

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 1 sur 18

Le PSSI-Thématiques est un document annexe à la procédure SQ419 « **Politique de Sécurité des Systèmes d'Information** ». Ce document regroupe l'ensemble des règles devant être appliquées afin de garantir, de manière cohérente et efficace, la Sécurité des Systèmes d'Information (SSI) de la CTS.

Organisation documentaire de la PSSI

La PSSI est composée d'un ensemble de documents :

- ✓ le document Politique de Sécurité des Systèmes d'Information-Générale (PSSI-G) qui définit les règles organisationnelles et techniques de protection du SI,
- ✓ le document Politique de Sécurité des Systèmes d'Information-Thématiques (PSSI-T) constituées de règles de sécurité thématiques pragmatiques (serveurs, réseaux, Internet, postes de travail, ...),
- ✓ des chartes (utilisateurs et administrateurs) et procédures opérationnelles spécifiques à la sécurité des systèmes d'information complètent la PSSI.

• **Suivi du plan d'action**

Il sera possible de ne pas appliquer une mesure si l'impossibilité est expliquée et justifiée.

Par défaut, toutes les mesures sont prises en compte.

Lorsqu'une mesure n'est pas applicable une justification est nécessaire afin d'identifier et d'accepter le(s) risque(s) résiduel(s).

• **Gestion des niveaux de règles**

Les règles sont classifiées selon 4 niveaux comme indiqué dans le tableau suivant.

- Les règles de niveau 1 et 2 correspondent aux exigences importantes de sécurité devant être mises en œuvre à la CTS.
- Les règles de niveau 3 et 4 sont à mettre en œuvre en fonction de l'analyse des enjeux de sécurité de la CTS.
- Pour toute question en rapport avec la PSSI vous pouvez prendre contact avec le RSSI (ssi@cts-strasbourg.fr).

Niveau	Détails
1	Règles incontournables, elles sont obligatoires et doivent être absolument implémentées dans l'ensemble du SI. Elles constituent la base de la sécurité.
2	Règles correspondantes à de bonnes pratiques sécuritaires, à implémenter sur tous les systèmes s'ils le supportent, obligatoirement sur les nouveaux systèmes et les systèmes critiques.
3	Règles à caractère obligatoire pour les systèmes critiques, elles peuvent être généralisées aux autres systèmes en fonction des événements.
4	Etat de l'art : règles obligatoires pour les systèmes vitaux.

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 2 sur 18

Les Réseaux

Objet

L'objectif de ce document est de fournir les éléments techniques constituant les règles d'architecture des réseaux de la CTS.

Règles

Règle	Description	Niveau de sécurité
Architecture		
RES01	Tous les serveurs accessibles depuis un réseau public doivent être cloisonnés au sein d'une DMZ ou d'un Vlan étanche (exemple : un serveur web accessible depuis Internet)	1
RES02	Les communications inter-réseaux doivent se faire à travers un élément de sécurité (routeur firewall) et en aucun cas par une ou des connexions physiques sur tout ou partie des réseaux à atteindre (suppression des ordinateurs à plusieurs cartes réseaux)	1
RES03	Tout accès externe critique doit être redondé.	3
Réseaux sans fil		
RES04	Tout accès sur un réseau sans fil doit se faire avec un protocole de chiffrement en WPA2 minimum.	1
RES05	Les bornes Wifi personnelles sont interdites	1
RES06	L'administration des infrastructures Wifi ne doit pas pouvoir se faire depuis la partie radio	2
Commutateurs réseaux		
RES07	Maintenir le micrologiciel des commutateurs réseaux régulièrement à jour	3
RES08	La configuration des commutateurs réseaux doit être sauvegardée régulièrement	2
RES09	La configuration du cœur de réseau doit être réalisée régulièrement	1
Firewall		
RES10	Les éléments de sécurité frontaux doivent être redondés	2
RES11	Les règles de sécurité doivent contenir de façon bien définie une source, une destination, un protocole et une description	1

