

**Direction de l’administration pénitentiaire**

**C.C.T.P. - ANNEXE 05 – PLAN D’ASSURANCE SÉCURITÉ**

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

1. **Sécurité des ressources humaines**
   1. **Recrutement**

*Indiquez si une attention particulière est liée au recrutement des personnes-clés de la SSI qui interviendront directement sur la sécurité de l’établissement (référent/expert sécurité local, responsable d’exploitation), précisez leur niveau de formation et s’ils sont régulièrement sensibilisés aux devoirs liés à leur fonction.*

* 1. **Gestion des départs et arrivées**

*Décrivez le processus de gestion des départs et arrivées des collaborateurs ainsi que des partenaires (gestion/révocation des comptes, droits d’accès au SI, gestion des habilitations, contrôle d’accès aux locaux, renouvellement des secrets associés aux comptes génériques etc.).*

* 1. **Sensibilisation et formation à la SSI**

*Décrivez le processus de sensibilisation des utilisateurs et administrateurs aux exigences de sécurité, indiquez s’ils sont formés à l’utilisation des outils conformément aux règles SSI, s’ils doivent se conformer à une charte informatique spécifique aux SI de Sûreté et les moyens permettant de garantir son application (annexe au contrat de travail, règlement intérieur, contrat de sous-traitance…)*

1. **Gestion documentaire et des biens**
   1. **Cartographie des actifs**

*Indiquez si une cartographie précise des SI sous exploitation est maintenue à jour au fil des évolutions.*

* 1. **Documentation**

*Indiquez si l’architecture des systèmes d’information est décrite et formalisée à travers des dossiers techniques, si les configurations sont documentées et maintenus au fil des évolutions apportées aux différents SI et si la documentation initiale présente dans les DOE fait l’objet de mises à jour lorsque nécessaire.*

* 1. **Procédures**

*Indiquez si l’ensemble des processus (métier, exploitation, administration, accès, contrôle, PCA, MCS…) fait l’objet de documentations accessibles et mises à jour en fonction des incidents rencontrés et de l’évolution des systèmes.*

*Indiquez également les processus de gestion des procédures (stockage, approbation, diffusion, révision).*

* 1. **Inventaire**

*Indiquez si un inventaire précis des ressources informatiques (composants matériels et logiciels, versions exactes) est réalisé et le cas échéant, précisez l’outillage permettant de réaliser sa tenue à mesure de l’évolution des différents SI.*

* 1. **Classification des informations**

*Indiquez si un processus d’évaluation de la sensibilité des données manipulées est présent et si un marquage systématique des documents est réalisé en fonction de leur niveau de sécurité.*

*Indiquez si les utilisateurs et administrateurs qui manipulent des données sensibles dans le cadre de leur fonction, assurent leur protection tout au long de leur cycle de vie, depuis la création du brouillon jusqu’à son éventuelle destruction.*

* 1. **Mise à jour du PAS**

*Indiquez si le PAS fait l’objet de mises à jour et avec quels critères (ex : nouvelles règles associées à un nouveau dispositif de sécurité, prise en compte d’incidents de sécurité nécessitant de nouvelles mesures…)*

1. **Gestion des accès logiques**
   1. **Droits d’accès aux ressources logiques**

*Indiquez si le contrôle d’accès s’appuie sur un processus formalisé en cohérence avec le rôle de l’exploitant, si les droits sont attribués selon les principes suivantes : besoin d’en connaître (chaque utilisateur n’est autorisé à accéder qu’aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l’accès), moindre privilège (chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui).*

* 1. **Gestion des habilitations logiques**

*Décrivez le processus de gestion des habilitations (qui attribue, révoque et contrôle les habilitations sur les différents SI de Sûreté).*

* 1. **Traçabilité des accès logiques**

*Indiquez si l’accès aux applications et systèmes, ainsi que l’attribution des habilitations font l’objet d’une traçabilité via des mesures techniques ou organisationnelles.*

