un représentant du RCSSI de la DAP tous les ans.</p> <p>Le RCSSI de la DAP peut demander des modifications de ces plans si nécessaire.</p>
SRH043 : Mise en œuvre des plans de sensibilisation et formation	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>La DAP et les sociétés prestataires doivent élaborer et mettre en œuvre des plans de sensibilisation et de formation du personnel à la sécurité des systèmes d'information et des mesures de sécurité associées.</p> <p>Ces plans doivent s'appuyer sur des programmes définis par la DAP et tenant compte de l'évolution de l'état de la menace afin d'intégrer la SSI dans le cycle de « vie » du personnel.</p> <p>Les programmes de formation doivent être différenciés en fonction des missions et responsabilités des personnels. Ces séances de formation doivent être adaptée aux profils des personnels, au niveau de sensibilité des informations traitées, aux enjeux des activités et aux risques pesant sur les SI utilisés.</p> <p>Les personnels doivent être correctement formés et entraînés à l'installation et l'utilisation des nouveaux systèmes.</p>

SRH044 : Remise à niveau du personnel		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	Une remise à niveau du niveau de formation d'un agent de la DAP ou d'un sous-traitant doit être effectuée si nécessaire dès la prise de fonction.	

SRH045 : Fréquence des sessions de formation		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<div>Une formation continue sur l'utilisation des systèmes d'information doit être prodiguée :</div> <div><div><div></div><div></div><div></div></div><div><div><div></div><div></div><div></div></div></div><ul style="list-style-type: none">tous les trois ans ou à chaque modification du système d'information (mise à jour matérielle ou logicielle) impactant le métier pour les agents de la DAP utilisant ces systèmes ;tous les ans ou à chaque modification du système d'information (mise à jour matérielle ou logicielle) impactant le métier pour le personnel de l'exploitant utilisant ces systèmes.</div>	

SRH046 : Traçabilité des participations aux sessions de sensibilisation et de formation des agents		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	Chaque séance de sensibilisation ou de formation des agents doit être insérée dans l'outil de suivi des formations du SIRH de la DAP et doit-être mise à disposition de la SSI.	

SRH047 : Traçabilité des participations aux sessions de sensibilisation et de formation des prestataires		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<div>Le RSSI des sociétés prestataires doit assurer la la traçabilité des sessions de sensibilisation et du parcours de formation SSI de son personnel.</div> <div>Un état des lieux des formations du personnel du prestataire à la SSI doit être mis à disposition du RCSSI de la DAP sur demande.</div>	

SRH048 : Revue des participations aux sessions de sensibilisation et formation		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	Tous les 3 ans une revue des actions de sensibilisation et de formation doit être menée par le service des ressources humaines de la DAP.	

3.2 Sécurité physique et environnementale

3.2.1 Zones sécurisées




3.2.1.1 Périmètre de sécurité physique




La chaîne SSI de sûreté de la DAP doit s'assurer de la sécurité physique des informations et s'appuie sur ses représentants sur chaque site (RISSI et Officier locaux de sécurité) avec pour objectif de :










- restreindre aux seuls utilisateurs autorisés l'accès physique aux informations, aux équipements, au SI et à son environnement physique ;
- protéger les locaux et l'infrastructure support des SI ;
- fournir les services de support aux SI ;
- protéger les SI contre les risques environnementaux.

Les règles ci-dessous sont ainsi applicables à tout site, interne ou externe à la DAP, susceptible d'héberger tout ou partie de l'activité (ex : prestataires ou sous-traitant de la DAP, etc.) et plus particulièrement les ressources informatiques de la DAP)

3.2.1.2 Contrôles physiques des accès




PHY001 : Responsabilité des règles définissant les accès physiques aux sites et locaux	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	Les règles définissant les accès physiques aux sites et locaux sont sous la responsabilité du chef d'établissement selon le niveau de sensibilité des différentes zones définies par l'annexe sécurité du <i>guide programmatique immobilier</i> [DAP-GUI-IMMO] [RI.40] .




PHY002 : Responsabilité des équipements techniques et des locaux informatiques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	Tout équipement technique et tout local informatique hébergeant des équipements du SI de la DAP, que l'équipement ou le local soit sous responsabilité de la DAP ou d'un tiers (ex : prestataire) doit être affecté à un responsable explicitement identifié.

PHY003 : Gestion et procédure d'accès temporaire	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Chaque collaborateur de la DAP, interne ou externe, ne doit être en mesure d'accéder qu'aux seuls éléments du SI (locaux, points d'accès, ressources logiques ou physiques) nécessaires à l'accomplissement de sa mission afin de limiter les risques d'erreur et de malveillance. Ainsi les accès sont limités aux seules personnes habilitées ou temporairement autorisées par le chef d'établissement pour les besoins de service, avec une attention particulière pour l'attribution des accès temporaires (prestataires, maintenance, travaux, ménage, etc.).</p> <p>Une <i>procédure d'accès aux locaux techniques</i> [DAP-ACC-LOC] [RI.09] doit être mise en place comportant un délai de prévenance d'au moins 48H.</p> <p>Une <i>fiche détaillée d'intervention</i> avec le modèle [DAP-INTV-PRESTA] [RM.07] doit accompagner la demande.</p>
PHY004 : Protection des salles informatiques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les salles informatiques hébergeant les composants du SI, serveurs ou réseaux de la DAP, doivent être protégées en permanence contre tout accès illicite et contre les agressions extérieures. Les salles hébergeant les équipements d'alimentation et de distribution d'énergie (arrivée, répartiteur, câbles) doivent également être protégées contre tout accès illicite et contre les dégradations volontaires ou involontaires.</p> <p>Dans le cas où les salles sont accessibles par des tiers (détenus ou public), elles doivent être banalisées (absence de signalétique publique).</p>
PHY005 : Journalisation des accès	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Tout accès physique aux équipements du système de sûreté doit être signalé et accompagné par un responsable ou responsable par procuration des systèmes de sûreté.</p> <p>Ces mouvements doivent être journalisés (en entrée et en sortie), les personnes qui accèdent aux salles informatiques doivent être identifiées nominativement (par badge ou par clé de sûreté).</p> <p>Cette action doit avoir été validée en amont, par le biais d'une demande instanciée sur la base du modèle [DAP-DDE-LOC] [RM.09], définissant la raison de l'accès, les actions menées et la liste des intervenants avec leurs rôles, conformément à la procédure [DAP-ACC-LOC] [RI.09].</p>




3.2.1.4 Sécurisation des bureaux, des salles et des équipements




3.2.1.4.1 Règles générales

PHY011 : Sécurisation des locaux d'hébergement	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les sites destinés à héberger les données des systèmes d'information de la DAP doivent être surveillés 24 h/24 et 7 j/7.</p> <p>Les entités chargées d'opérer les systèmes d'information de la DAP ont l'obligation de mettre en œuvre un dispositif permettant de réserver l'accès aux locaux aux seules personnes autorisées.</p> <p>Ils doivent détailler tous les moyens mis en œuvre afin d'assurer la sécurité des locaux d'hébergement, notamment :</p> <ul style="list-style-type: none"> • les moyens de surveillance, dispositifs anti-intrusion dont les baies informatiques ; • les contrôles et enregistrements des accès (gardiennage, sas, moyen d'identification, etc.) ; • la protection physique des équipements (verrouillage des baies, etc.)


PHY012 : Dérogation pour l'utilisation de salles présentant des défauts de couverture des risques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Le RCSSI de la DAP peut autoriser l'utilisation de salles ne répondant pas à toutes les exigences énumérées ci-dessus.</p> <p>Les défauts de couverture aux risques identifiés doivent être précisés dans le document remis par le responsable désigné pour vérifier la conformité du site.</p>

3.2.1.4.2 Découpages en zones de sécurité

PHY020 : Localisation des locaux hébergeant des serveurs ou des équipements	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les locaux hébergeant des serveurs ou des équipements réseau ou télécom doivent se trouver dans une zone réservée.</p>


PHY021 : Référentiel du niveau de sécurité de chaque zone	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Chaque zone possède un niveau de sécurité décrit dans l'<i>annexe sécurité du guide programmatique immobilier</i> [DAP-GUI-IMMO] [RI.40].</p>


3.2.1.4.3 Exigences propres aux bureaux
















PHY030 : Utilisation des bureaux	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les bureaux doivent dans la mesure du possible ne pas héberger de ressources critiques ou sensibles (en privilégiant pour cela les infrastructures d'une salle informatique sécurisée, qu'elle soit locale, régionale ou nationale), et sinon appliquer des mesures de protection logiques (chiffrement, authentification renforcée) et physiques (contrôles d'accès) supplémentaires (validées par le RCSSI de la DAP (exemple : salle de crise).</p>

3.2.1.5 Exigences propres aux locaux techniques


3.2.1.5.1 Salles informatiques (informatique et téléphonie)

PHY040 : Utilisations de locaux dédiés	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Chaque local doit être dédié à la seule fonction de local technique informatique/téléphonie.</p>


PHY041 : Sécurisation des locaux situés hors enceinte d'un établissement fermé	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Si le local est situé hors enceinte d'un établissement fermé, les points d'accès à la salle doivent être vidéo-surveillés en permanence et l'issue de secours doit être pourvue d'une alarme d'ouverture.</p> <p>Le local doit être de préférence aveugle, la présence de fenêtres ou de murs vitrés nécessitant la mise en place de moyens de sécurisation complémentaires (opacification et grilles anti-intrusion).</p> <p>Le local doit disposer d'un dispositif de détection d'intrusion physique (détection de mouvements par infrarouge ou hyperfréquence) activé en dehors des périodes normales de travail et relié au poste permanent de surveillance pour le report d'alarme.</p> <p>Ces dispositifs d'alerte sont reliés à un poste de gardiennage interne ou externe (ex : PCI) permettant, en cas de déclenchement, l'intervention de personnels spécialisés, en toutes circonstances, en moins de 30 minutes.</p>


PHY042 : Installation des câbles de courant faible	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	La salle doit assurer le passage des câbles de courant faible, permettant de les soustraire à un éventuel dégât des eaux (inondations, défaut d'étanchéité, infiltrations, ruptures de canalisation, fuite de climatiseur) et dans le cas de salles sujettes à un risque identifié d'inondation, un dispositif de détection et un dispositif d'évacuation d'eau doivent être mis en place en complément conformément à l' <i>annexe sécurité du guide programmatique immobilier</i> [DAP-GUI-IMMO] [RI.40] .
PHY043 : Sécurité des installations électriques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	La salle doit être conforme aux normes de sécurité définies dans l' <i>annexe sécurité du guide programmatique immobilier</i> [DAP-GUI-IMMO] [RI.40] des installations électriques (notamment la mise à la terre) et disposer de dispositifs d'élimination de l'électricité statique (revêtement du sol, etc.), inondations et de lutte contre la foudre (parafoudres).
PHY044 : Climatisation des salles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	La salle doit être équipée d'un système de climatisation permettant de maintenir une température et une hygrométrie adéquates conformément à l' <i>annexe sécurité du guide programmatique immobilier</i> [DAP-GUI-IMMO] [RI.40] . Alternativement, l'installation d'une simple ventilation peut être envisagée pour les petites pièces aveugles dont la température reste fraîche toute l'année.
PHY045 : Protection contre les signaux parasites compromettants	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	Pour se protéger contre les signaux parasites compromettants l'installation d'une cage de Faraday ou la faradisation des locaux est requise conformément à l' <i>annexe sécurité du guide programmatique immobilier</i> [DAP-GUI-IMMO] [RI.40] .
PHY046 : Procédures réflexes de réaction en cas de sinistre	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	Des procédures réflexes de réaction en cas de sinistre spécifique au site, adaptées aux caractéristiques spécifiques des installations (système d'extinction incendie par gaz inerte, etc.) permettant aux personnels de gérer les situations d'urgence en heures ouvrées ou non ouvrées, doivent être formalisées, diffusées et affichées dans les salles concernées.

	Ces procédures sont testées a minima une fois par an et sont adossées aux plans de continuité d'activité (PCA) et de reprise d'activité (PRA) qui doivent traiter les risques de sinistres physiques et environnementaux.
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


PHY047 : Contrôles réguliers des composants du SI	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des contrôles réguliers des composants du SI doivent être réalisés pour garantir leur efficacité par les équipes responsables de l'équipement sur la base des fiches de contrôle présentes dans le classeur [RM.36].</p> <p>La révision des fiches de contrôles doit être réalisée tous les ans et tracée dans un PV instancié sur la base du modèle [DAP-PVC-EPI] [RM.08].</p> <p>Ces contrôles doivent conduire à un plan de remédiation instancié sur la base du modèle [DAP-REV-FCCS] [RM.06] transmis à la direction interrégionale (DISP) de ressort.</p> <p>Ce plan est consolidé au travers de toutes les fiches présentant des anomalies et suivi à fréquence a minima trimestrielle jusqu'à mise en œuvre de toutes les actions.</p>


3.2.1.5.2 Stockage des matières dangereuses dans les locaux techniques


PHY050 : Stockage des substances dangereuses ou combustibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Il est interdit de stocker des substances dangereuses ou combustibles ainsi que des objets de destruction sans protection (hache, pelle ...) dans (ou à proximité) d'une salle technique informatique.</p>

PHY051 : Stockage des fournitures	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Il est également interdit de stocker les fournitures en vrac, comme les cartons et les papiers, ou les matériels en attente d'évacuation ou de destruction dans (ou à proximité) de ces mêmes locaux.</p>


3.2.1.5.3 Fermeture des bureaux


PHY060 : Sécurisation des bureaux	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les bureaux doivent être sécurisés en fonction des informations qu'ils contiennent ou en fonction des informations auxquelles ils peuvent accéder, conformément aux prescriptions de l'<i>IGI1300</i> [IGI1300] [RRG.02].</p>

PHY061 : Prévention des dégâts des eaux des locaux	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des mesures de prévention des dégâts des eaux des locaux techniques et informatiques doivent être mis en œuvre, notamment :</p> <ul style="list-style-type: none"> en surélevant les équipements informatiques et de téléphonie d'au moins 15 cm par rapport au niveau du sol pour les salles informatiques situées en rez-de-chaussée ; en éloignant les équipements des installations d'eau qui risqueraient de se rompre ou de fuir (réseaux d'eau, climatiseur, radiateur...).

