

Exigences de sécurité	Précisions
Sécurité des ressources humaines	
– Recrutement	Vérification de l'identité et de situation légale
– Gestion des arrivées départ	"Circuit" arrivé/départ (Perception et réintégration doc. et matériel, gestion des comptes)
– Sensibilisation et formation à la Sécurité Numérique	Sensibilisation a la sécurité des systèmes d'information
Gestion des actifs	
– Cartographie des actifs	Quels sont les moyens informatiques et comment ils sont reliés entre eux
– Classification des actifs	Le cas échéant, pour ce qui est classifié au regard de l'IGI1300
– Protection des informations	Quelles mesures sont prises (Physiques et organisationnelles)
Gestion des accès logiques	
– Droits d'accès aux ressources	Qui gère les droits d'accès et comment ils sont appliqués
– Contrôle d'accès logique aux SI	Quel dispositif protège l'accès logique (Mot de passe, certificat, carte ...)
– Gestion des habilitations	Habilitations au sens de l'IGI1300 (Protection des données classifiées)
– Gestion des sessions inactives	Comment sont contrôlées et gérées les sessions inactives
– Traçabilité des accès	Comment sont tracé les accès (journaux logiciels, SMSI ...)
Gestion des authentifiants	
– Gestion des mots de passe	Rythme de changement, politique de complexité...
– Gestion des certificats électroniques	Le cas échéant
Sécurité physique	
– Contrôle d'accès physique aux locaux	Quel dispositif protège l'accès physique aux locaux (bareaudage, clé, verrou...)
– Traçabilité des accès physiques aux locaux	Journaux de lecteur de badge, registre...
– Protection des zones de sécurité physique	Système d'alarme volumétrique, périmétrique ...
Sécurité de l'exploitation des SI	
– Durcissement des ressources informatiques	Mesures mises en place (démarche qui consiste principalement à réduire à l'indispensable les objets installés sur le système, ainsi qu'à éliminer les utilisateurs et les droits non indispensables, tout en conservant les fonctionnalités requises.)
– Sauvegardes et restauration	Dispositif, fréquence, tests...
– Gestion des correctifs de sécurité	Mise à jour de sécurité, automatique, liste de diffusion
– Lutte contre les codes malveillants	Anti-virus, parefeu logiciel, anti spam
– Administration des SI	Qui est responsable de l'administration des systèmes d'information?
Sécurité des communications	
– Politique de sécurité des communications	Existence, date de mise à jour, références...
– Sécurisation des transmissions de données	Dispositif de chiffrement, méthode, canaux ...
– Accès à distance aux SI	Par quels moyens, avec quelles protections ?
– Accès au réseau interne depuis des équipements non maîtrisés	Le cas échéant (oui /non)
Maintenance des SI	
– Maintien du niveau de sécurité des SI	Comment, Qui, procédure ?
– Sécurité de la maintenance des SI	Qui maintient, Comment, quelle procédure et/ou dispositif de sécurité ?
– Mise au rebut	Procédure, destruction des supports
Relation avec les tiers	
– Gestion de la sécurité avec les sous-traitants	Vérification d'un niveau de sécurité au moins équivalent
Gestion des incidents et des alertes	
– Veille et gestion des vulnérabilités techniques	Matériel et logiciel, inscription aux listes, diffusion des CVE...
– Détection et dispositif de gestion des incidents	Comment, qui, où ?
– Journalisation des incidents et des alertes	Comment, qui, procédure ?
– Gestion de crise	Procédure, dispositif
Gestion de la continuité d'activité	
– Définition, mise en œuvre et maintien du plan de continuité d'activité	Existence, qui, fréquence ?
– Protection des données de sauvegarde	Lieu d'entrepôt, sauvegardes déconnectées...
Mise à jour des systèmes et logiciels	
– Sécurité des postes de travail	Mise à jour de sécurité, automatique, liste de diffusion
– Utilisation de terminaux personnels (BYOD)	oui/non, mesures de protection
– Privilèges des utilisateurs sur les postes de travail	Compte administrateur, droits étendus...
– Stockage des informations	Comment, où ?
– Protection des données critiques	Comment, où ?
– Configuration du navigateur internet	limitations, sécurisations
Gestion de la documentation	
– Référentiel documentaire	Existence d'une documentation de référence ? Quels accès
– Gestion de la documentation	qui, comment ?,avec un focus sur les documents sensible qui serait identifié diffusion restreinte ou secret
Contrôle et évaluation	
– Contrôles récurrents de conformité à la PSSI	Qui, fréquence ?
– Audits ponctuels de conformité à la PSSI	Qui, fréquence ?
Organisation de la sécurité	Description sommaire des rôles et fonctions
Responsabilités liées au PAS	Comment sont elles prises en compte et gérées
Procédures d'évolution du PAS	Comment sont elles prises en compte et gérées
Mesures de sécurité	Comment sont elles prises en compte et gérées