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 3 sur 18

RES12	La configuration des firewalls doit être sauvegardée régulièrement	1
RES13	Assurer la gestion, la validation et la traçabilité des changements des règles de firewall.	3
Général		
RES14	Tout dispositif de sécurité doit être configuré pour générer des traces de sécurité. Au minimum, les traces suivantes doivent être consultables : - Messages d'alertes - Messages d'erreur - Etat des sessions VPN - Tentatives (échec ou succès) de connexion (login ou session) Les traces doivent être protégées en intégrité et en confidentialité et doivent être conservées autant de temps que nécessaire et dans le respect des traitements déclarés.	4
RES15	Tout élément de sécurité critique doit être maintenu par son constructeur et changé à la fin de sa période de maintenance.	3

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 4 sur 18

Les Serveurs

Objet

L'objectif de ce document est de disposer des règles de sécurité afin de limiter les différents risques décrits ci-dessous.

Les serveurs sont des outils de production essentiels pour l'exécution de nombreux processus de l'entreprise. Ces serveurs doivent être protégés, car leurs modes de fonctionnement induisent de nombreux risques de différentes natures. Par exemple, la messagerie électronique (messages circulant en clair, sans garantie d'authenticité ni de l'émetteur ni du contenu) présente des risques tels que :

- la perte, l'interception, l'altération, la destruction de messages ;
- la diffusion par erreur d'informations confidentielles ;
- l'abus d'usage, le harcèlement (spam), entraînant une dégradation du service ;
- la diffusion d'informations à caractère illégal ;
- la propagation de codes malveillants (virus, vers, Troyens) ;
- l'usurpation d'identité.

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 5 sur 18

Règles

Règle	Description	Niveau de sécurité
	Règles générales	
SRV01	Les règles d'utilisation de la messagerie électronique sont décrites dans une charte d'utilisation spécifique ou au sein de la charte informatique. Ces règles sont destinées à tous les utilisateurs des systèmes de messagerie.	1
SRV02	Les utilisateurs sont régulièrement sensibilisés aux risques liés à l'utilisation de la messagerie (phishing, spam, virus, etc.) et aux règles de bon usage de la messagerie électronique.	2
SRV03	Tout serveur équipé d'un environnement Microsoft Windows doit bénéficier d'un antivirus fonctionnel et à jour.	1
SRV04	L'installation d'un environnement serveur doit être approuvé par le correspondant sécurité et doit satisfaire à l'ensemble des règles de la PSSI qui le concerne. Dans le cas contraire l'installation sera refusée.	1
SRV05	L'intégration d'une solution logicielle ne doit pas dégrader le niveau de sécurité de la CTS et doit se conformer aux exigences de la PSSI.	1
	Architecture de messagerie	
SRV03	L'échange de courriers électroniques doit se faire uniquement par l'intermédiaire d'un relais de messagerie sécurisé.	1
SRV04	Un logiciel antivirus doit être installé sur les serveurs et relais de messagerie. Il doit être configuré afin d'analyser et de protéger le contenu de l'ensemble des courriers électroniques et des pièces jointes	1
SRV05	Un dispositif de filtrage doit être mis en œuvre, afin de contrôler plus particulièrement les messages non sollicités (spamming, mailings publicitaires, par exemple) et les pièces jointes illicites.	1
SRV06	La chaîne de liaison d'un service de messagerie électronique doit garantir que l'en-tête d'un message sortant vers l'Internet ne contient aucune donnée exploitable par un attaquant potentiel (Adresse réseau, nom des relais de messagerie, nom et version du ou des logiciels antivirus).	1
SRV07	Les serveurs de messagerie doivent mettre en œuvre des dispositifs permettant de rejeter les courriers électroniques dont la provenance ne correspond pas au nom de domaine de l'émetteur (anti spoofing ou usurpation d'adresse mail).	1
SRV08	Des outils de chiffrement des pièces jointes sont mis à disposition des utilisateurs de la messagerie	2
	Webmail	
SRV09	La connexion de l'utilisateur à un Webmail doit se faire avec un flux chiffré	1
SRV10	La connexion de l'utilisateur à un Webmail doit se faire avec une authentification forte	4