PHY062 : Maintenance des équipements de fonctionnement des services essentiels et de sécurité	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Il est obligatoire de préciser dans les contrats de maintenance des équipements de fonctionnement des services essentiels définis dans l'analyse de risque et de sécurité (extincteurs, climatisation, eau, détection de fumée et de chaleur, détection d'ouverture et d'effraction, groupe électrogène, ...) un délai d'intervention adapté en cas de défaillance, et les contrôler au moins une fois par an.</p>

3.2.1.6 Travail dans les zones sécurisées

PHY070 : Règles de contrôle d'accès aux bâtiments	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Le contrôle d'accès aux bâtiments hébergeant des ressources informatiques ou des points d'accès à ces ressources est régi par les dispositions spécifiques accessibles auprès de la chaîne sécurité défense de la DAP, sur le contrôle d'accès physique aux bâtiments.</p> <p>Dans le cas d'hébergement dans le bâtiment d'un tiers, les dispositions correspondantes de la PSSI de l'organisme tiers doivent être transmises à leur correspondant SSI au sein de la DAP (RCSSI, RISSI) pour validation sur leur conformité avec les exigences de la DAP explicitées dans le présent référentiel.</p>





PHY071 : Règles sur les principes du cloisonnement réseau s'appliquant aux SI	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des règles de cloisonnement réseau s'appliquent au sein des SI des zones sécurisées.</p> <p>Ainsi, un câblage réseau apparent entre deux équipements situés dans une même zone ne peut transiter par une zone moins sensible (par exemple devoir sortir de la zone sécurisée, pour des contraintes bâtimentaires ou autre).</p>


3.2.1.7 Zones de livraison et de chargement


Aucune exigence spécifique hormis l'application de la *politique* [MJ-PMSN] [RRS.05].


3.2.2 Matériels


3.2.2.1 Emplacement et protection du matériel

PHY080 : Protection lors du démarrage des postes utilisateurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Le démarrage des postes utilisateurs ou des serveurs ne doit pouvoir s'effectuer que sur des médias contrôlés, ce qui implique que le démarrage des machines à partir d'un CD/DVD, d'une clé USB ou du réseau (WoL) doit être impossible (à l'exception d'une opération de maintenance réalisée par un administrateur qualifié).</p> <p>La mise en œuvre de cette mesure nécessite la <i>protection de l'accès au BIOS</i> de l'ordinateur par un mot de passe, conformément à la procédure [DAP-PROT-BIOS] [RI.79].</p>
PHY081 : Exécution automatique de fichiers exécutables se trouvant sur un périphérique externe	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les ordinateurs ne doivent pas autoriser le lancement de l'exécution automatique de fichiers exécutables se trouvant sur un périphérique externe venant d'être connecté (typiquement via un port USB ou le lecteur CD/DVD).</p> <p>La fonction de démarrage automatique du média amovible doit être inhibée au niveau du système d'exploitation.</p>
PHY082 : Scellés de sécurité	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Dans le cas des postes situés en zone de détention, des <i>scellés de sécurité</i> doivent être posés pour garantir la non-ouverture du boîtier et le non-usage des ports de communication conformément à la <i>procédure</i> [DAP-PLAC-SCSEL] [RI.15].</p> <p>Les numéros des scellés de sécurité placés sur ces postes doivent être inventoriés au sein du <i>classeur de sécurité sur la base du modèle</i> [DAP-INV-SCSEL] [RM.10].</p> <p>L'ensemble des scellés ainsi posés doit être vérifié au minimum une fois par an par le CLSI de l'établissement. La vérification devra être inscrite dans le document d'<i>inventaire</i> [DAP-INV-SCSEL] [RM.10].</p>
PHY083 : Sensibilisation à la vérification des scellés	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les agents et le personnel de l'exploitant doivent être sensibilisés à la vérification régulière des scellés.</p>


PHY084 : Vérification de la conformité des éléments de configuration des équipements	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	Un outil de vérification régulière de la conformité des éléments de configuration des équipements doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.


PHY085 : Sécurisation des imprimantes et des copieurs multifonction	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	Les spécificités liées à la <i>sécurisation des imprimantes et des copieurs multifonction</i> doivent être formalisées dans la procédure [DAP-SECU-IMPR] [RI.69] qui est notamment basée sur les exigences de la <i>politique [MJ-PMSN] [RRS.05]</i> .


PHY086 : Protection des automates	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Tous les automates doivent être protégés conformément à leur niveau de sensibilité, quel que soit leur emplacement (hors ou à l'intérieur du RGI).</p> <p>Ces systèmes doivent être protégés contre les accès physiques non autorisés et contre les risques environnementaux (dégâts des eaux, températures de fonctionnement non adéquates, incendie...).</p>

PHY087 : Protection des ports USB	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	Les ports USB des stations de travail et serveurs hors de locaux techniques sécurisés doivent être protégés via un filtrage logique (ex : désactivation dans le BIOS, désactivation par l'OS, agent de filtrage de station blanche) ou un filtrage physique (carter, bloqueur de port USB) en fonction de l'analyse de risques du SI associé.


3.2.2.2 Sécurité du câblage

PHY090 : Règles définissant la sécurité du câblage	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	Le câblage réseau/téléphonique et/ou informatique doit respecter les exigences du <i>Guide de référence système de câblage [DAP-GUI-CABLE] [RI.38]</i> (normes, repérage, recette...)

PHY091 : Contrôle de l'installation par la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	La pose et le raccordement initiaux de ces équipements doivent être réalisés par l'intégrateur dans le cadre du projet d'implémentation mais sous couvert, contrôle et accord préalable de la DAP.

PHY092 : Séparation des éléments mutualisés	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	Dans les éléments devant être mutualisés comme les baies de brassage, des mesures de séparation explicites doivent être appliquées (marquage), tel le découpage en plusieurs parties de la baie sous forme de platines de brassage affectées à l'usage exclusif de chacune des entités devant partager l'infrastructure de câblage.

3.2.2.3 Inspection du matériel

PHY100 : Inspection physique du matériel	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Le matériel est inspecté régulièrement pour se prémunir de la pose éventuelle de dispositif d'écoute.</p> <p>L'organisation et la fréquence de ces <i>inspections</i> devra faire l'objet d'une <i>procédure spécifique</i> [DPA-INSP-MAT] [RI.55] validée par la DAP.</p>

3.2.2.4 Sécurité du matériel et des actifs hors des locaux

3.2.2.4.1 Mise au rebut, recyclage des matériels

PHY110 : Mise au rebut		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	La mise au rebut des supports doit respecter la procédure [DAP-DSTR-MAT] [RI.10] annexée à la <i>politique</i> [MJ-PMSN] [RRS.05] .	

3.2.2.4.2 Matériel utilisateur laissé sans surveillance

PHY120 : Verrouillage physique des postes de travail portables		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Les utilisateurs dotés d'un ordinateur portable doivent systématiquement l'attacher à un câble antivol lorsqu'ils arrivent à leur prise de poste. En cas d'absence prolongée, le poste devra être éteint et rangé dans un caisson fermé à clé.	

PHY121 : Verrouillage manuel des postes de travail		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Les utilisateurs doivent éteindre leur machine lorsqu'ils quittent leur poste en fin de journée ou pour une durée supérieure à une journée. Lors des absences momentanées, les sessions doivent être fermées ou verrouillées.	

PHY122 : Verrouillage automatique des postes de travail		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Un verrouillage automatique du poste de travail en cas d'inactivité prolongée doit être mis en œuvre sur l'ensemble des postes de travail. À ce titre, l'exploitant met en place un écran de veille contrôlé par mot de passe se déclenchant automatiquement au bout de 5 minutes d'inactivité. Des exceptions peuvent-être mises en place sur certaines fonctions (ex : poste de supervision), sous validation du RCSSI.	





3.3 Gestion de l'exploitation et de la maintenance

3.3.1 Procédures et responsabilités liées à l'exploitation

3.3.1.1 Documentation des procédures d'exploitation

EXP001 : Contenu des procédures d'exploitation	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> </div>	<p>Les procédures d'exploitation décrivent pour chaque système à charge les éléments suivants (liste non exhaustive) :</p> <ul style="list-style-type: none"> • Sur le volet <i>fonctionnel</i> : <ul style="list-style-type: none"> ○ une description du système ; ○ une référence au dossier d'architecture technique • Sur le volet <i>technique</i> : <ul style="list-style-type: none"> ○ le processus d'administration de la solution (matériel et logiciel système) ; ○ les contrôles applicables aux supports amovibles ou matériels ; ○ la sécurité des documents (identification, classification, ...) ; ○ la sécurité physique (contrôle d'accès ; sécurité des salles serveurs) ; ○ démarrage et arrêt des serveurs hébergés dans les salles informatiques (déroulé des opérations, intervenants autorisés, etc.) ; ○ maintenance des serveurs (durée, modalité d'intervention, intervenants autorisés, procédure de retour en arrière) ; ○ sauvegarde système et applicative ; ○ supervision système et applicative ; ○ procédures de redémarrage et de récupération du système à appliquer en cas de panne du système ; • Sur le volet <i>organisationnel</i> : <ul style="list-style-type: none"> ○ les responsabilités des parties prenantes ; ○ la gestion des comptes et les droits utilisateurs et techniques ; ○ le signalement des incidents de sécurité ; ○ les relations avec les autres partenaires (exemple : maintenance) ; ○ traitement et manipulation des données ; ○ gestion des erreurs susceptibles d'apparaître lors de l'exécution d'une tâche ; ○ contacts avec l'assistance technique en cas de difficultés techniques ; ○ instructions particulières sur la manipulation des supports et des données de sortie création, manipulation, destruction, mise au rebus ...). <p>Les auteurs, les destinataires et les responsables de la validation du document doivent être précisés pour chaque document.</p> <p>La liste de tous les livrables permettant d'assurer correctement l'exploitation est dressée et tenue à jour dans un référentiel sous la responsabilité de l'exploitant.</p>

EXP002 : Mise à jour de la documentation	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <div></div> <div></div> <div></div> </div>	<p>La mise à jour de la documentation doit être effectuée au plus tôt.</p> <p>À tout moment, elle doit être conforme à la réalité technique des systèmes en production ou organisationnelle.</p> <p>Elle doit être gérée durant toute la durée de vie du SI associée, de son initialisation jusqu'à son décommissionnement.</p> <p>La documentation élaborée doit prendre en compte une gestion des versions et être historisée.</p> <p>Les <i>procédures d'exploitation</i> doivent être révisées selon un <i>processus</i> [DAP-REV-PES] [RI.27], au minimum une fois par an via un <i>modèle de PV</i> [DAP-PVR-PES] [RM.11], qui sera remis à l'administration pénitentiaire.</p>
EXP003 : Validation des procédures	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <div></div> <div></div> <div></div> </div>	<p>Les procédures d'exploitation sont validées avant l'homologation sous l'autorité du RCSSI de la direction de l'administration pénitentiaire et contrôlées durant la phase d'exploitation au moins une fois par an.</p>
EXP004 : Mise à disposition des guides d'administrateur	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <div></div> <div></div> <div></div> </div>	<p>Pour les administrateurs, l'intégrateur doit :</p> <ul style="list-style-type: none"> • mettre à disposition des administrateurs les guides d'exploitation des zones d'interconnexions du service ; • élaborer et mettre à disposition des administrateurs du service les guides d'administration des dispositifs du service ; • élaborer et mettre à disposition des administrateurs les guides d'administration des dispositifs des systèmes d'information administrés dans le cadre de la délivrance du service ; • élaborer et mettre à disposition des administrateurs les guides d'administration des dispositifs des systèmes d'information qui les concernent ainsi que les bonnes pratiques d'administration sécurisées, qui doivent être inclus dans le plan de formation.

EXP005 : Directives de sécurité spécifiques à chaque application	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des directives de sécurité spécifiques à chaque application doivent être élaborées et accessibles aux utilisateurs de l'application soit au travers d'un document spécifique soit au travers d'un guide d'utilisation.</p> <p>Par exemple, les précautions d'utilisation concernant les bornes biométriques doivent être accessibles aux personnels de surveillance (sans pour autant l'être aux personnes détenues)</p>
EXP007 : Définition des responsabilités liées à la gestion et l'exploitation des SI	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les responsabilités des acteurs et les procédures liées à la gestion de l'exploitation de l'ensemble du SI doivent être établies via une <i>matrice de gestion de responsabilités</i> [RI.06].</p>
EXP008 : Documentation de réversibilité	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>La documentation technique du SI doit être maintenue à jour et intégrer tous les éléments permettant d'assurer sa réversibilité : elle permet de lister l'ensemble des moyens (humains et matériels, procédures et référentiel de la documentation d'exploitation) utilisés par l'exploitant, ainsi que les modalités permettant d'extraire tous les éléments de configuration du SI ou des données métier à reprendre dans le cadre de la réversibilité.</p>
EXP009 : Information aux administrateurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Il est recommandé d'informer les administrateurs de la traçabilité technique de leurs actions d'administration et de la possibilité de supervision à laquelle ils sont soumis au titre de la politique de sécurité des systèmes d'information.</p>

EXP010 : Validation et documentation des interventions des prestataires sur les SI de sûreté		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Les interventions techniques effectuées par les prestataires sur les équipements des systèmes de sûreté doivent être systématiquement validées par la DAP.</p> <p>Chaque intervention doit donner lieu à un rapport d'intervention précisant le problème, les actions effectuées pour sa résolution, l'identité des personnes présentes ainsi que leur rôle [RM.07][DAP-INTV-PRESTA] [RM.07].</p>	

3.3.1.2 Sécurité liée à l'exploitation

Ce chapitre correspond au Chapitre « 12 – Sécurité liée à l'exploitation » de l'ISO 27002:2022 [RD.10].