*La durée de rétention des journaux devra être indiquée.*

*Indiquez si les opérations d’administration sont tracées de manière à pouvoir gérer au niveau individuel l’imputabilité des actions.*

1. **Gestion des authentifiants**
   1. **Gestion des mots de passe**

*Décrivez les règles de gestion et de protection des mots de passe donnant un accès aux systèmes et applications. La politique est susceptible de contenir la fréquence de renouvellement des mots de passe, de leur niveau de complexité, de l’outillage permettant leur stockage, des règles de bonne hygiène sécurité (ex : pas de mot de passe en clair dans un fichier ou papier), de la réinitialisation du mot de passe lorsqu’il a été communiqué à un tiers, d’une procédure de renouvellement en cas de suspicion de compromission.*

*La politique de mot de passe pourra être adaptée en fonction des contraintes techniques de chaque système, pour concilier sécurité et exploitabilité.*

* 1. **Gestion des certificats électroniques**

*Décrivez les règles de gestion et de protection des certificats électroniques s’ils sont utilisés sur le SI de sûreté, ainsi que leur niveau de conformité vis-à-vis des règles dictées par le RGS.*

1. **Sécurité physique**
   1. **Contrôle d’accès physique aux locaux**

*Décrivez les règles de gestion permettant garantir la sécurité des accès physiques aux équipements informatiques du SI de sûreté (ex : mise en place de moyens permettant de restreindre et contrôler les accès physiques aux armoires informatiques).*

*Indiquez si les moyens de protection s’appuient sur des produits qualifiés lorsqu’ils sont disponibles et s’ils bénéficient d’un maintien en condition de sécurité rigoureux tout au long de leur cycle de vie.*

* 1. **Traçabilité des accès physiques aux locaux**

*Indiquez si une procédure de traçabilité des accès physiques aux locaux des SI de sûreté est réalisée, que ce soit pour le personnel de l’entreprise ou pour ses sous-traitants, si les traces sont conservées et pour quelle durée, si celles-ci respectent les textes protégeant les données personnelles.*

1. **Sécurité de l’exploitation des SI**
   1. **Durcissement des ressources informatiques**

*Indiquez si des moyens sont mis en place pour réduire la surface d’attaque des systèmes et applications en exploitation. Ces moyens de durcissement, outre le changement de mot de passe et certificat par défaut, peuvent-être la désactivation des services réseaux inutiles, la désactivation des ports USB, la mise en place de mécanismes de protection spécifiques comme le déploiement de GPO, l’application des recommandations de l’ANSSI, du CIS Benchmarks, d’une prestation spécifique d’un intégrateur.*

* 1. **Sauvegardes et restaurations**

*Indiquez si des procédures de sauvegardes et restaurations de chaque SI sont présentes, si ces procédures sont régulièrement testées et à quelle fréquence.*

* 1. **Protection contre les codes malveillants**

*Décrivez comment les systèmes sont protégés contre les codes malveillants (antivirus).*

*La procédure d’exploitation des antivirus doit indiquer, la fréquence de mise à jour des bases de signatures et des moteurs, si des analyses sont réalisées sur les détections et fonctionnement du dispositif (ex : machine régulièrement infectée, taux de mise à jour des systèmes, défaillance de l’antivirus).*

* 1. **Importation de données depuis l’externe**

*Décrivez comment des données provenant de l’externe sont importées sur le SI de sûreté sans porter atteinte à l’intégrité des systèmes (ex : processus de décontamination via une station blanche, contrôle d’intégrité des fichiers avant exécution).*

* 1. **Sécurité des nouvelles applications**

*Indiquez si la mise en place d’une nouvelle application ou d’un matériel, y compris pour un besoin justifié qui serait susceptible de compromettre la sécurité de l’infrastructure, fait l’objet d’une alerte sécurité auprès des ressources SSI de la DAP (ex : installation d’un dispositif de télémaintenance/télémesure connecté à Internet ou à une ligne spécialisée, installation d’une box Internet…).*