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 6 sur 18

	Configuration	
SRV11	Tous les mots de passe par défaut doivent être changés suite à une installation de service de messagerie	1
SRV12	Le relais automatique de tout message entrant vers une adresse externe à l'entreprise est interdit (reroutage, email professionnel vers messagerie personnelle)	1
SRV13	Afin de réduire les risques de saturation du système ou de surcharge du réseau, le nombre de destinataires d'un même message, ainsi que du volume de données transmises doivent être limités (Maximum 50 Mo).	1
SRV14	Tout rejet ou suppression de fichier joint doit faire l'objet d'un message de notification à l'émetteur.	2
SRV15	Les règles de sécurité (routage, filtrage d'adresses, de contenu...) mises en œuvre dans les relais de messagerie doivent être consignées dans un document spécifique.	3
	Exploitation	
SRV16	Tout message non conforme à la politique de sécurité doit être intercepté et faire l'objet d'un processus de mise en quarantaine ou de rejet, avec notification à la fonction administration.	1
SRV17	La typologie des adresses de messagerie des personnes non salariées ou externes, mais bénéficiant d'une adresse de messagerie au sein de la CTS est différenciée (par exemple en précédant l'adresse du suffixe « EXT »)	2
SRV18	La gestion des comptes de messagerie au sein de la CTS doit s'appuyer sur des processus et procédures communs, notamment : - La prise en compte des arrivées, mutations et départs, pour les activations et clôtures des droits d'accès ; - La suppression / l'archivage dans des délais appropriés, du contenu des boîtes de messagerie, en cas de départ d'un utilisateur.	3
SRV19	Les interactions des administrateurs avec les données des utilisateurs sont strictement limitées dans le cadre de l'exécution de leur mission, conformément aux règles énoncées dans la fiche descriptive de poste.	1
SRV20	Une revue régulière des journaux d'activité est mise en place pour générer des alertes auprès des administrateurs cas de suspicion d'abus de droits et répondre aux éventuelles demandes des autorités judiciaires.	4
SRV21	La CTS définit et couvre ses objectifs de protection des données personnelles pour ses systèmes de messagerie	2
	Règles d'accès à la messagerie	
SRV22	En dehors des délégations directement accordées par le titulaire d'une boîte aux lettres en utilisant la fonctionnalité mise à disposition par son logiciel de messagerie, aucun accès ne peut être fait par un utilisateur ou un administrateur à la messagerie d'un tiers, sauf exception justifiée par les nécessités de service (absence imprévue, situation de départ...), Cette intervention devra faire l'objet d'une autorisation explicite et formelle au DRH ou au RSSI.	2
SRV23	L'utilisateur ne peut pas utiliser sa boîte aux lettres professionnelle sur une messagerie grand public (Yahoo, Gmail, etc.) pour envoyer ou recevoir des messages à caractère professionnel.	2
SRV24	Les utilisateurs ne doivent pas configurer eux-mêmes leur messagerie d'entreprise sur des clients non sécurisés (mobile et desktop)	1

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 7 sur 18

	Maintien en condition opérationnelle	
SRV25	Les journaux d'activité des infrastructures de messagerie sont régulièrement contrôlés pour vérifier l'absence d'utilisation malveillante de la messagerie.	4
SRV26	Les relais de messagerie exposés sur Internet font régulièrement l'objet de tests d'intrusion. Ces audits donnent lieu, le cas échéant, à des plans d'actions de sécurisation, qui devront être mis en œuvre par la CTS.	4

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 8 sur 18

Règles Internet

Objet

L'objectif de ce document est de fournir les éléments techniques constituant les règles de connexions à Internet appliquées aux équipements d'interconnexion réseaux.