EXP020 : Protection des services d'information essentiels		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Les SI de sûreté doivent être sécurisés en s'appuyant notamment sur les bonnes pratiques du guide « <i>Recommandations pour la protection des systèmes d'information essentiels</i> » de l'ANSSI [ANSSI-R-SIE] [RD.16].</p>	

3.3.1.3 Maintenance en condition opérationnelle et de sécurité


EXP030 : Conformité du prestataire au référentiel PAMS		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Le prestataire doit respecter les exigences du <i>référentiel d'administration et de maintenance sécurisé</i> de l'ANSSI [ANSSI-R-PAMS] [RD.01] pour maintenir les SI de la DAP.</p> <p>Les exigences qui ne peuvent pas être appliquées devront être communiquées au RCSSI de la DAP pour arbitrage.</p>	


EXP031 : Veille MCO/MCS		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Une veille technologique doit être réalisée sur l'ensemble des composants matériels et logiciels en production dans le cadre du MCO/MCS.</p>	


EXP032 : Veille technologique sur les vulnérabilités	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Une veille technologique sur les vulnérabilités pouvant impacter tout ou partie du système doit être assurée.</p> <p>Cette veille s'effectue notamment auprès de CERT comme le CERT-FR.</p> <p>Les alertes associées sont intégrées à la procédure de <i>gestion des incidents</i> [DAP-GEST-INC] [RI.30].</p>
EXP033 : Contextualisation de la menace	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Toutes les vulnérabilités potentielles doivent faire l'objet d'une contextualisation de la menace dans l'environnement concerné.</p>
EXP034 : Processus de MCO et MCS	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Les processus de maintien en condition opérationnelle (MCO) et maintien en condition de sécurité (MCS) sont décrits dans le cadre du plan d'assurance sécurité (PAS) fourni par l'exploitant et validé par l'administration pénitentiaire.</p> <p>Tous les changements apportés aux systèmes d'informations de la DAP sont conformes à ces processus.</p>
EXP035 : Gestion de la fin de support d'une application ou d'un matériel	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Lors du référencement de nouvelles solutions ou lors de la revue annuelle des solutions déjà inscrites au <i>cadre de cohérence technique</i> [DAP-CCT] [RI.54], le RCSSI s'assure de leur viabilité (feuille de route des produits, capacité à intégrer des besoins clients dans l'année, durée de vie des versions, suivi du MCS).</p> <p>Dès la connaissance de l'arrêt du support d'une application, d'un composant associé (framework, base de données) ou d'un matériel, la DAP doit proposer une migration au titre du MCS vers un nouveau composant sans altérer les exigences métiers.</p>
EXP036 : MCS lors de mise en œuvre de solutions temporaires	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>La mise en œuvre d'une solution « temporaire » qui peut ponctuellement dégrader le respect des exigences de sécurité induites par les besoins métiers doivent être tracées et validées par le RCSSI de la DAP avant le déploiement.</p> <p>Concomitamment, elle doit faire l'objet d'un plan d'actions afin de revenir dans un état « stable ».</p>

3.3.1.4 Gestion des changements

EXP040 : Mise à jour du dossier d'architecture	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <div></div> <div></div> <div></div> </div>	<p>Pour toute évolution du système existant, le dossier d'architecture est mis à jour pour prendre en compte les éventuels nouveaux besoins de sécurité identifiés par les commanditaires. Le service en charge de la réalisation du projet, de l'application ou de l'évolution complète le dossier existant afin d'apporter des garanties sur la prise en compte des besoins de sécurité exprimés par l'administration.</p> <p>Il doit également décrire dans ce dossier les évolutions d'architecture technique retenues, les solutions mises en œuvre et les risques résiduels. Toute évolution ne peut être mise en production qu'après validation des mises à jour du dossier d'architecture et décision d'acceptation des risques par le RCSSI DAP.</p>
EXP041 : Procédures de mises à jour des systèmes	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <div></div> <div></div> <div></div> </div>	<p>Les mises à jour applicatives ou apportées aux équipements et aux systèmes, utilisés dans le cadre des projets ou de la bureautique de la DAP, doivent suivre un processus issu de procédures formalisées par l'intégrateur précisant la conduite :</p> <ul style="list-style-type: none"> • des tests fonctionnels et de performance ; • des tests de non-régression ; • des tests de conformité aux exigences SSI ; • des tests de qualification et de validation. <p>Ces procédures doivent introduire la notion de reprise et de restauration du dernier état sûr connu, dans le cas où la mise à jour sur le système ou l'équipement en production ou de l'applicatif ne permettrait pas d'obtenir le résultat escompté.</p>




EXP042 : Passage en comité de déploiement	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les déploiements sur les plateformes de production doivent obligatoirement passer par un comité de déploiement, conformément à la <i>procédure de gestion du déploiement</i> [DAP-CHMG] [RI.52].</p> <p>Les étapes à prendre en compte sont <i>a minima</i> les suivantes:</p> <ul style="list-style-type: none"> • identification des changements à déployer ; • évaluation des impacts opérationnels sur le service rendu ; • validation des procédures de retour à la situation d'origine en cas d'abandon suite à un échec des changements ou à des événements imprévus ; • validation des cibles (sites pilotes puis généralisation) et de la proposition de planning de déploiement (qui pourra être légèrement ajustée <i>a posteriori</i> si besoin) ; • communication des informations détaillées sur les changements aux utilisateurs concernés s'il y a un impact fonctionnel ou organisationnel ; • consignation des changements et mise à jour des versions applicatives ou des configurations associées dans le plan d'urbanisation de la DAP le cas échéant.

EXP043 : Contenu des procédures de mises à jour	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les procédures de mises à jour doivent comprendre entre autres :</p> <ul style="list-style-type: none"> • un point d'entrée métier et opérationnel ; • démarrage et arrêt des services hébergés (déroulé des opérations, intervenants autorisés ...) ; • maintenance des serveurs (durée, modalité d'intervention, intervenants autorisés) ; • le temps maximum d'indisponibilité du système. • les modalités de retour arrière • vérification que la faille ou le bug a bien été traité à la suite du changement.

EXP044 : Réalisation des mises à jour dans le cadre des fiches réflexes	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Tout déploiement d'une mise à jour pour adresser un besoin de sécurité (correction d'une vulnérabilité) ou un besoin métier (besoin d'une nouvelle fonctionnalité) ne peut se faire sur un site qu'après avoir été validé par la DAP sur la plateforme d'intégration. Une fois un module applicatif ou correctif validé, l'exploitant local du SI du site est autonome dans son déploiement, dans le strict respect des consignes de déploiement prévues par la DAP.</p> <p>Dans le cas d'une force majeure imposant un déploiement en urgence sans validation au niveau national, l'exploitant (administrateur de la plateforme) doit obligatoirement en informer le responsable d'établissement et la cellule SSI de la DAP.</p>

EXP045 : Modification du SI en dehors du cadre des fiches reflexes	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>En dehors du cadre des fiches réflexes, l'intégrateur doit assister l'exploitant pour réaliser une modification du SI (suite à une mise à jour ou incident).</p>
EXP046 : Procédure de mise à jour en urgence	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Une procédure de mises à jour en urgence doit être proposée par l'intégrateur en fonction de la contextualisation réalisée.</p>
EXP047 : Processus de modification légitime de privilège	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Le processus de modification légitime de privilèges doit faire l'objet d'un flux de validation. Cela implique notamment que :</p> <ul style="list-style-type: none"> • l'attribution des rôles d'administrateurs fonctionnels soit soumis à la validation d'un responsable métier ; • l'attribution des rôles d'administrateurs techniques soit soumis à la validation d'un responsable technique.
EXP048 : Recette applicative suite à une mise à jour	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Une recette des applications doit être réalisée sur la base d'un cahier de recette après une mise à jour et formalisée sur la base du <i>modèle de PV</i> [DAP-PVR-APPL] [RM.13].</p> <p>Le cahier de recette doit être fourni par l'intégrateur, déroulé par l'exploitant et approuvé in fine par le chef d'établissement.</p>

3.3.2 Résilience

EXP061 : Déclinaison des exigences DIMA et PDMA	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Le délai d'interruption maximum autorisé (DIMA) et le niveau de perte de données maximum autorisé (PDMA) en cas d'incident devront être définis spécifiquement pour chaque site et système d'information au regard des besoins de sécurité de chaque système d'information.</p> <p>Le niveau de PDMA est exprimé en jour ou en heure en fonction du système d'information.</p>
EXP062 : Certification Tiers III pour les centres de données	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Le ou les centres de données auront obtenu un niveau minimum équivalent à la certification Tiers III afin d'atteindre l'exigence de disponibilité demandée.</p> <ul style="list-style-type: none"> • cette capacité exige que tous les systèmes composant les circuits d'alimentation et de distribution soient redondants ; • les groupes électrogènes destinés à garantir l'autonomie de l'alimentation en électricité doivent pouvoir fonctionner à charge nominale sans que leur durée du fonctionnement doive être limitée ; • aucune vanne de jonction ne doit être mise en place entre deux réseaux d'eau glacée, car la maintenance de cette vanne obligerait à arrêter le fonctionnement du data center ; • toutefois, le fonctionnement du système informatique peut être interrompu en cas d'incident ou de panne ; • le taux de disponibilité doit s'élever à 99,982 % et les éventuels moments d'indisponibilité ne doivent pas dépasser un total de 96 minutes par an. <p>Si la certification n'est pas formellement obtenue, tous les éléments permettant de couvrir les exigences associées à ce niveau de certification devront être fournies à la DAP afin de prouver l'équivalence.</p>
EXP063 : Mesures contre les défaillances électriques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des mesures doivent être prises contre les défaillances électriques, en assurant un contrôle et un secours opérationnel de l'alimentation (par onduleur et groupe électrogène).</p> <p>Un délai minimal de secours de l'alimentation principale doit permettre de réaliser les opérations d'arrêt propre (et éventuellement de sauvegarde) nécessaires à une reprise d'activité efficace.</p>

EXP064 : Mesures contre les défaillances des réseaux de télécommunications



Face aux défaillances des réseaux de télécommunications, un secours est assuré en portant une attention particulière aux procédures de basculement vers des lignes de secours en cas d'interruption de ligne.

La redondance des moyens de communication (performances des équipements et capacités des lignes identiques entre secours et nominal) est définie pour les plateformes de production et les établissements sensibles en fonction des besoins de haute disponibilité de chaque système d'information et de chaque site.

Une solution de redondance dégradée (performances et capacités inférieures) est mise en œuvre pour les autres sites de l'administration pénitentiaire.

EXP065 : Contrôle des mécanismes de résilience et de tenue à la charge

Réf. GRC : non implémenté

ISO27002:2022 : non référencé






Les mécanismes de résilience des services essentiels tels que définis dans l'analyse de risque (ex : alimentation électrique, climatisation, télécommunication) doivent faire l'objet d'un contrôle de bon fonctionnement pour vérifier la résilience aux pannes des composants redondés. Un suivi capacitaire du dimensionnement associé doit être opéré afin d'anticiper les prochaines évolutions logicielles et matérielles du SI.




Ces contrôles doivent être formalisés au sein de fiches de contrôle dédiées du classeur de sécurité **[RM.36]** et opérés a minima une fois par an.




La maintenance et des tests de bon fonctionnement en condition réelle (en charge) devront faire l'objet d'un *PV sur la base du modèle x* ainsi que d'un plan d'actions si nécessaire.

3.3.3 Sauvegarde

3.3.3.1 Stratégie de sauvegarde


EXP070 : Définition de la stratégie de sauvegarde	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Une stratégie de sauvegarde doit systématiquement être définie en précisant notamment :</p> <ul style="list-style-type: none"> • les créneaux de sauvegardes, • les durées de rotation et de rétention des données sauvegardées, • les durées et les modalités de conservation (externalisation ...), • les références des bandes utilisées ainsi que celles du lecteur, • les fréquences de tests de ces sauvegardes, • la correspondance entre les identifiants des bandes et les données contenues ; • les données sauvegardées et le processus de mise à jour des jobs de sauvegarde ; • les personnes responsables des plans de sauvegardes et les opérateurs ; • le processus de vérification et de validation des sauvegardes ; • le processus de restauration des données (personnes autorisées, répertoires destination, chargement des bandes, slots et lecteurs utilisables ...). <p>Cette exigence concerne notamment les sauvegardes :</p> <ul style="list-style-type: none"> • des données et fichiers « métier » ; • des sources des logiciels et applications informatiques appartenant à la DAP ; • des fichiers de configuration des logiciels et applications informatiques ; • des comptes utilisateurs et des droits associés ; • des traces et journaux « fonctionnels ou métiers », « applicatifs » et « techniques ».


EXP071 : Réalisation des opérations de sauvegardes	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les opérations de sauvegardes doivent être effectuées sur un périmètre précis, et donner lieu à un compte-rendu avec indicateur de réussite ou d'échec.</p>


DEV072 : Sauvegarde du patrimoine informationnel	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les applications (sur étagère ou développées) doivent intégrer des mécanismes de sauvegardes et restauration des données adaptés aux niveaux de disponibilité, d'intégrité, de confidentialité et de preuves (DICP) de l'application.</p>


3.3.3.2 Stockage des sauvegardes

EXP080 : Protection des supports de sauvegarde	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <div></div> <div></div> <div></div> </div>	<p>Les supports de sauvegarde dédiés aux informations sensibles du système d'information doivent être protégés contre les risques de divulgation et d'accès aux informations par des personnes non autorisées.</p> <p>Les supports de sauvegarde des données sensibles hors-lignes, externalisés ou non, doivent faire l'objet d'un chiffrement conforme au <i>référentiel général de sécurité (RGS)</i> [RGS] [RRG.01] afin de garantir leur confidentialité.</p>


EXP081 : Externalisation des sauvegardes	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Un double des sauvegardes doit être conservé dans des locaux physiquement séparés, avec recours à un prestataire ou partenaire externe dont les locaux sont situés sur le territoire français.</p> <p>L'externalisation périodique de ces supports de sauvegarde doit être mise en œuvre pour les systèmes contenant des informations demandant un niveau de disponibilité égal ou supérieur à D2 (cf <i>métriques SSI DAP</i> [DAP-METR-SSI] [RI.58]).</p> <p>Cette externalisation doit être réalisée de manière physique (déplacement des supports de sauvegarde vers le site de secours).</p> <p>La fréquence de l'externalisation comme celle des sauvegardes doivent être déterminées de manière à permettre d'assurer le besoin de continuité des systèmes sauvegardés en cas de sinistre majeur sur le site nominal.</p> <p>Lorsque l'externalisation n'est pas possible ou nécessaire, les sauvegardes contenant les configurations systèmes et les données sensibles doivent être placées dans une armoire ignifugée, sécurisée selon la sensibilité des informations contenues. Cette armoire ne doit pas être située dans le local technique qui contient les serveurs.</p> <p>Seules les personnes explicitement autorisées et nominativement identifiées peuvent accéder au contenu de l'armoire.</p>

EXP082 : Règles de stockage de données dans une infrastructure de type « cloud »	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Le stockage de tout ou partie des données dans une infrastructure de type « cloud » ou « nuage » peut être envisagé aux conditions suivantes :</p> <ul style="list-style-type: none"> • la mise en œuvre doit être formellement autorisée par l'Autorité nationale (ANSSI) ; • la solution d'informatique en nuage doit respecter le <i>référentiel SECNUM-Cloud</i> de l'ANSSI [SecNumCloud] [RD.08] sur les prestataires de service d'informatique en nuage de confiance ; • la qualification de la solution d'informatique en nuage doit être au minimum de niveau « Essentiel » selon le <i>référentiel SECNUM-Cloud</i> de l'ANSSI [SecNumCloud] [RD.08] ; • la validation du RCSSI.