* 1. **Maintien en Condition Opérationnel**

*Décrivez la stratégie de MCO (préventif et évolutif) pour les différents systèmes et indiquez si certaines actions (rétablissement du service en cas d’incident majeur, visite de contrôle, mise à jour de composants) sont sous-traitées à un partenaire spécialisé (ex : intégrateur).*

*Le cas échéant, indiquez si cette sous-traitance est contractualisée tout au long du marché de gestion déléguée en mentionnant une matrice des rôles et responsabilités (RACI), les éventuels engagements associés.*

* 1. **Administration**

*Indiquez si les opérations d’administration sur le SI de sûreté s’appuient sur des protocoles sécurisés, des postes dédiés, des accès nominatifs permettant d’imputer les actions à un niveau individuel en respectant les principes de besoin d’en connaître et de moindre privilège.*

*Indiquez si les privilèges sur les SI sûretés pour chaque administrateur sont spécifiés dans un référentiel maintenu à jour et consultable à tout moment dans le cadre d’une opération de contrôle.*

1. **Maintien en condition de sécurité**
   1. **Contrats de support**

*Indiquez si le matériel, les systèmes d’exploitation et les applications exploitées font l’objet d’un support valide de la part d’un éditeur ou d’un prestataire durant toute la durée du contrat de gestion déléguée.*

*Indiquez si la gestion de l’ensemble des contrats de supports est consignée dans un référentiel en précisant l’outil.*

* 1. **Obsolescence logicielle et matérielle**

*Indiquez si les systèmes obsolètes font l’objet d’une migration vers des versions supportées par l’éditeur et tenue à jour lorsque nécessaire.*

* 1. **Veille sécurité**

*Indiquez si l’ensemble des composants constituant le SI fait l’objet d’une veille sécurité, précisez les canaux utilisés pour cette veille (abonnement éditeur, CERT-FR, SOC interne, liste de diffusion, flux RSS…) et décrivez le processus de veille interne à l’organisation décliné pour la DAP.*

*Dans le cas du recours à un SOC externe à l’établissement pour l’activité de veille, décrivez comment la sécurité des données sensibles de la DAP (inventaire logiciel et matériel) est garantie.*

* 1. **Politique de suivi et d’application des correctifs sécurité**

*Décrivez comment le maintien en condition de sécurité des systèmes d’exploitation, des micrologiciels et des applications pour chaque système d’information est assuré et à quelle fréquence.*

*Indiquez les moyens permettant d’assurer la gestion des correctifs propre à chaque système (mise à jour via CD, clef USB, serveur de mise à jour…).*

* 1. **Sous-traitance du Maintien en Condition de Sécurité**

*Indiquez si certaines actions du MCS (ex : veille sécurité, application des correctifs etc.) sont sous-traitées à un prestataire spécialisé (ex : intégrateur).*

*Le cas échéant, indiquez si cette sous-traitance est contractualisée tout au long du marché de gestion déléguée en mentionnant une matrice des rôles et responsabilités (RACI).*

* 1. **Mise au rebût**

*Indiquez si les données non chiffrées de toute ressource informatique sont effacées avant l’envoi en maintenance externe.*

*Indiquez si les données d’une ressource informatique amenée à quitter définitivement l’établissement sont effacés.*

*Indiquez si l’effacement des données sensibles cités dans les deux cas ci-dessus est réalisée de façon systématiquement sécurisée et en s’appuyant sur des produits labellisés (certifiés, qualifiés) par l’ANSSI.*

1. **Relation avec des tiers**
   1. **Gestion de la sécurité avec une autre entité du groupe ou d’un sous-traitant**

*Décrivez les moyens mis en œuvre pour garantir la sécurité des données de la DAP lors du recours à une prestation externe à l’entité juridique signataire du contrat de gestion déléguée.*