Règles

Règle	Description	Niveau de sécurité
	Architecture d'accès à Internet	
INT01	La mise en œuvre du dispositif de filtrage (firewall) depuis le réseau interne de l'entreprise vers Internet, et réciproquement, doit être réalisée sur la base du principe fondamental selon lequel « tout ce qui n'est pas autorisé est interdit » : - au niveau des protocoles d'échange ; - au niveau des ressources accédées.	1
INT02	Tout le trafic Internet, entrant et sortant, doit être filtré par des serveurs mandataires, situés dans un sas physique ou logique (également appelé DMZ – Zone démilitarisée -). La DMZ forme une zone de cloisonnement intermédiaire entre Internet et le réseau interne de l'entreprise. Parmi ces serveurs mandataires, on trouve : - les serveurs web (pour les protocoles http, HTTPS et FTP) ; - les serveurs accessibles directement depuis l'extérieur (serveur DNS, par exemple) ; - le relais de messagerie électronique...	1
INT03	L'ensemble des flux entrants et sortants depuis / vers Internet doit être analysé et protégé par un dispositif antiviral.	1
INT04	Un filtrage URL catégoriel doit être mis en œuvre au niveau des accès Internet. La liste des catégories autorisées est validée par le RSSI ou le correspondant sécurité. Des dérogations peuvent être allouées au cas par cas.	1
INT05	Tout utilisateur du service de navigation web (HTTP) doit être identifié et authentifié.	1
INT06	Tout utilisateur du service de navigation doit être protégé des menaces externes liés à ses téléchargements (refus de certaines extensions .exe, .com etc ... et analyse des téléchargements).	1

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 9 sur 18

Postes de travail et terminaux

Objet

L'objectif de ce document est de fournir règles de sécurité relatives aux postes de travail et aux terminaux destinés aux utilisateurs. Ces éléments représentent les premiers points d'entrée vers le système d'information de la CTS et doivent donc être gérés et protégés de façon adéquate.

Règles

Règle	Description	Niveau de sécurité
	Gestion du parc informatique	
WKS01	Tout poste de travail doit être affecté à un utilisateur ou à une entité dont le responsable est identifié	1
WKS02	Un inventaire des postes de travail doit être en place et mis à jour régulièrement. Cet inventaire doit contenir à minima le nom des postes de travail, la version de l'OS, la liste des logiciels avec leur version, le nom de l'utilisateur.	2
WKS03	Une politique de nommage des postes de travail doit exister	2
	Installation et configuration des postes de travail	
WKS04	L'installation et la configuration d'un poste de travail ou d'un terminal informatique doit être opéré par les équipes techniques du service informatique.	1
WKS05	Pour les postes de travail un master doit exister avec les dernières mises à jour de sécurité intégrées.	2
WKS06	Les applications installées doivent bénéficier d'une licence en cours de validité. L'utilisation de copies contrefaites est strictement interdite.	1
WKS07	Les droits des utilisateurs doivent être limités sur les stations de travail. Si un utilisateur doit être administrateur de son poste il doit être sensibilisé aux risques encourus. Le compte « Administrateur local » doit être connu uniquement du service informatique et ne doit être divulgué à personne.	1
WKS08	Le verrouillage de session automatique doit être activé au-delà de 15 minutes d'inactivité maximum.	1
WKS09	Chaque poste de travail possède un antivirus actif et à jour et une analyse totale doit être planifiée régulièrement. Tout nouveau fichier accédé doit être scanné, et le programme antivirus ne doit pas pouvoir être désactivé par l'utilisateur.	1
WKS10	Les correctifs de sécurité doivent être appliqués régulièrement sur tout type de terminaux (ordinateurs fixes et portables, smartphones, tablettes)	1