EXP083 : Gestion des sauvegardes pour les systèmes avec un niveau de disponibilité très élevé	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Dans le cas d'un niveau de disponibilité très élevé, de niveau D3, les supports de sauvegarde peuvent être maintenus dans les dispositifs de sauvegarde/restauration pour permettre le respect de ce besoin de sécurité, dans la mesure où les besoins de confidentialité ou d'intégrité sont peu significatifs (de niveau inférieur ou égal à C1, respectivement I1, cf <i>métriques SSI DAP [DAP-METR-SSI] [RI.58]</i>).</p> <p>Dans le cas contraire, soit le commanditaire réévalue ses besoins de sécurité, soit le haut-niveau de disponibilité doit être assurée par d'autres solutions techniques (SAN multisite ou géographiquement réparti sur un site).</p>

EXP084 : Gestion des sauvegardes pour les systèmes sensibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Pour tous les systèmes sensibles (SIIV), les supports de sauvegarde sont stockés dans des conteneurs sécurisés et ignifugés.</p>

3.3.3.3 Tests des sauvegardes




EXP090 : Test périodique des sauvegardes et restauration	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>La sauvegarde et la restauration des sauvegardes doit être testée périodiquement afin de garantir la capacité de restituer le service complet d'un composant du système d'information.</p> <p>Cette périodicité sera fonction de la sensibilité face à la disponibilité des données, au minimum chaque année.</p>




EXP091 : Test des plans de sauvegardes et restauration avant la mise en production du nouveau système	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Avant la mise en production d'un nouveau système, les plans de sauvegarde et de restauration doivent être testés sur le nouveau composant afin de garantir la reprise des données à la suite d'un incident potentiel.</p>




EXP092 : Gestion du cycle de vie des supports de sauvegarde	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Le cycle de vie des supports de sauvegardes doit être défini précisant pour chaque type de support, une indication sur la date de remplacement de celui-ci en pourcentage de sa durée de vie.</p> <p>Les supports de sauvegardes doivent être testés périodiquement afin de garantir leur état, de manière à prévenir toute défaillance ou panne. Il faut être vigilant sur la durée de vie des supports car certains conservent les données sur une durée plus ou moins longue.</p> <p>Les tests de restauration de sauvegardes et des supports doivent faire l'objet de procès-verbaux incluant un indicateur de réussite ou d'échec ainsi qu'un plan d'action si nécessaire afin de corriger les problèmes rencontrés.</p> <p>Afin d'effectuer ces tests, il convient d'en informer l'établissement pénitentiaire, la chaîne SSI ainsi que le RCSSI de la DAP avec un délai de prévenance d'un mois.</p>




EXP093 : Remplacement des supports de sauvegardes en cas de défaillance ou panne	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Les supports de sauvegardes doivent être remplacés immédiatement en cas de défaillance ou de panne.</p>

3.3.3.4 Récupération des données sur sauvegarde




EXP100 : Gestion des demandes de récupération de données sauvegardées	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les demandes de récupération de données sauvegardées doivent être motivées et faire l'objet d'une procédure de contrôle strict afin de garantir que toute demande de restauration d'une donnée soit faite sous contrôle du chef d'établissement en informant la chaîne SSI.</p> <p>Les demandes de récupération de données sauvegardées doivent être consignées.</p>

EXP101 : Personnel habilité à valider les demandes de récupération des données	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Une matrice permettant de connaître la liste des personnes habilitées à valider les <i>demandes de récupération des données</i> [DAP-DDE-TRACES] [RM.20], en fonction du périmètre de la demande, doit être disponible.</p>

EXP102 : Revue du personnel habilité à valider les demandes de récupération des données	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>La matrice permettant de connaître la liste des personnes habilitées à valider les <i>demandes de récupération des données</i> [DAP-DDE-TRACES] [RM.20], doit être revue annuellement pour chaque périmètre donné et les changements doivent être tracés.</p>

EXP103 : Rapport annuel des demandes de récupération de données sauvegardées	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les demandes de récupération de données sauvegardées doivent faire l'objet d'un rapport annuel à destination de la DAP.</p>

3.3.3.5 Règles de conservation des sauvegardes et d'archivage

EXP110 : Archivage	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les documents conservés pour des raisons légales, contractuelles ou nécessaires au bon fonctionnement du système d'information doivent être archivés en tenant compte de leur sensibilité, leur durée de vie et des types de supports conformément à la procédure d'archivage des documents et informations légales [DAP-ARCHIVAGE] [RI.70].</p>

3.3.4 Protection contre les logiciels malveillants


Les logiciels malveillants se propagent sous forme de pièces jointes à un mail, via les supports amovibles ou par l'exploitation d'une faille de sécurité.


Les risques encourus en cas de contamination sont :


- La panique (peut faire plus de dégâts que le virus) ;
- La perte d'image ;
- La fuite d'information ;
- La perte d'information (effacement d'un fichier non encore sauvegardé) ;
- Le cheval de Troie (mise en place d'une porte dérobée dans le système) ;
- L'utilisation de ressources humaine pour éradiquer le virus ;
- La saturation des ressources informatiques.


Des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants doivent être mises en place sur l'ensemble du système d'information.


Cependant les systèmes anti-virus restent faillibles donc des mesures complémentaires doivent être prises telle la désactivation de l'ouverture automatique des pièces jointes, la sauvegarde régulière du poste et ne pas baser toute sa confiance dans les solutions techniques.


EXP120 : Désactivation des systèmes de protection contre le code malveillant	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les systèmes de protection contre les codes malveillants ne doivent pas être désactivés sans justification.</p> <p>Le RCSSI de la DAP doit valider la désactivation de ce type de protection.</p>

EXP121 : Déploiement de solutions de protections des postes de travail	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des solutions de protection (anti-virus, EDR...) contre les attaques doivent être déployées sur tous les serveurs, et les postes de travail. Ces solutions ainsi que leurs bases de connaissance doivent être mises à jour régulièrement (cf. <i>politique générale de lutte antivirale</i> appelée « PGLA » dans la suite du document [MJ-DAP-PGLA] [RI.22]). Cette politique précise également les zones d'exclusions d'analyse antivirale qui peuvent s'avérer nécessaires au bon fonctionnement du SI.</p>

EXP122 : Actions à effectuer en cas de contamination avérée	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>En cas de contamination avérée, le système doit immédiatement être déconnecté du réseau et la chaîne SSI doit être notifiée.</p> <p>Aucun support de stockage amovible en lecture/écriture (clef USB, disque dur portable, etc.) ne devra être connecté sur cette machine en dehors d'une opération de décontamination.</p> <p>Toutes les règles concernant ces contrôles sont précisées dans une <i>Politique Générale de Lutte Anti-virale (PGLA)</i> [MJ-DAP-PGLA] [RI.22] de la DAP.</p>

EXP123 : Mise en place de station blanche afin d'analyser les médias	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des moyens de vérification anti-virale (station blanche) des médias doivent être mis à disposition des utilisateurs de l'AP, afin de permettre une vérification du contenu du support.</p> <p>L'exploitant doit maintenir à jour la station de décontamination et toutes les briques logicielles qui la composent.</p>

EXP124 : Gestion des alertes anti-virales	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>La gestion des alertes (virus, failles de sécurité, avertissements...) relève de la responsabilité de l'exploitant sous contrôle du RCSSI de la DAP.</p> <p>Le circuit de suivi et de prise en compte de ces informations est précisé dans la <i>PGLA</i> de la DAP [MJ-DAP-PGLA] [RI.22].</p> <p>Seul le RCSSI de la DAP (ou les personnes désignées pour cette tâche) est autorisé à faire suivre les informations de gestion des alertes en dehors du circuit de diffusion de l'information définie dans la PGLA.</p>


EXP125 : Choix de l'antivirus sur les postes de travail et serveurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Afin de renforcer la sécurité globale et sur application du principe de défense en profondeur, le logiciel installé sur les serveurs frontaux doit être différent des logiciels installés sur les serveurs backend et les postes utilisateurs.</p> <p>Le RCSSI de la DAP doit valider les solutions identifiées par l'intégrateur.</p>

3.3.5 Relations avec les fournisseurs


3.3.5.1 Règles générales

FOU001 : Clauses de sécurité dans les contrats	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>Tout nouveau contrat ou convention de service conclu avec un tiers dans le cadre d'un système d'information de la DAP contient des clauses traitant explicitement de la sécurité du système d'information.</p> <p>Le contrat doit assurer la prise en compte par le tiers des PSSI de la DAP et des éventuelles mesures spécifiques résultant de l'analyse de risques de ce tiers (habilitation requise pour l'organisme et ses personnels, isolement ou sécurisation renforcée de ses infrastructures, etc.).</p> <p>Il intègre également une partie concernant le non-respect des engagements (pénalités et responsabilités).</p> <p>Tout nouveau contrat doit systématiquement intégrer une clause de réversibilité dont les conditions principales sont détaillées dans le <i>clausier de sécurité des marchés [DAP-SEC-AO] [RI.84]</i>.</p> <p>Au regard des évolutions réglementaires posant désormais un cadre juridique et légal systématiquement applicable aux SI de Sûreté, il conviendra d'établir un protocole de mise en conformité à cette nouvelle réglementation pour les tiers dont le contrat est déjà engagé. Ce protocole devra permettre de définir la cible de conformité à atteindre ainsi que les grandes étapes intermédiaires pour l'atteindre.</p>

FOU002 : Marché de défense et sécurité		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	Tout marché auprès de tiers permettant d'adresser des prestations liées à un SIIV doit être un marché de défense ou de sécurité, au titre des alinéas 4 et 7 de l'ordonnance [Ord-Cde-Publique] [RL.02].	
FOU003 : Recours à la sous-traitance de rang 2		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	La sous-traitance de rang 2 est interdite sauf accord préalable du RCSSI de la DAP.	
FOU004 : Responsabilité des clauses contractuelles et des engagements		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	Le représentant légal de chacune des sociétés prestataires de la DAP est responsable des clauses contractuelles et des engagements en matière de sécurité des systèmes d'information durant la durée d'exécution du contrat. Tout marché passé avec un titulaire doit inclure une clause de réversibilité avec une durée strictement nécessaire et suffisante pour assurer la transition avec le nouveau titulaire, incluse dans la durée du contrat.	
FOU005 : Plan d'assurance sécurité		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<p>Un <i>plan d'assurance sécurité (PAS)</i> devra être annexé à chaque contrat.</p> <p>Le PAS devra :</p> <ul style="list-style-type: none">• Démontrer la conformité à la présente PSSI et documents afférents• Prouver la capacité du prestataire à se mettre au niveau des besoins de sécurité <p>Le PAS devra se baser sur le modèle fourni par la DAP [DAP-PAS] [RM.15].</p> <p>Une déclinaison du PAS devra être propre à chaque établissement via une annexe spécifique.</p>	




FOU006 : Modalité de revue et évolution du plan d'assurance sécurité	
Réf. GRC : non implémenté	ISO27002 :2022 : non référencé
	<p>En cas d'évolution majeure (système, environnement, ...), une revue du PAS et de ses annexes doit être réalisée par la DAP et le prestataire.</p> <p>Celle-ci pourra éventuellement mener à une mise à jour de celui-ci.</p>




FOU 07 : Accord de non-divulgence	
Réf. RC : non référencé	ISO27 002:2 22 : non référencé

	<p>Un <i>accord de non-divulgence (AND)</i> [DAP-NDA] [RM.22] doit être intégré à tout contrat passé avec un prestataire impliqué sur le système d'information.</p> <p>L'AND doit comporter les informations ci-dessous :</p> <ul style="list-style-type: none"> • la définition des informations à protéger, • la durée de l'engagement et des actions à engager à expiration, • le besoin d'en connaître et le cloisonnement du partage de l'information, • la responsabilisation et les actions des acteurs pour éviter une diffusion d'informations non autorisée (maîtrise du droit de divulgation), • l'autorisation d'utilisation d'informations sensibles ou confidentielles, • le droit d'audit et de contrôle des activités traitant des informations sensibles ou confidentielles, • les modalités de restitution ou de destruction d'informations à l'expiration de l'engagement, • les actions à engager en cas de violation de l'engagement, • la signature d'un engagement de confidentialité et de non-divulgence à l'entrée et à la sortie du programme. <p>Le représentant du prestataire devra faire respecter cet AND pour chaque collaborateur concerné par l'intermédiaire de la signature d'une AND individuelle ou d'une charte informatique reprenant <i>a minima</i> les engagements de confidentialité avec la DAP.</p>
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------




3.3.5.2 Intervenants SSI du prestataire




FOU010 : Désignation du RSSI du prestataire	
Réf. GRC : non implémenté	ISO27002 :2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Un responsable de la sécurité des systèmes d'information (RSSI), point de contact de la DAP, doit être nommé par le prestataire.</p> <p>Il pilote l'ensemble des actions relevant de la sécurité des systèmes d'information du périmètre d'activités pour lequel la DAP missionne le prestataire.</p>
FOU011 : Désignation du DPD du prestataire	
Réf. GRC : non implémenté	ISO27002 :2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Un délégué à la protection des données (DPD), point de contact de la DAP, doit être nommé par le prestataire.</p> <p>Il pilote l'ensemble des sujets relevant de la protection des données à caractère personnel du périmètre d'activités pour lequel la DAP missionne le prestataire.</p>
FFOU012 : Désignation de l'officier de sécurité du prestataire	
Réf. GRC : non implémenté	ISO27002 :2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Un officier de sécurité (OS), point de contact de la DAP, doit être désigné par le prestataire.</p> <p>Il pilote sur le périmètre d'activités pour lequel la DAP missionne le prestataire :</p> <ul style="list-style-type: none"> • les questions relevant de la protection du secret de la défense nationale • les sujets relevant de la sécurité et de la défense • ainsi que toutes les actions relevant de la sûreté physique et environnementale des biens et des personnes.

FOU013 : Intervenants sécurité du prestataire		
Réf. GRC : non implémenté		ISO27002 :2022 : non référencé
  	<p>Ces interlocuteurs (RSSI, officier de sécurité et référent pour la protection des données) doivent notamment :</p> <ul style="list-style-type: none"> transmettre l'organisation de la défense, la sécurité et la protection des données à caractère personnel du fournisseur à la direction pénitentiaire pour validation ; valider l'ensemble des actions réalisées au titre de la gestion de la sécurité du projet pour ce qui les concerne. ; s'assurer que les mesures visant à éviter la compromission d'information ou de supports classifiés et la fuite d'information sensibles ou DCP sont mises en œuvre ; contrôler la mise en application des Exigence formulées par la DAP pour ce qui les concerne ; réaliser les formations et les sensibilisations adaptées pour le personnel concerné par le système d'information ; formaliser un processus de remonté d'incident et le transmettre à la DAP, le processus doit renseigner : <ul style="list-style-type: none"> Matrice de contact. Processus d'activation des astreintes. remonter sans délais à la DAP tout incident ou toute compromission liée aux systèmes d'information. 	