* 1. **Acquisition de produits et services de confiance**

*Indiquez si les critères sécurité sont toujours évalués lors du choix de produits et solutions permettant la réalisation de la prestation demandée, et si le recours à des produits labellisés est privilégié dans la mesure du possible.*

1. **Gestion des journaux et des incidents**
   1. **Horodatage des évènements**

*Indiquez si les journaux des systèmes et métadonnées de vidéosurveillance font l’objet d’un horodatage exploitable dans le cadre d’une procédure réglementaire, en précisant le cas échéant les moyens associés pour atteindre cet objectif.*

* 1. **Journalisation des incidents et alertes**

*Indiquez pour chaque SI si les évènements de sécurité produits sont conservés et avec quelle politique d’archivage.*

* 1. **Analyse des journaux**

*Indiquez si l’expert sécurité local procède ponctuellement à l’analyse des journaux, surveille les comportements anormaux, les dysfonctionnements et les tentatives d’accès illicites survenant sur les éléments sensibles de chaque SI.*

* 1. **Qualification des incidents sécurité**

*Indiquez si tout incident sécurité, même apparemment mineur, dont l’impact est susceptible d’atteindre le fonctionnement nominal de l’établissement, fait l’objet d’un compte-rendu et d’une communication à la chaîne SSI.*

* 1. **Gestion de crise**

*Décrivez le processus de gestion d’une crise cybersécurité, précisez comment la chaîne opérationnelle notifie la chaîne fonctionnelle SSI (rôle précis de chaque acteur), comment l’incident est qualifié et piloté, en heures ouvrées et non ouvrées, quels sont les processus d’escalade et comment la DAP est impliquée dans cette gestion de crise.*

1. **Gestion de la continuité d’activité**
   1. **Mise en œuvre des dispositifs techniques et des procédures**

*Indiquez si des dispositifs techniques (ex : supervision) et des procédures opérationnelles contribuant à la continuité d’exploitation (PCA) sont mis en œuvre, décrivez-les le cas échéant.*

* 1. **Protection de la disponibilité des sauvegardes**

*Indiquez si les sauvegardes de données sont soumises aux mêmes risques de sinistres que les données en ligne. Si une contre-mesure est en place pour atténuer le risque, décrivez-la.*

* 1. **Protection de la confidentialité des sauvegardes**

*Indiquez comment l’intégrité et la confidentialité des sauvegardes sont garanties pour chaque SI.*

* 1. **Exercice du Plan local de continuité d’activités des SI**

*Indiquez si des exercices réguliers du Plan local de Continuité des Activités pour chaque SI sont réalisés, à quelle fréquence et par qui ils sont pilotés (RSSI de l’organisation, responsable d’exploitation local…).*

1. **Contrôle et évaluation**
   1. **Contrôles récurrents de conformité au PAS et aux PSSI**

*Indiquez si la conformité au PAS et aux PSSI de la DAP sont vérifiés par des contrôles réguliers, précisez la fréquence ainsi que l’entité en charge de cette réalisation à chaque type d’audit (action locale sur l’établissement, action du RSSI, audit d’un prestataire indépendant etc.).*

*Indiquez comment le résultat des contrôles sont consignés, puis partagés avec la DAP et si un plan d’actions permettant de remédier aux écarts identifiés est mis en place.*

* 1. **Reporting SSI**

*Décrivez comment est mis en place le tableau de bord SSI, précisez les indicateurs de performances sécurité utilisés et la fréquence de collecte.*

*Celui-ci doit fournir à la DAP une vision générale du niveau de maturité de la sécurité des SI de sûreté, de leur évolution, de la production documentaire, de suivre la bonne application du PAS, de contrôler la réalisation des objectifs opérationnels, d’améliorer la qualité de service et de détecter au plus tôt les retards dans la réalisation de certains objectifs de sécurité.*