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 10 sur 18

WKS11	La mise au rebut d'un terminal doit s'accompagner d'un effacement complet des données avant destruction.	2
Gestion des accès		
WKS12	Chaque utilisateur du SI possède un compte nominatif protégé par un mot de passe robuste.	3
WKS13	Le contrôle à distance des ordinateurs est strictement limité aux équipes du support informatique.	1
WKS14	Le mot de passe du compte principal Active Directory doit être changé tous les 12 mois, doit comporter au moins 12 caractères alphanumériques avec un caractère spécial.	3
WKS15	Les accès aux différentes applications informatiques doivent tous être gérés par les équipes de l'exploitation informatique. Il est strictement interdit de déléguer un accès (création, modification) à un autre service.	4
Règles supplémentaires à destination des ordinateurs portables		
WKS16	Tous les accès distants initiés depuis un ordinateur portable doit se faire à travers des flux chiffrés (https, tunnel IPSEC etc...)	1
WKS17	L'utilisation de support amovible est proscrite. Si son utilisation est inévitable les supports de stockage externes doivent être distribués par le service informatique et chiffrés si possible.	2
WKS18	Chaque poste nomade dispose d'une solution de chiffrement activée.	3
Règles supplémentaires à destination des smartphones		
WKS19	Une solution doit permettre de supprimer à distance les données présentes sur un smartphone critique perdu ou volé.	3
WKS20	Si un utilisateur est amené à recevoir des e-mails critiques sur son smartphone, une solution doit permettre de chiffrer l'appareil ainsi que ses flux.	4
Règles d'utilisation générale des terminaux		
WKS21	Chaque utilisateur du système d'information doit avoir lu et approuvé la charte informatique de la CTS.	1
WKS22	Les utilisateurs doivent être sensibilisés aux risques liés à leur poste de travail : e-mails frauduleux, pièces jointes suspectes, téléchargement illégaux etc ... et dans un cadre plus général ils doivent respecter la charte informatique.	2
WKS23	Une solution de chiffrement sur les postes critiques doit être installée et activée	4

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 11 sur 18

Développement et Bases de données

Objet

Les bases de données représentent l'essence de la CTS, elles doivent par conséquent être garanties cohérentes, disponibles et pérennes. Ces exigences se traduisent par des règles de sécurité sur les bases de données mais également sur les développements logiciels.

Règles

Règle	Description	Niveau de sécurité
	Bases de données	
DEV01	Le mot de passe du compte SA doit être changé et doit respecter les exigences de sécurité en termes de complexité.	1
DEV02	Les services de bases de données doivent s'exécuter avec des comptes systèmes de l'annuaire et des droits adaptés.	1
DEV03	Les correctifs de sécurité des bases de données doivent être installés s'ils sont supportés.	1
DEV04	Les services pack doivent être installés s'ils sont supportés par les applicatifs.	2
DEV05	Les bases de données doivent faire l'objet d'un plan de sauvegarde adéquat en fonction de la criticité de celles-ci.	1
	Développement	
DEV06	Les sources de développement doivent être centralisées et protégées par un mot de passe complexe.	2
DEV07	Les mots de passe embarqués dans le code de développement doivent être chiffrés à l'aide d'un algorithme récent.	2
DEV08	Les fichiers de configuration ne doivent pas contenir de mot de passe.	1

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 12 sur 18

Sauvegardes et Restaurations

Objet

Cette fiche technique aborde les règles de sécurité relatives à la sauvegarde et à l'archivage des données numériques. Les règles précisent les éléments nécessaires pour la sécurisation des sauvegarde (protection des données, contrôles).