FOU014 : Responsable sécurité des systèmes de sureté désigné par la DAP		
Réf. GRC : non implémenté		ISO27002 :2022 : non référencé
  	<p>La DAP doit désigner a minima un responsable sécurité pour faciliter les relations entre les différents intervenants sécurité du prestataire, et de mettre à disposition de la maîtrise d'œuvre l'ensemble des documents nécessaires au bon déroulement du projet sécurité en lien avec le prestataire.</p> <p>Il a également pour mission de s'assurer de la prise en compte globale de la sécurité, par la maîtrise d'ouvrage et la maîtrise d'œuvre tout au long du cycle de vie du système.</p>	




3.3.5.3 Externalisation d'application


FOU020 : Conditions d'externalisation des services applicatifs	
Réf. GRC : non implémenté	ISO27002 :2022 : non référencé
  	<p>Toute externalisation de service applicatif de la DAP doit être analysée dans le cadre de l'analyse de risques spécifique à chaque système d'information.</p> <p>Elle doit ensuite être validée par le RCSSI de la DAP et faire l'objet d'un contrat ou d'une convention entre la DAP, l'hébergeur et l'exploitant.</p>


FOU021 : Validation des contrats d'externalisation	
Réf. GRC : non implémenté	ISO27002 :2022 : non référencé
  	<p>Le RCSSI de la DAP doit être impliqué dans le processus de validation de toute modification du contrat d'externalisation.</p>

3.3.5.4 Accès des intervenants aux systèmes d'informations de la DAP


FOU030 : Recensement des intervenants accédant aux SI de la DAP	
Réf. GRC : non implémenté	ISO27002 :2022 : non référencé
  	<p>Tous les intervenants dépendant des fournisseurs qui ont ou pourraient avoir un accès légitime aux systèmes d'information de la DAP, plus particulièrement ceux manipulant des données à caractère personnel, doivent être nominativement identifiés et recensés dans un <i>registre administratif</i> [DAP-REG-SIS] [RM.16] remis à la DAP pour validation.</p> <p>Cette exigence concerne tous les partenaires et leurs sous-traitants, les accès s'effectuent depuis un site de la DAP ou dans les locaux des fournisseurs.</p>

FOU031 : Restriction des SI autorisés à abriter les données de la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les données de la DAP doivent être stockées uniquement sur ses propres SI ou ceux dont elle a la connaissance (ex : plateforme de qualification chez un intégrateur).</p>



FOU032 : Utilisation des données de la DAP par les fournisseurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les fournisseurs ne doivent pas utiliser les documents et informations traités à des fins autres que celles spécifiées, qu'il s'agisse de personnes privées ou publiques, physiques ou morales sans l'autorisation préalable de la DAP.</p> <p>Toutes les mesures doivent être prises pour éviter leur utilisation détournée ou frauduleuse.</p> <p>Les fournisseurs ne doivent réaliser aucune copie des documents, données et supports d'informations qui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation prévue.</p> <p>Les prestataires doivent obtenir l'accord préalable de la DAP pour le traitement ou la modification de données à caractère personnel.</p>

FOU033 : Etat des lieux d'entrée et de sortie d'un exploitant	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>L'entrée et la sortie d'un exploitant sur un SI doit faire l'objet d'un <i>état des lieux</i> selon la procédure établie par la DAP dans le cas des exploitants [DAP-ARR-EXPL] [RI.61], à défaut, d'une procédure de l'exploitant et doit être sanctionnée par un <i>PV</i> basé sur cette procédure.</p>

3.3.5.5 Chaîne d'approvisionnement informatique



FOU040 : Profondeur de la chaîne d'approvisionnement	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>La chaîne d'approvisionnement devra comporter le moins d'intermédiaires possible (ex : privilégier un circuit direct constructeur sans distributeur).</p>


3.3.5.6 Surveillance et revue des services des fournisseurs


FOU050 : Contrôle de la qualité de service des prestataires par la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Le RCSSI de la DAP s'assure que le tiers maintient une capacité de service suffisante et qu'il dispose de plans réalisables pour veiller au respect des dispositions relatives à la continuité du service en cas de défaillance majeure du service ou de sinistre.</p> <p>Il aura notamment la charge de l'analyse des tableaux de bords fournis par l'exploitant du SI lors des comités de suivi et pilotage de la sécurité.</p>
FOU051 : Validation du délai de préparation maximum du prestataire	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Chaque fournisseur s'engage à accepter d'être audité par la DAP ou par toute entité mandatée par la DAP afin de vérifier le bon respect des exigences de sécurité formalisées.</p> <p>Le fournisseur s'engage à garantir la disponibilité des ressources nécessaires afin de permettre à la DAP ou à l'organisme mandaté par celle-ci de mener un audit sur son organisation et son système dans les 3 mois suivant la demande d'Audit de la DAP.</p>


3.3.6 Interconnexion des réseaux


3.3.6.1 Transfert de l'information par voie électronique

RSX001 : Contrôle des réseaux de communication	
	<p>La DAP doit avoir une visibilité de l'ensemble des réseaux de communications de chaque établissement pénitentiaire (sûreté ou non), avec les moyens de sécurité associés (liste exhaustive des interconnexions, tout service confondu).</p>
RSX002 : Solutions de signatures et chiffrement des informations	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des solutions de signatures et/ou de chiffrement des informations seront mises en œuvre en fonction de la confidentialité des données manipulées et échangées.</p> <p>Les solutions de signature et de chiffrement adoptées doivent être conformes aux règles et recommandations du <i>référentiel général de sécurité (RGS) [RGS] [RRG.01]</i>.</p>

RSX003 : Chiffrement des données sensibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les données de catégorie C2 ou supérieure en confidentialité doivent être chiffrées et celles de catégories C3 doivent être stockées et transportées de la même manière que les documents au format papier, conformément aux prescriptions de l'<i>IGI1300</i> [IGI1300] [RRG.02].</p>

RSX004 : Protection des accès aux bases de données	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des mesures de cloisonnement sont mises en œuvre au niveau des bases de données pour garantir en fonctionnement nominal, l'inaccessibilité des données sensibles aux intervenants techniques (et vice-versa).</p> <p>Ce cloisonnement peut s'appuyer sur le chiffrement des données en base comme sur les mécanismes avancés de contrôle d'accès aux données mis en œuvre par les systèmes de gestion de bases de données.</p>

RSX005 : Protection des échanges de données sensibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les échanges de données sensibles entre les composants applicatifs du système d'information ou avec des composants externes doivent être protégés contre toute divulgation non maîtrisée :</p> <ul style="list-style-type: none"> • la diffusion externe de données sensibles impose d'établir un inventaire : <ul style="list-style-type: none"> - des personnes destinataires autorisées ; - des échanges inter-applicatifs ;

RSX006 : Conditions de diffusion externe d'informations sensibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>La diffusion externe d'informations sensibles sera effectuée par du personnel de la DAP, conformément au niveau de confidentialité affecté à l'information.</p> <p>Ainsi le niveau C2 demande uniquement l'inventaire des personnes destinataires, alors que le niveau C3 demande l'application des prescriptions de l'<i>IGI 1300</i> [IGI1300] [RRG.02].</p>

RSX007 : Formalisation d'une politique d'échange	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Une politique d'échange formelle doit être élaborée conformément aux accords sur les échanges et en respectant la législation en vigueur.</p> <p>Le chiffrement des données sensibles avant envoi sera effectué en utilisant les logiciels autorisés par la DAP et porté dans le <i>cadre de cohérence technique</i> de la DAP [DAP-CCT] [RI.54].</p> <p>En cas d'utilisation d'une plate-forme d'échange, seule la solution ministérielle portée par le secrétariat général du ministère est autorisée.</p> <p>Une plateforme alternative pourra être envisagée après un accord explicite du RCSSI de la DAP.</p>




RSX008 : Limitation des données sur le réseau	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Aucunes données autres que celles nécessaires au fonctionnement, l'administration et la journalisation du système de sûreté ne doivent transiter par ce réseau.</p>




3.3.6.2 Transfert de l'information par voie papier

RSX010 : Transmission des documents papier contenant des DCP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Seuls les documents papier contenant des données à caractère personnelle (DCP) strictement nécessaires au traitement doivent être transmis.</p>




RSX011 : Traçabilité de la transmission des documents papier contenant des DCP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Toute transmission de documents au format papier contenant des DCP doit être tracée dans une demande instanciée sur la base du modèle [DAP-DDE-DACP] [RM.17.1] et validée.</p> <p>Un inventaire de tous ces demandes doit être créé et tenu à jour sur la base du modèle [DAP-REG-DACP] [RM.17.2].</p>

3.3.6.3 Politiques en matière de transfert de l'information

RSX020 : Règles de transmission des informations	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>La transmission vers l'extérieur de messages internes ou de données propres à la DAP est autorisée si ces messages ou informations ont été :</p> <ul style="list-style-type: none"> anonymisés conformément aux recommandations de la directive sur la protection des données instituées par la <i>directive 95/46/CE</i> [D95-46-TDCP] [RL.06] ; blanchis de toute donnée permettant d'avoir des informations sur le système ou l'organisation, conformément au <i>guide de mise au rebut</i> de la DAP [DAP-DSTR-MAT] [RI.10]. <p>Ces informations ne doivent pas permettre aux personnes non habilitées d'obtenir des informations sur l'organisation et les SI de la DAP.</p> <p>Les techniques d'anonymisation doivent être décrites dans le dossier d'homologation de l'application.</p>

RSX021 : Règles de publication de documents numériques vers le public	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Toutes les informations vers le public sont soumises à validation du service de communication de l'administration centrale de la DAP, qui pourra s'appuyer sur l'expertise des différentes sous-directions pour juger du bienfondé de l'information communiquée.</p>

3.3.6.4 Messagerie électronique

RSX030 : Protection des informations des courriers électroniques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Le niveau de sécurité du courrier électronique est faible, il ne doit pas servir à transmettre des informations classifiées de niveau C3 en confidentialité.</p> <p>Toutes les informations classifiées au niveau C2 devront être protégées (chiffrées) avec un outil figurant dans le <i>cadre de cohérence technique (CCT)</i> de la DAP [DAP-CCT] [RI.54] avant d'être transmises.</p>

RSX031 : Format des documents bureautiques transmis		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	L'ensemble des documents bureautiques doivent être transmis dans un format non modifiable (exemple PDF).	
	Le recours à l'annotation des documents reste possible si besoin.	

3.3.7 Gestion des journaux

Les mesures de protection des journaux mentionnées ici s'appliquent aussi bien aux applications des SI de sûreté qu'aux composants d'infrastructure et de gestion centralisée des journaux.

3.3.7.1 Informations à journaliser

LOG001 : Stratégie de journalisation et de surveillance propre à chaque SI	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Une stratégie de collecte de journaux et de surveillance doit être définie pour chaque système.</p> <p>Cette stratégie de collecte doit être cohérente avec les risques identifiés pour chaque système.</p> <p>En cas d'incapacité à journaliser certains éléments définis dans la stratégie de collecte, un plan d'action doit permettre de compenser ces manquements ou acter l'acceptation de ce manquement.</p> <p>Dans le deuxième cas, une validation du RCSSI de la DAP est nécessaire.</p>
LOG002 : Événements relatifs à l'authentification des utilisateurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Les événements relatifs à l'authentification des utilisateurs, à la gestion des comptes, des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité du SI de sûreté ainsi que son fonctionnement doivent faire l'objet d'une consignation dans des journaux.</p>
LOG003 : Journalisation des actions d'administration	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Toutes les actions d'administration sur les systèmes de sûreté doivent être journalisées.</p>
LOG004 : Politique d'archivage des journaux des applications	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Le délai d'archivage des journaux des applications doit être défini pour chaque système d'information conformément à sa politique d'archivage.</p>


LOG005 : Utilisation d'une source de temps fiable	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Tous les événements journalisés doivent être horodatés avec une source de temps de fiable et identique pour l'ensemble des composants du SI de sûreté.


3.3.7.2 Protection de l'information journalisée


LOG010 : Protection des journaux	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Les équipements de journalisation et les informations journalisées doivent être protégés contre : <ul style="list-style-type: none"> • la modification des types de messages enregistrés, • la modification ou la suppression des fichiers journaux, • le dépassement de la capacité de stockage des fichiers des journaux.

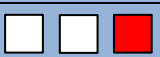
LOG011 : Protection des journaux vis-à-vis des administrateurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Les administrateurs « sécurité », « télécom », « système » et « réseaux » ne doivent pas être en mesure d'effacer, modifier leurs propres activités ou de désactiver l'historisation de ces activités sans que de telles actions ne soient détectables. Dans la mesure du possible, le rôle d'administrateur ayant accès aux données doit être séparé de celui ayant accès aux traces.

LOG012 : Protection des journaux sensibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Les journaux définis comme sensibles par l'analyse de risques du SI sont protégés par des mécanismes conformes aux règles et recommandations du <i>référentiel général de sécurité (RGS) [RGS] [RRG.01]</i> et pouvant assurer leur besoin d'intégrité (supérieur ou égal au niveau I2). Ces traces doivent être protégées par une fonction « cachet serveur » conforme au <i>RGS [RGS] [RRG.01]</i> , lors de la centralisation des informations afin d'en garantir l'intégrité.

LOG013 : Conservation des informations journalisées	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les journaux doivent être conservés sur un système de stockage différent et indépendant du système qui les a produits :</p> <ul style="list-style-type: none"> • En enregistrant les journaux sur un système de fichiers dédié disposant d'une capacité de stockage suffisante ; • En exportant les journaux vers un serveur de collecte de l'infrastructure (envois au fil de l'eau ou envois planifiés) ;

LOG014 : Rotation des informations journalisées	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Un système de rotation des informations journalisées doit être mis en place pour assurer la conservation des logs les plus récents en cas d'augmentation de la volumétrie imprévue.</p>

LOG015 : Mise à disposition des traces	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Toutes les traces générées par les composants du système d'information doivent être à la disposition de la DAP.</p>

LOG016 : Protection des accès aux traces métier	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>L'accès aux traces métier des systèmes d'information de la DAP doit être protégé et strictement contrôlé, particulièrement pour les traces concernant les informations et les fonctions les plus sensibles (de niveau T2 et supérieur, cf <i>métrique sécurité DAP [DAP-METR-SSI] [RI.58]</i>).</p> <p>Ainsi l'accès est accordé sur autorisation explicite consignée du propriétaire concerné (i.e. le chef d'établissement) ou du RCSSI de l'administration pénitentiaire. Ceux-ci peuvent donner explicitement une délégation pour la réalisation technique de l'accès à la trace (tel au CLSI pour le chef d'établissement).</p> <p>Dans tous les cas, le propriétaire concerné et le RCSSI de l'administration pénitentiaire sont informés de manière formelle de l'accès à la trace demandée.</p> <p>L'accès aux traces métier ne doit pas permettre leur altération par la personne réalisant l'action de récupération d'une trace. Les rôles/profils utilisés pour l'accès aux traces doivent être complètement dédiés à cette tâche et être affectés à des comptes nominatifs.</p>

LOG017 : Protection des accès aux traces techniques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> </div> <p> L'accès aux traces techniques des systèmes d'information de la DAP doit être protégé et strictement contrôlé, particulièrement pour les traces concernant les informations et les fonctions les plus sensibles (de niveau T2 et supérieur) conformément à la <i>procédure de demande d'accès aux traces</i> [DAP-DDE-TRACES] [RI.25]. </p> <p> Ainsi l'accès est accordé sur autorisation explicite consignée du propriétaire concerné (i.e. le chef d'établissement) ou du RCSSI de l'administration pénitentiaire. Ceux-ci peuvent donner explicitement une délégation pour la réalisation technique de l'accès à la trace (tel au CLSI pour le chef d'établissement). </p> <p> Dans tous les cas, le propriétaire concerné et le RCSSI de l'administration pénitentiaire sont informés de manière formelle de l'accès à la trace demandée. </p> <p> L'accès aux traces techniques ne doit pas permettre leur altération par la personne réalisant l'action de récupération d'une trace. Les rôles/profils utilisés pour l'accès aux traces doivent être complètement dédiés à cette tâche et être affectés à des comptes nominatifs. </p>	

LOG018 : Processus d'accès aux traces	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </div> <p> Une liste de profils habilités à faire une demande d'accès à des traces techniques ou métier, ainsi que les utilisateurs en mesure d'approuver cette demande doit être disponible. </p> <p> Cette liste basée sur le <i>modèle</i> [DAP-DDE-TRACES] [RM.20] doit être revue au minimum annuellement et sanctionnée par un <i>PV</i> [DAP-PVR-TRACES] [RM.23]. </p>	

3.3.8 Revue des droits d'accès utilisateurs

GAC001 : Mise à disposition des droits d'accès sur le système de sureté		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	À tout moment, la DAP doit pouvoir avoir accès sur demande au récapitulatif des droits configurés sur l'ensemble des SI.	

GAC002 : Revue des droits d'accès		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<p>Une revue des droits d'accès et des comptes utilisateurs doit être menée régulièrement, soit :</p> <ul style="list-style-type: none">• Au moins une fois par an pour les utilisateurs sans droits administrateurs particuliers ;• Au moins tous les six mois pour les administrateurs des applications ou des serveurs sensibles. <p>Cette <i>revue</i> doit donner lieu à un <i>PV</i> basé sur le modèle [DAP-PVR-COMPTES] [RM.19.1] accompagné de son annexe [DAP-PVA-COMPTES] [RM.19.2].</p>	

GAC003 : Audit des comptes à privilèges		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<p>Pour les comptes système, un audit régulier au sein des SI doit être effectué. Cet audit doit permettre de repérer les comptes qui ne sont plus utilisés et ceux qui ont des privilèges élevés. La fréquence de cet audit sera précisée dans les directives de sécurité propres au système et seront dépendantes du besoin de sécurité de ce système.</p>	

GAC004 : Restitution de l'audit des comptes à privilège élevés		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<p>La liste issue de cet audit doit être présentée au responsable de la gestion de ces droits associés aux comptes pour être étudiée et ainsi s'assurer de la justification des comptes existants et des droits associés.</p> <p>A l'issue de l'audit, un PV basé sur les modèles [DAP-PVR-COMPTES] [RM.19.1] accompagné de son annexe [DAP-PVA-COMPTES] [RM.19.2] doit être établi afin d'approuver que tous les comptes ont été traités. Ce PV doit être remis au Chef d'établissement avec une copie à la DISP.</p> <p>La DAP doit être informée et avoir la capacité d'accéder à ces informations.</p>	

3.3.9 Politiques d'utilisation des mesures cryptographiques

CRY001 : Respect du référentiel général de sécurité		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	Tout élément relatif à l'utilisation de mesures cryptographique sur tout ou partie du périmètre du système d'information doit respecter le <i>référentiel général de sécurité [RGS] [RRG.01]</i> .	
CRY002 : Réalisation d'analyses de risque		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	La DAP doit réaliser des analyses de risque génériques pour chaque SI de sureté afin de déterminer les données à chiffrer.	
CRY003 : Chiffrement des supports		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	Les informations doivent être chiffrées conformément aux analyses de risques de la DAP (un disque dur entier, une partition, un conteneur, certains fichiers, des données d'une base de données, un canal de communication, un support amovible...) en fonction de la sensibilité des données.	
CRY004 : Solutions de chiffrement référencées		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	Les solutions de chiffrement utilisées devront être référencées dans le <i>cadre de cohérence technique (CCT) [DAP-CCT] [RI.54]</i> . L'utilisation d'un produit non présent au catalogue devra faire l'objet d'une demande de dérogation argumentée et motivée adressée au RCSSI.	
CRY005 : Contrôle des mesures cryptographiques		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	Un contrôle permettant de vérifier que les <i>mesures cryptographiques</i> sont toujours au niveau de sécurité recommandé par l'ANSSI [ANSSI-G-EIDAS] [RD.09] doit être effectué annuellement.	

CRY006 : Procédure de recouvrement des secrets	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	L'intégrateur doit réaliser une procédure pour assurer le recouvrement des secrets (mots de passe administrateurs, CD de recouvrement, ...) pour chaque système. Celle-ci doit être validée par le RCSSI de la DAP.

CRY007 : Mécanisme de séquestre	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Lorsqu'un besoin opérationnel ou des obligations juridiques (notamment de réquisition judiciaire) l'exigent, une mise sous séquestre des clés de déchiffrement permettant leur recouvrement doit être utilisée.


CRY008 : Conformité de l'utilisation des certificats	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	L'utilisation de certificat doit être conforme aux préconisations du référentiel <i>général de sécurité (RGS)</i> [RGS] [RRG.01] .


3.4 Contrôle d'accès

3.4.1 Exigences générales en matière de contrôle d'accès

Le contrôle d'accès nécessite l'identification et l'authentification de tous les acteurs du SI, la détermination des droits et privilèges consentis à chaque entité. Le RCSSI de la direction de l'administration pénitentiaire doit veiller à limiter l'accès aux informations, ressources ou SI placés sous sa responsabilité aux seuls utilisateurs autorisés. Les utilisateurs ne doivent avoir accès qu'aux informations, ressources, systèmes, applications, transactions ou fonctions qu'ils sont en droit de connaître ou de mettre en œuvre compte tenu de leurs attributions, habilitation de sécurité et besoin d'en connaître.

GAC010 : Utilisateurs des systèmes d'information de sûreté	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Seuls les agents ou les prestataires de la DAP peuvent-être utilisateurs des systèmes d'information de sûreté. L'utilisation de ces SI par toute Personne Placée Sous Main de Justice (PPSMJ) est de ce fait formellement proscrite.













GAC011 : Gestion des accès au SI	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>La politique d'accès des utilisateurs doit respecter des principes fondamentaux :</p> <ul style="list-style-type: none"> • tout ce qui n'est pas explicitement autorisé est interdit • respect « du moindre privilège » nécessaire à la stricte réalisation de son activité quotidienne et sur le « besoin d'en connaître » liés à sa fonction • mise en œuvre autant que possible d'une séparation des tâches sensibles entre les utilisateurs du système (afin de réduire les risques de mauvais usages, qu'il s'agisse d'une négligence ou d'un acte délibéré). <p>Pour l'exemple, un utilisateur qui pour son besoin métier peut endosser un rôle d'administrateur fonctionnel mais également d'utilisateur classique sur un même SI, devra utiliser des comptes d'accès différenciés pour ces deux activités aux périmètres distincts. De même, un rôle d'administrateur fonctionnel doit limiter son champ d'activité à la seule administration fonctionnelle et ne pas cumuler les droits d'un utilisateur sans privilège.</p>

GAC012 : Accès distant aux systèmes d'information de sûreté	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Par défaut, l'accès distant sur un système d'information de la DAP n'est pas autorisé. L'autorisation d'accès distant sur un système d'information de la DAP doit être systématiquement étudié pour chaque système d'information dans le cadre de l'analyse de risque en fonction de la criticité du système et des mesures de protection mises en œuvre.</p> <p>L'autorisation d'accès distant doit être étudié <i>a minima</i> pour les cadres suivants :</p> <ul style="list-style-type: none"> • Télétravail ; • Permanenciers, incluant : <ul style="list-style-type: none"> ◦ Permanences fonctionnelles/métier ; ◦ Permanences techniques/exploitation informatique ; • Agents mis à disposition d'autres services ; • Nomadisme ; • Assistance ou exploitation à distance (si applicable).

3.4.2 Gestion des accès utilisateurs

GAC020 : Authentification systématique et nominative des utilisateurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>L'authentification des utilisateurs et des opérateurs du système d'information doit être systématiquement mise en œuvre pour la totalité des accès, que ces accès concernent les données, les traitements ou les ressources.</p> <p>Chaque utilisateur doit posséder un compte d'accès unique et nominatif qui dispose des droits et privilèges strictement nécessaires à son profil sur les applications et les systèmes.</p> <p>Au niveau des zones où les applications sont fonctionnelles 24h/24 et où une authentification nominative n'est pas possible à cause des contraintes métier (ex : supervision), des mesures compensatoires permettant d'identifier les utilisateurs ayant menés des actions via un compte générique sur le système de sûreté doivent être mises en place (ex : caméra dans le local).</p> <p>Un accès en écriture sur le système ou l'application ne doit être possible qu'avec une authentification nominative.</p>
GAC021 : Profils et matrice d'habilitation sur les SI	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </div>	<p>Des <i>profils d'habilitation</i> séparant les tâches et les domaines de responsabilité doivent être définis pour chaque système et application au niveau national conformément à la procédure [DAP-REV-HAB] [RI.13].</p> <p>L'intégrateur doit créer ces différents profils sur les systèmes et applications.</p> <p>L'exploitant doit affecter à chaque utilisateur, <i>tous les profils nécessaires à l'exécution de sa mission dans les SI auxquels il accède</i>, conformément au modèle [DAP-MHAB-SIS] [RM.12], rempli et validé par le chef d'établissement.</p> <p>Les non-conformités à la matrice nationale dues à des contraintes opérationnelles, devront être validées par la DAP.</p>
GAC022 : Exigence sur les comptes utilisateurs et leur attribution	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>Le compte d'accès doit respecter les exigences suivantes :</p> <ul style="list-style-type: none"> • Une traçabilité de la correspondance entre l'utilisateur et le compte dont il a l'usage doit être mise en œuvre ; • Les comptes génériques temporaires sans utilisateur attribué doivent être impérativement désactivés. • Être conforme à la procédure [DAP-REV-HAB] [RI.13] émise par la DAP • Être affecté aux différents profils d'habilitation pour les SI dont il a besoin dans une matrice instanciée sur la base du modèle [DAP-MHAB-SIS] [RM.12].

GAC023 : Restriction des accès aux postes de travail	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<p>L'accès physique aux postes de travail de sûreté doit être restreint aux seules personnes autorisées (dispositif physique assurant la restriction d'accès au local contenant le poste).</p> <p>Si l'accès ne peut pas être protégé (ex : zone de détention), une autorisation explicite du RCSSI de la DAP doit être réalisée.</p>
GAC024 : Attribution des autorisations aux utilisateurs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<p>Le responsable hiérarchique d'un utilisateur attribue fonctionnellement les droits nécessaires à l'exercice de sa mission.</p> <p>La gestion des droits est réalisée par profil (groupe d'utilisateurs) et non par utilisateur lorsque la fonction est disponible.</p> <p>L'attribution technique des droits métiers doit être redondée sur plusieurs utilisateurs pour gérer les absences.</p> <p>Si des besoins de privilèges particuliers sont nécessaires et n'ont pas été qualifiés, un environnement spécifique doit être mis en œuvre pour réaliser cette tâche (environnement de développement, de tests, etc.).</p> <p>Si les accès nécessaires ne sont pas conformes à la procédure [DAP-REV-HAB] [RI.13], une validation de la DAP est nécessaire pour justifier l'exception.</p>
GAC025 : Gestion des changements de fonction des arrivées et des départs	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<p>Les exploitants des comptes systèmes, applicatifs ou bureautique de la DAP doivent procéder à la modification du compte nominatif d'un utilisateur, à sa désactivation ou à sa suppression après un changement de poste ou d'emploi ou après le départ de l'utilisateur de la DAP.</p>

GAC026 : Gestion des manquements aux exigences liées aux suppressions de comptes	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Une désactivation ou une suppression toujours non effective 3 mois après le départ de l'utilisateur concerné doit être considéré comme un incident de sécurité auprès du RCSSI.</p> <ul style="list-style-type: none"> ce délai avant incident peut être réduit en fonction des privilèges de l'utilisateur ou des circonstances de son départ. pour les droits ouverts sur les applications critiques et sensibles, la suppression des droits doit être immédiate au départ de l'agent.
GAC027 : Revue des comptes	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Chaque trimestre une <i>revue des comptes</i> menée par la DAP et par les sous-traitants, formalisée par une <i>procédure d'exploitations sécurisée (PES)</i> [DAP-REV-COMPTES] [RI.53] doit être consolidée par un représentant le plus proche de la chaîne SSI (RISSI en région, RCSSI en central).</p> <p>Cette <i>revue</i> doit donner lieu à un <i>PV</i> basé sur le modèle [DAP-PVR-COMPTES] [RM.19.1] accompagné de son annexe [DAP-PVA-COMPTES] [RM.19.2].</p>
GAC028 : Règles d'ouverture de session	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les processus de connexion à un système ou une application doivent respecter les règles suivantes :</p> <ul style="list-style-type: none"> En cas d'échec de connexion, la raison précise de cet échec doit être tracée sans afficher à l'utilisateur si le compte existe (« mot de passe invalide » doit être remplacé par « identifiant ou mot de passe invalide ») ; Des dispositifs doivent être mis en place pour limiter le nombre de tentatives de connexion, par exemple : bloquer, au moins temporairement, le compte utilisateur après cinq échecs de connexion.
GAC029 : Durée maximale de validité d'une session	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>En fonction des rôles, des comptes et des contraintes, une session authentifiée doit disposer d'une durée maximale de validité.</p> <p>Il est ainsi recommandé de forcer la réauthentification des utilisateurs après une période adaptée au cas d'usage.</p>

GAC030 : Gestion des comptes pour les utilisateurs présents de façon temporaire

Réf. GRC : non implémenté

ISO27002:2022 : non référencé



L'ouverture d'un compte pour les utilisateurs présents de façon temporaire (exemple : contrat à durée déterminée) est attribuée pour la durée du contrat et renouvelée si nécessaire.

GAC031 : Usage et privilèges des comptes génériques

Réf. GRC : non implémenté

ISO27002:2022 : non référencé



Les comptes génériques ne doivent pas avoir de privilège d'administration et doivent être clairement documentés.

Les postes utilisés avec des comptes génériques doivent être configurés en mode kiosk, ne permettant l'accès qu'aux applications nécessaires.

Les comptes génériques techniques et fonctionnels doivent être assignés aux seuls groupes de personnes autorisés, leur utilisation doit être strictement encadrée.

GAC032 : Compte par défaut des systèmes Windows

Réf. GRC : non implémenté

ISO27002:2022 : non référencé



Sur les postes avec un système d'exploitation Windows, il existe par défaut un compte administrateur local, permettant des tâches d'administration sur le poste de manière locale.

Son mot de passe par défaut doit être changé, ce compte désactivé, un nouveau compte administrateur local créé et ce nouveau couple compte/mot de passe doit être stocké sous scellé à la responsabilité de la DAP.

Son utilisation doit pouvoir être détectée.

GAC033 : Usage et privilèges des comptes de service

Réf. GRC : non implémenté

ISO27002:2022 : non référencé



Des comptes de service pour les processus automatiques doivent être mis en place.

Les privilèges des comptes de services doivent être limités au maximum et sans privilège d'administration.

3.4.3 Gestion des accès à privilèges




GAC040 : Attribution des privilèges administrateurs		
Réf. GRC : non implémenté	ISO27002:2022 : non référencé	
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	L'attribution d'habilitations ou de privilèges administrateurs doit faire l'objet d'une procédure d'exploitation sécurisée (PES) en fonction de chaque SI impliquant la validation formelle du responsable de l'exploitation et garantissant une journalisation.	




GAC041 : Authentification à double facteur des accès d'administration		
Réf. GRC : non implémenté	ISO27002:2022 : non référencé	
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Une authentification à double facteur doit régir les accès d'administration des systèmes de sûreté.	

GAC042 : Authentification à double facteur des accès distants		
Réf. GRC : non implémenté	ISO27002:2022 : non référencé	
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Une authentification à double facteur doit régir les accès distants réalisés depuis un autre site. Le système de gestion à distance doit être conforme aux exigences de la règles 18 de l'Arrêté du 23 décembre 2021 fixant les règles de sécurité et modalités de déclaration des SIIV et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Activités judiciaires » relative aux accès distants [Arr-SIIV-Jud] [RL.01] .	