Règles

Règle	Description	Niveau de sécurité
Généralités		
B&R01	Pour toute application, une politique de sauvegarde doit être définie par les équipes fonctionnelles et validée par le service d'exploitation. Elle est fonction du volume, du type, et de la durée légale de rétention des données. Elle doit inclure : - Les éléments à sauvegarder, les types de données - Les fréquences de sauvegarde (perte de données admissibles, fréquence minimum des sauvegardes, méthode de sauvegarde). - Le stockage des données sauvegardées	2
B&R02	Une politique de sauvegarde générale doit être écrite et tenue à jour	1
B&R03	Les données sauvegardées doivent inclure l'ensemble des éléments nécessaires à la restauration d'un service ou d'une application : - Les systèmes d'exploitation - Les applications ; - Les données.	2
Contrôles et tests		
B&R04	Des tests de restauration doivent être réalisés régulièrement afin de qualifier l'efficacité des sauvegardes	2
B&R05	Un contrôle journalier des sauvegardes doit être effectué et provoquer des actions correctrices en cas de dysfonctionnement.	1
Protection des données		
B&R06	Une séparation physique entre les données originales et les données sauvegardées doit exister.	1
B&R07	Les données à caractère personnel doivent être détruites ou anonymisées dès que le délai de conservation déclaré ou imposé par la CNIL est dépassé.	1

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 13 sur 18

Equipements industriels

Objet

Les systèmes industriels utilisent aujourd'hui abondamment les technologies de l'information alors qu'ils n'ont pas été conçus pour faire face aux menaces qu'elles introduisent.

Élaborer une politique robuste sur la sécurité informatique commence par bien comprendre les risques auxquels l'organisation est confrontée ainsi que les risques auxquels elle peut exposer ses clients.

Règles

Règle	Description	Niveau de sécurité
	Généralités	
SII01	Établir une cartographie du système industriel : physique, logique et des applications (les flux seraient un plus).	1
SII02	La cartographie du système industriel devra être revue régulièrement, à chaque modification du système industriel et au moins une fois par an.	2
	Architecture des réseaux	
SII03	Le réseau informatique industriel doit être séparé du réseau informatique bureautique.	1
SII06	Les différents réseaux industriels doivent être cloisonnés entre eux.	2
SII07	Les flux réseaux entre les différents réseaux industriels doivent être filtrés par un élément de sécurité.	1
SII08	Les flux entre les réseaux industriels et le réseau local bureautique doivent être filtrés par un élément de sécurité.	1
SII09	Les accès des réseaux industriels vers Internet doivent être limités au strict nécessaire.	1
	Accès aux équipements	
SII10	Identifier qui a besoin d'accéder physiquement aux équipements et pourquoi.	1
SII11	Installer les serveurs et les équipements réseaux dans des locaux fermés sous contrôle d'accès.	1
	Accès logiques	
SII12	Protéger l'accès aux automates par un mot de passe et ne pas laisser les comptes par défaut. Privilégier des mots de passe robustes.	1

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 14 sur 18

SII13	Les intervenants et/ou les prestataires doivent posséder leurs propres comptes avec des privilèges adéquat. Le compte administrateur ne doit pas être utilisé pour l'exploitation ou la maintenance.	3
SII14	La journalisation des accès doit être active et consultable.	3
	Sécurité	
SII15	Les systèmes industriels doivent être protégés par un antivirus actif et à jour dans la mesure du possible.	4
SII16	Les systèmes industriels doivent bénéficier d'un contrat de maintenance assurant notamment le patch management quand celui-ci est possible.	3
SII17	Activer les fonctions de traçabilité si les équipements et logiciels le permettent (Sys log, SNMP V3, « Windows Event », fichier texte, etc.	3
SII18	Générer des alertes pour certains styles d'évènements critiques.	4
SII19	Les intervenants devront être sensibilisés à la cybersécurité des systèmes industriels. (Pour les internes session de sensibilisation).	1
	Sauvegarde	
SII20	Un plan de sauvegarde des données importantes devra être mis en place afin de permettre leur restauration en cas d'incident. Les données concernées sont toutes les données nécessaires à la reconstruction du système après un sinistre : les programmes, les fichiers de configuration, les firmwares, les procédures etc ... Cela peut également concerner des données ayant un aspect réglementaire comme des exigences de traçabilité.	2

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 15 sur 18

Locaux physiques

Objet

Ces règles présentent les normes de sécurité relatives à la protection physique de tout lieu hébergeant des ressources informatiques.