GAC043 : Gestion des comptes utilisateurs et administrateurs		
Réf. GRC : non implémenté	ISO27002:2022 : non référencé	
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Les utilisateurs/administrateurs doivent disposer d'un compte sans privilège (non-administrateur) sur leur poste de travail. Si besoin, un second compte peut être affecté à un utilisateur avec plus de privilèges.	


GAC044 : Autorisation d'accès avec privilèges élevées aux systèmes		
Réf. GRC : non implémenté	ISO27002:2022 : non référencé	
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Les autorisations d'accès sur un système en production nécessitant des privilèges systèmes élevés, données à un utilisateur, doivent être justifiées (activité de support, de maintenance ou d'administration des systèmes).	


GAC045 : Règles à suivre pour guider l'attribution des droits	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les règles suivantes doivent être suivies pour donner les autorisations à un utilisateur :</p> <ul style="list-style-type: none"> les accès privilégiés ne doivent être donnés qu'en vertu du strict besoin de la fonction ou de la mission ; les privilèges associés aux logiciels de base (par exemple système d'exploitation, SGBD ...) et les catégories de personnels qui y ont accès doivent être identifiés ; les comptes privilégiés ne doivent pas être utilisés lorsque d'autres solutions de moindres privilèges sont possibles ; autant que possible, des processus doivent être mis en œuvre pour minimiser l'utilisation des comptes privilégiés, et des comptes moins privilégiés doivent être utilisés pour l'activité quotidienne ; l'utilisation de ces comptes doit pouvoir être audité à tout moment, à la suite d'un incident ou dans le cas d'un contrôle inopiné (pour s'assurer que seules les personnes dont la fonction le justifie ont des accès privilégiés).


GAC046 : Distinction des droits entre comptes utilisateurs et comptes à privilèges	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Un utilisateur final ne doit pas avoir accès à des comptes privilégiés, et ainsi un utilisateur n'assumant pas des fonctions d'administration ne doit en aucun cas posséder des droits privilégiés sur une application ou système.</p>

3.4.4 Gestion des mots de passe


GAC050 : Unicité des mots de passe	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Les mots de passe doivent être différents entre les différents systèmes et applications (sauf en cas d'utilisation d'annuaire centralisé).</p>


GAC051 : Confidentialité des authentifiants utilisateur	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	Les mots de passe et autres secrets (code PIN, passphrase, clef privée...) sont strictement personnels et ne doivent en aucun cas être divulgués à un tiers, y compris l'exploitant en charge de la gestion de l'application.

GAC052 : Durée de vie des mots de passe	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	Les mots de passe ont une durée de vie maximale, telle que définie dans la <i>politique de mots de passe</i> de l'application ou à défaut de la DAP [MJ-DAP-MDP] [RI.26] .

GAC053 : Stockage des mots des passes sur les systèmes et applications	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	Les mots de passe doivent être stockés sous forme chiffrée avec un sel dans les applications avec l'utilisation impérative d'algorithmes de chiffrement à sens unique (ou fonctions de hachage) conforme à la <i>politique de mots de passe</i> [MJ-DAP-MDP] [RI.26] .

3.4.5 Gestion des comptes génériques

GAC060 : Initialisation et renouvellement des mots de passe des comptes génériques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les mots de passe des comptes génériques doivent être initialisés à la réception de chaque SI et renouvelés conformément à la <i>politique de mot de passe</i> de la DAP [MJ-DAP-MDP] [RI.26].</p> <p>Certains systèmes peuvent nécessiter une politique de mots de passe spécifique (exemple : fréquence de renouvellement plus importante en raison de la sensibilité de l'application).</p>

GAC061 : Changement des mots de passe des comptes génériques à la livraison du système	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les mots de passe des comptes génériques doivent être modifiés par l'exploitant avant la mise en service du système livré par l'intégrateur.</p> <p>Ils doivent répondre à la politique de mot de passe de chaque SI et doivent être stockés de façon sécurisée après leur initialisation.</p>

3.5 Acquisition et développement des systèmes d'information

La sécurité doit être intégrée au cycle de vie du SI, de la conception au décommissionnement effectif de celui-ci.

Dans le développement du SI, la prise en compte de la sécurité est réalisée à l'initialisation du projet, y compris en mode Agile afin d'éviter des modifications, des surcoûts, des baisses de performances ou des limitations d'emploi.

Afin de s'assurer que les équipements ou prestations de services acquises par les entreprises cotraitantes et sous-traitantes du système d'information auprès de prestataires externes sont conformes ou compatibles avec cette PSSI, le RCSSI de la direction de l'administration pénitentiaire s'assure que les conditions générales d'achat intègrent bien les différents besoins de sécurité de la PSSI en vigueur.

Le RCSSI de l'administration pénitentiaire doit aussi s'assurer que les exigences de sécurité sont présentes dans les divers cahiers des charges rédigés par les parties prenantes du prestataire en vue de l'acquisition de tout équipement ou prestation de service susceptible d'avoir un impact sur les informations, ressources ou SI relevant du projet.

L'analyse des offres contient de manière systématique une partie SSI et protection des données. Elle est prise en compte dans le choix du prestataire.

3.5.1 Standardisation et homogénéisation des solutions techniques




ACQ001 : Cadre de cohérence technique (CCT)	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> </div> <p> L'administration pénitentiaire doit élaborer et maintenir à jour le référentiel [DAP-CCT] [RI.54], dont le but est de standardiser, harmoniser et industrialiser toutes les solutions permettant de rendre le service attendu par les SI. </p> <p> Il adresse la liste consolidée des matériels, logiciels et fournisseurs strictement nécessaires à l'activité et doit être approuvé par le RCSSI de la DAP. </p> <p> Le choix et l'installation de nouveaux matériels, composants ou moyens logiciels dans les bureaux, salles techniques et informatiques doivent figurer dans le <i>référentiel [DAP-CCT] [RI.54]</i> de la DAP. </p> <p> Le CCT fait état du respect de la propriété intellectuelle en mentionnant <i>a minima</i> le type de licence et l'éditeur du logiciel concerné. </p> <p> Par ailleurs, un suivi des versions supportées par chaque éditeur ou constructeur doit permettre de prévoir et planifier en anticipation les montées de versions ou changement de matériel (suivi de l'obsolescence). </p>	

ACQ002 : Mise à jour du CCT et dérogation	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>L'intégrateur contribue à la mise à jour du CCT avec la validation de la DAP.</p> <p>L'utilisation d'un produit ou d'un service non présent au CCT (labellisé ou non), devra faire l'objet d'une demande de dérogation argumentée et motivée adressée au RCSSI de la DAP.</p> <p><i>In fine</i>, ce produit ou ce service pourra être logiquement intégré au CCT après validation du RCSSI de la DAP.</p>

ACQ003 : Instruction des besoins métiers	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Tous les besoins métiers doivent être centralisés à la DAP, pour être instruits et évalués, conformément à la <i>procédure</i> [DAP-CHMG] [RI.52].</p> <p>La procédure de gestion du changement permet d'adresser dans l'ordre et <i>a minima</i> :</p> <ul style="list-style-type: none"> • La pertinence du nouveau besoin métier exprimé (périmètre d'applicabilité et impacts organisationnel le cas échéant) ; • La faisabilité technique pour y répondre ; • Les impacts SSI et Informatique et Libertés, le cas échéant. <p>Tous ces points seront consolidés et adressés au travers de la <i>fiche</i> [DAP-FEB] [RI.17].</p>

3.5.2 Sécurité des développements et logiciels




DEV001 : Centralisation du développement au niveau de la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Les développements d'applications doivent être centralisés au niveau de la DAP pour les SI métier comme pour les SI de sûreté. La DAP, si elle s'appuie sur des prestataires externes pour ces développements ou un éditeur pour des adaptations spécifiques sur un logiciel, assurera alors le contrôle de l'application des exigences de la présente PSSI par le prestataire ou l'éditeur.</p>




DEV002 : Développement d'application en local	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Un besoin local ne doit pas conduire à un développement spécifique non validé par la DAP.</p> <p>Tout outil d'automatisation et d'industrialisation de fonctions d'exploitation par l'exploitant qui aurait été réalisé localement doit être remontée auprès de la DAP afin d'être évalué en termes de sécurité et de couverture du besoin fonctionnel.</p> <p>Si cette solution est validée, elle pourra être intégrée dans le processus d'exploitation (une mise à jour des documents d'exploitation) et partagé avec tous les exploitants. À défaut, elle sera refusée (décision motivée) et son usage bloqué.</p>
DEV003 : Application des bonnes pratiques de développement	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les développeurs de logiciels intègrent les règles et les bonnes pratiques conformément à la <i>procédure</i> [DAP-DEV-SEC] [RI.37].</p>
DEV004 : Cycle de mise en production	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les environnements de développement, de test et d'exploitation doivent être distincts conformément à la <i>procédure</i> [DAP-CYCL-VIE] [RI.62.2].</p>

DEV005 : Contrôle d'intégrité du code avant livraison	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>L'intégrité des codes exécutables, scripts, configurations, bases de données des applications jugées sensibles devra pouvoir être vérifiée (HASH, signature électronique, chiffrement) entre le développeur ou intégrateur jusqu'au déploiement sur l'environnement de production de la DAP.</p> <p>Les mesures mises en œuvre devront permettre de détecter toute perte d'intégrité sur une livraison.</p>
DEV006 : Environnement de développement dédié	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Les développements doivent être effectués dans un environnement distinct de celui de la production.</p>
DEV007 : Utilisation des données réelles hors production	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>L'utilisation de données réelles est interdite en dehors de l'environnement de production.</p> <p>Pour un besoin spécifique de ce type de données en dehors de l'environnement de production, les règles ci-dessous doivent être observées :</p> <ul style="list-style-type: none"> les règles de confidentialité des données doivent être appliquées, ces règles définies pour chaque application doivent être validées par le RCSSI de la DAP ; la législation sur les informations à caractère personnel doit être respectée et les données réelles utilisées ne doivent être accessibles qu'aux seuls personnels autorisés pour ce type de données.
DEV008 : Jeux de données de développement et anonymisation des données de production	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Durant les phases de développements et de tests, toutes les recettes se font sur des jeux de données spécifiques aux environnements.</p> <p>Les données de production qui seraient importées dans d'autres environnements doivent être au préalable anonymisées.</p>




3.6 Gestion des incidents




3.6.1 Responsabilité et procédures




GDI001 : Processus de traitement des incidents et de crise	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Sous la responsabilité du Directeur de l'Administration Pénitentiaire, le RCSSI de la DAP établit et maintient une capacité à traiter les incidents de sécurité de façon centralisée.</p> <p>Ceci implique qu'il met en œuvre un processus de traitement des incidents de sécurité sur tout le SI de son périmètre de responsabilité, qui inclut les activités de préparations, de détection, d'analyse, d'endiguement et de rétablissement des systèmes et réseaux.</p> <p>Il trace, documente et rend compte des incidents aux autorités et aux services appropriés conformément à la réglementation en vigueur.</p> <p>Pour atteindre cette mission, il contrôlera et s'appuiera sur les processus de traitement des incidents et de crise définis au niveau de chaque site en s'inscrivant dans le processus de gestion de crise global de la DAP et ministériel.</p>
GDI002 : Formalisation des procédures de traitement des incidents et de gestion de crise	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Les procédures de traitement des incidents et de gestion de crise [DAP-GEST-INC] [RI.30] doivent être formalisées et conformes au <i>décret du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics</i> [Dec-SecNumEP] [RRG.05].</p> <p>Cela comprend des actions préventives pouvant aller jusqu'à l'isolation réseau des SI subissant l'incident et curatives pour rétablir les services du SI impacté.</p>
GDI003 : Outillage associé à la gestion de crise	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>L'organisation de crise nécessite des infrastructures SI pour son bon fonctionnement, dont en particulier les moyens de communication tels que des accès téléphoniques directs (hors PBX), dont une ligne sécurisée RIMBAUD, un accès au RPVJ et au service de messagerie, des postes fixes et/ou nomades contenant les plans de continuité (également présents au format papier), et si possible des moyens de visioconférence.</p> <p>La salle de crise doit ainsi être choisie judicieusement pour pouvoir être réquisitionnée à tout moment tout en assurant la disponibilité et une protection des moyens de crise pour qu'ils ne soient pas accédés, avec le risque d'être altérés, en dehors de la mobilisation de la cellule de crise (salle à accès restreint fermée à clef, armoire sécurisée protégeant les accès réseaux et les équipements de crise).</p>




GDI004 : Activation des plans de continuité	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	Le responsable de la cellule de crise prend la décision d'activation des plans de continuité si nécessaire, conformément au processus de gestion d'incident.

3.6.2 Signalement des événements liés à la sécurité de l'information




GDI010 : Détection d'incident par un utilisateur externe	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	Dans le cas d'incidents détectés sur les ressources utilisées par un utilisateur externe de la DAP, ce dernier doit conjointement prévenir sa hiérarchie et la chaîne fonctionnelle SSI de sa société ainsi que de la DAP.




GDI011 : Traitement et traçabilité des incidents	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Tout incident sur le système d'information, quel que soit son niveau de gravité, doit donner lieu à une déclaration dans un outil dédié conformément à la <i>procédure de gestion des incidents</i> [DAP-GEST-INC] [RI.30].</p> <p>L'exploitant doit également disposer d'une procédure interne de gestion de crise et des incidents qui doit être communiquée sur demande au RCSSI de la DAP.</p> <p>Une estimation du niveau de gravité de l'incident doit être réalisée sur la base des <i>métriques de sécurité</i> de la DAP [DAP-METR-SSI] [RI.58].</p> <p>Dans le cas d'un incident de sécurité, le RCSSI de la DAP doit être informé sans délais.</p>




GDI012 : Procédure de gestion d'équipements compromis	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	En cas de suspicion de compromission d'un équipement, la <i>procédure de gestion d'un élément compromis</i> [DAP-GEST-COMPRO] [RI.23] doit être respectée.

GDI013 : Mise en place d'un service de détection qualifié PDIS	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Un service de détection qualifié PDIS doit être mis en place et viser à :</p> <ul style="list-style-type: none"> • Détecter les tentatives d'attaque et les attaques réussies. • Permettre une réaction rapide en cas de compromission afin d'en limiter le périmètre et l'impact ; • Générer et remonter des traces permettant de réaliser des investigations a posteriori en cas d'incident (alertes, métadonnées, etc.) ;

3.6.3 Réponse aux incidents liés à la sécurité de l'information

GDI020 : Mobilisation de la chaîne SSI en cas de crises des SI de sûreté	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Tous les correspondants SSI directement concernés par une crise touchant la sécurité des systèmes de sûreté doivent être mobilisés.</p>

GDI021 : Mobilisation de l'exploitant en cas de crise	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>L'exploitation doit participer à l'activation d'une Cellule situation anticipation (CSA) touchant à la sécurité des SI.</p>

GDI022 : Collecte, conservation et protections des preuves en cas d'incident	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>En cas d'incident de sécurité, la DAP peut être amenée à collecter, conserver, protéger et présenter des éléments de preuves.</p> <p>Celles-ci peuvent être utilisées afin de prendre des mesures contre une personne ou une organisation.</p> <p>Si les mesures prises contre une personne ou une organisation après un incident de sécurité impliquent des procédures judiciaires, les éléments de preuve doivent être collectés, conservés, protégés et présentés conformément aux règles en vigueur.</p>

GDI023 : Réalisation de l'investigation numérique par un prestataire PRIS		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	En cas d'incident, la DAP doit faire appel à un prestataire de réponse aux incidents de sécurité qualifié (PRIS), afin de réaliser une investigation numérique sur le périmètre.	

3.6.4 Capitalisation des incidents liés à la sécurité de l'information

GDI030 : Création d'une base d'incidents et capitalisation		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Une base d'incidents doit être créée afin de mutualiser les connaissances et de bénéficier d'un retour d'expérience, cela inclue des bilans à chaud, à froid ainsi que des plans de recommandations.</p> <p>Ces informations doivent être utilisées pour identifier les incidents récurrents et/ou aux conséquences significatives.</p> <p>Afin de répondre aux incidents types, des fiches de procédures résultant des incidents précédents doivent être documentées.</p>	

GDI031 : Analyse des incidents		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Les incidents qualifiés comme étant significatifs doivent être analysés en termes de types, volumes et coûts, afin de les quantifier et de suivre leur évolution.	

GDI032 : Pilotage des indicateurs de suivi des incidents		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Un indicateur de suivi des incidents de sécurité est intégré au tableau de bord présenté mensuellement, au cours des comités de sécurité pilotés et animés par le RCSSI de la DAP.	

GDI033 : Remontées des capitalisations sur les incidents		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Les résultats de la capitalisation d'incidents doivent être remontés trimestriellement à la chaîne SSI et annuellement sous forme de tableaux de bord et de fiches de retour d'expérience.	

3.7 Gestion du plan de continuité et de reprise de l'activité

3.7.1 Introduction de la continuité et la reprise d'activité

Le RCSSI de la DAP collecte et vérifie les différents documents de chaque entité pour avoir une vision globale de la continuité et la reprise d'activité qu'il pilote, en tenant compte du contexte d'emploi et des risques qui pèsent sur le SI pour les réduire.

Les plans de continuité et reprise d'activité (PCA/PRA) sont un ensemble de plans prédéterminés et testés afin d'assurer la continuité des activités essentielles, consécutifs à un sinistre majeur (épidémie, inondation, séisme, incendie, etc.).

Il comprend classiquement des plans de continuité et reprise informatique (PCI/PRI), un plan de gestion de crise et un plan de continuité métier.

Les plans de secours informatique sont un sous-ensemble des PCA/PRA comprenant un ensemble de procédures et de moyens permettant de garantir le maintien des systèmes d'information dans des temps correspondants au besoin en disponibilité préalablement défini.

3.7.2 Plan de continuité et reprise informatique

3.7.2.1 Constitution du PCI/PRI

GCA001 : Définition et mise en œuvre des plans de secours informatique	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>La définition et la mise en œuvre des plans de continuité et reprise informatique des systèmes est réalisée avec le concours du centre compétence national, des intégrateurs, la validation des chefs d'établissements et de de leurs correspondants SSI (RCSSI, RISSI, correspondant local SSI), garants de la cohérence entre les PCI et les besoins métiers identifiés dans les PCA correspondants.</p> <p>Le plan de secours informatique, instancié sur la base du modèle [DAP-PCRI] [RM.30] doit en particulier prévoir :</p> <ul style="list-style-type: none"> • l'organisation des sauvegardes de secours (fréquence, méthode) dédiées aux besoins du PCI et leur externalisation concernant les SI sensibles pour pouvoir traiter les risques environnementaux ; • un SI de secours, distinct du SI principal de production et apportant un niveau de protection physique homogène avec celui du site de production principal ; -> à remplacer par une forte résilience du mono site ; • les priorités et la progressivité du rétablissement des services (compte tenu de la criticité de chacune des applications) ; • les procédures détaillées de secours et de reprise pour chacune des applications sensibles ; • les éventuelles inhibitions temporaires et acceptées (après analyse détaillée des justifications) de certains mécanismes de sécurité ou exigences des présentes PSSI ; • les mesures organisationnelles (gestion des personnels informatiques et sécurité, gestion des infrastructures, etc.) ; • la périodicité des tests.

GCA002 : Plan de secours pour les salles informatiques	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<div> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> </div>	<p>Toute salle informatique hébergeant des applications métiers ou des infrastructures sensibles (SIIV), doit disposer d'un <i>plan de continuité et reprise informatique</i> formalisé par l'exploitant et instancié sur la base du modèle [DAP-PCRI] [RM.30].</p>

GCA003 : Hébergement du matériel de reprise d'activité dans un Shelter		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<p>Le matériel de reprise d'activité en cas de sinistre du SI de sureté doit être localisé dans un Shelter (conteneur hébergeant un centre de données) à proximité des serveurs de production habituels s'il ne peut être hébergé dans les locaux de l'établissement (ex : contrainte logistique, manque de place).</p> <p>Une dérogation à cette exigence doit être validée par le RCSSI de la DAP.</p>	
GCA004 : Cas d'impossibilité d'externalisation du matériel de secours pour le PCI/PRI		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<p>Si le matériel de reprise d'activité se compose de moyens informatiques portables (bande de sauvegardes, procédure papier, ordinateur portable...) et que leur externalisation n'est pas possible, le lieu de stockage privilégié doit être un coffre ignifugé dans un bureau sécurisé (fermant à clef).</p>	
GCA005 : Prise en compte du DIMA dans les processus des plans de secours informatique		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<p>Les plans [DAP-PCRI] [RM.30] doivent prendre en compte les délais d'interruption maximums autorisés (DIMA) définis pour chaque système d'information.</p>	
GCA006 : Intégration des plans de secours informatique dans les procédures de sécurité		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div><div></div><div></div><div></div></div></div>	<p>Les procédures d'exploitation de l'exploitant du SI doivent intégrer les plans [DAP-PCRI] [RM.30].</p>	

3.7.2.2 Tests des plans de secours informatique

GCA010 : Test annuel des plans de secours informatique	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Les plans [DAP-PCRI] [RM.30] doivent être testés au minimum annuellement.

GCA011 : Consignation des résultats des tests et retour d'expérience	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Les résultats des tests des <i>plans</i> [DAP-PCRI] [RM.30] font l'objet d'un compte rendu détaillé consigné dans un PV.</p> <p>Chaque campagne de test doit faire l'objet d'un « retour d'expérience », afin de faire évoluer ces plans pour optimiser leur fonctionnement. Ces éléments doivent être mis à disposition de la chaine SSI de la DAP.</p>

3.7.2.3 Sensibilisation du personnel aux procédures de secours informatique

GCA020 : Sensibilisation du personnel aux plans de secours informatique	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	La sensibilisation et la formation des agents et collaborateurs concernés par les plans [DAP-PCRI] [RM.30] sont de la responsabilité du RCSSI de la DAP.

3.7.3 Plan de continuité et reprise d'activité

GCA030 : Détermination des risques d'interruption des services de la DAP		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>Les mesures prises pour la continuité et la reprise d'activité (PCA/PRA) doivent être basées sur l'identification des événements redoutés pouvant interrompre les processus internes de l'administration pénitentiaire.</p> <p>Une analyse de risques doit ainsi déterminer les probabilités et les conséquences de ces événements sur la sécurité de l'information.</p>	

GCA031 : Intégration de l'informatique dans les plans de continuité et de reprise d'activité		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>Les plans de continuité et de reprise d'activité intègrent un volet de plan [DAP-PCRI] [RM.30].</p> <p>Ils doivent être formalisés et actualisés a minima tous les 3 ans.</p>	













GCA032 : Intégration des évolutions architecture techniques aux plans de secours		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>Les évolutions d'architecture ou de configuration doivent faire l'objet de tests pour garantir le maintien de l'efficacité et la non-régression du PCA/PRA.</p> <p>Ces exercices peuvent conduire à une amélioration des PCA/PRA.</p>	

GCA033 : Responsable central du processus de gestion du plan de secours		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>Un responsable central du processus de gestion des plans de continuité et reprise doit être désigné.</p>	





GCA034 : Pilotage des tests des plans de secours		
Réf. GRC : non implémenté		ISO27002:2022 : non référencé
<div><div></div><div></div><div></div></div>	<p>Les tests des plans de secours (PCA/PRA) ayant un impact sur la détention doivent faire l'objet d'un pilotage global de la part du chef d'établissement, sous couvert de la DI et de la DAP afin de les valider et les prioriser.</p> <p>Le RCSSI de la DAP doit être informé des dates de planification des tests.</p>	




3.8 Conformité




3.8.1 Conformité aux obligations légales et réglementaires




CNF001 : Cadre des exigences légales et réglementaires	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Le RCSSI doit identifier, documenter et mettre à jour explicitement toutes les exigences légales, réglementaires et contractuelles en vigueur applicables aux différents SI et à ses utilisateurs dans le cadre des exigences légales et réglementaires imputables au système d'information.</p> <p>Ce cadre des exigences doit être disponible dans le document <i>corpus documentaire référence</i> [MJ-DAP-REF] [RI.04].</p> <p>Une mise à jour de ce document doit être effectuée a minima annuellement et à chaque mise à jour majeure d'un référentiel.</p>
CNF002 : Droits de propriété intellectuelle des logiciels	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Tout code source développé pour le compte de la DAP est la propriété de la DAP.</p> <p>Les droits de propriété intellectuelle de tout logiciel installé et utilisé dans le système d'information doivent être respectés.</p>
CNF003 : Mesures de protection et de confidentialité des renseignements personnels	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Le responsable de traitement s'assure de la protection et de la confidentialité des données à caractère personnel (DCP).</p> <p>Le cadre réglementaire des DCP est défini au travers du <i>règlement général sur la protection des données (RGPD)</i> [RGPD] [RL.03], de la <i>loi informatique et liberté (LIL)</i> [L78-17-CNIL] [RL.04] et de la <i>directive Police-Justice</i> [DirPolJus] [RL.05].</p>
CNF004 : Homologation des SI de sûreté	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Tous les systèmes de sûreté doivent faire l'objet d'une homologation par l'ANSSI pour les SSIIV ou d'une homologation interne DAP pour les non SIIV en s'appuyant sur le <i>modèle de dossier</i> [DAP-DH] [RM.26].</p>




3.8.2 Audits

CNF011 : Mise à disposition des moyens de protection des SI des prestataires	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Sur demande, le prestataire doit mettre à disposition du RCSSI de la DAP les documents (dossier d'architecture, procédures...) décrivant les moyens de protection en place pour protéger toutes informations de la DAP, que ce soit sur son SI ou celui d'un partenaire qui assure l'hébergement.</p>
CNF012 : Audit des prestataires et de leurs partenaires d'hébergement	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Chaque prestataire s'engage à accepter d'être audité par la DAP ou tout tiers qualifié par elle, afin de vérifier le bon respect :</p> <ul style="list-style-type: none"> - des exigences de sécurité formalisées par la présente PSSI ; - des bonnes pratiques de sécurité (notamment la conformité avec les référentiels de sécurité de l'ANSSI). <p>Ces audits peuvent concerner le SI du prestataire ou de l'infrastructure d'hébergement chez un partenaire à qui il aura confié des données de la DAP.</p> <p>Ces audits sont préparés par le RCSSI de la DAP qui planifie les dates de l'audit avec son homologue chez le tiers. Les résultats sont communiqués aux deux parties.</p> <p>Le prestataire s'engage à garantir la disponibilité des ressources nécessaires afin de permettre à la DAP ou à l'organisme mandaté par celle-ci de mener un audit sur son organisation et son système dans les 3 mois suivant la demande d'audit de la DAP.</p> <p>Le prestataire doit préciser dans la convention de service qu'il s'engage à mettre à disposition toutes les informations nécessaires à la réalisation d'audits de conformité menés par la DAP ou tout tiers qualifié par elle.</p>
CNF013 : Contenu et diffusion des rapports d'audits	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Ces audits doivent faire l'objet de rapports incluant une synthèse managériale, les points de non-conformité ainsi qu'un plan de remédiation.</p> <p>Les résultats d'audits doivent être communiqués au minimum au RCSSI de la DAP, aux commanditaires et à l'exploitant concerné.</p>
CNF014 : Notification du RCSSI en cas de découverte de vulnérabilité critique lors d'un audit	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>En cas de vulnérabilité majeure découverte lors de l'audit, celle-ci doit faire l'objet d'une notification au RCSSI de la DAP dans les 24H suivant la découverte, sans attendre la livraison de l'audit final.</p>


CNF015 : Réalisation d'audit sur des SI hors périmètre de la DAP	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Pour réaliser des tests et audits sur des SI n'appartenant pas à la DAP, mais utilisés pour les applications pénitentiaires, une autorisation préalable de l'organisme « propriétaire » est nécessaire.</p> <p>Dans certains cas, les contrôles seront préparés conjointement et réalisés par l'organisme en question.</p>


CNF016 : Audit avant la mise en production	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Un audit doit être réalisé avant la mise en service de chaque système d'information de sûreté.</p> <p>Les audits peuvent porter sur :</p> <ul style="list-style-type: none"> • la revue de codes ; • la revue d'architecture ; • la revue de configuration ; • des tests d'intrusion ; • des processus techniques ou organisationnels.

CNF017 : Audit des logiciels et des données des systèmes sensibles	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Un audit régulier des logiciels et les données (traces, configurations...) des systèmes sensibles doit être réalisé afin de vérifier le non-contournement des politiques en place.</p> <p>L'organisation et la fréquence de ces audits devra faire l'objet d'une procédure de sécurité (PES) spécifique validée par la DAP.</p>

CNF018 : Mécanismes de contrôle interne	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
  	<p>Chaque système d'information est audité avant son homologation.</p> <p>Tous les ans, la mission de contrôle interne (MCI) évalue la conformité d'un SI au regard des référentiels réglementaires applicables identifiés dans le cadre de son homologation.</p>

3.8.3 Reporting

CNF020 : Tableaux de bords de l'état du niveau de sécurité des systèmes d'information	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Des tableaux de bords doivent présenter de façon périodique et régulière l'état du niveau de sécurité des systèmes d'information.</p> <p>La construction des tableaux de bords doit être automatisée et documentée.</p> <p>Elle pourra être réalisée manuellement uniquement en cas de contrainte technique majeure.</p>

CNF021 : Comité de suivi et de pilotage de la sécurité	
Réf. GRC : non implémenté	ISO27002:2022 : non référencé
	<p>Le responsable de la sécurité désigné par le prestataire prend en charge l'organisation de comités de suivi et pilotage de la sécurité. Ces comités devront être détaillés dans le document d'exploitation et être en cohérence avec le document interne de la DAP définissant le suivi de sécurité des systèmes de sureté, entre autres les points suivants seront à définir :</p> <ul style="list-style-type: none"> • fréquence de la tenue des comités • intervenants • ordre du jour (retour sur incidents, MCS, audits, évolution du contexte, sensibilisation des intervenants, revue des tableaux de bords ...). • livrables • template.