Il est impératif de préserver les équipements informatiques de tout dommage physique et d'assurer leur fiabilité de fonctionnement, car de nombreuses causes peuvent compromettre la sécurité physique, telles que :

- une intrusion dans une salle informatique : vol d'équipement, altération, copie, écoute, ...
- un incident ou un accident au niveau des salles informatiques : incendie, dégât des eaux, catastrophe naturelle, sabotage matériel ...
- Toute salle hébergeant des ressources informatiques partagées ou des infrastructures de communication est à minima considérée comme sensible et doit appliquer au moins l'ensemble des règles de niveau un.
- Les salles critiques, hébergeant des ressources dont un défaut de sécurité engendrerait des dysfonctionnements gênants la conduite des activités, doivent au moins mettre en œuvre les règles de niveau un et deux.
- Les salles vitales, comme celles hébergeant des ressources qui requièrent des niveaux de disponibilité, d'intégrité et de confidentialité maximum, doivent mettre en œuvre l'ensemble des règles énoncées ci-dessous.

Règles

Règle	Description	Niveau de sécurité
	Généralités – Equipements des locaux	
LOC01	Le local technique doit être exclusivement réservé à l'hébergement de matériel informatique et de télécommunication.	1
LOC02	Le stockage d'équipements non autorisés ou de matériaux inflammables au sein du local technique est proscrit (matériel d'entretien, cartons, papiers, poubelles, balais, etc....) Celui-ci doit être entretenu de manière régulière.	1
LOC03	Tous les locaux hébergeant des dispositifs informatiques doivent être équipés avec des systèmes de détection (incendie, intrusion) qui doivent être associés à un contrat de service d'intervention disponible 24h/24 et disposant des consignes pour réagir.	1
LOC04	Les locaux techniques doivent être équipés d'une climatisation dimensionnée efficacement afin que les équipements techniques puissent fonctionner dans des conditions optimales (18-21°C)	1
LOC05	Les locaux techniques doivent être équipés d'une sonde de température avec une remontée automatique vers les équipes supports en cas de dépassement de la température maximale de fonctionnement des équipements.	2

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 16 sur 18

LOC06	Les locaux techniques sont équipés d'un extincteur CO2 à main (Classe B et feux d'origine électrique).	1
LOC07	Les consignes de sécurité en cas d'incendie sont affichées et un bloc autonome "Sortie de Secours" est fonctionnel.	1
LOC08	Des mesures de prévention contre les incendies, sont affichées dans les locaux techniques, comme l'interdiction de fumer et l'interdiction de stocker du matériel inflammable.	1
LOC09	Tous les dispositifs mis en place de détection, protection et lutte contre le feu doivent être maintenus en condition opérationnelle (maintenance régulière, contrôle annuel).	1
LOC10	Les locaux techniques doivent être équipés de dispositifs de détection de fuite et d'humidité reliés à un système de gestion des alarmes.	3
Contrôle d'accès		
LOC11	Un système de contrôle d'accès permet de limiter les accès aux locaux techniques au personnel habilité (serrure à clé, digicode, badge).	1
LOC12	Les supports de contrôle d'accès (badges, clés...) sont strictement personnels et ne doivent pas être prêtés à un tiers	1
LOC13	L'ensemble des dispositifs techniques de contrôle d'accès physique permettent de tracer et d'identifier (identité, jour, heure) les accédants aux locaux techniques	2
LOC14	Le contrôle d'accès physique doit permettre aux équipes de sécurité incendie de pénétrer dans les locaux en cas d'urgence	1
LOC15	Un affichage sur la porte d'entrée doit porter la mention "Accès Réservé".	2
LOC16	Un responsable des accès physiques doit être identifié et doit gérer les droits d'accès nominatifs selon le mode opératoire de gestion des droits d'accès définis.	2

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 17 sur 18

Prestataire externe

Objet

La sous-traitance peut faire courir des risques informatiques à la CTS (perte de production due à une erreur, propagation de codes malveillants, vol d'information ...) et doit donc être soumise à des règles de sécurité.

Cette fiche technique s'adresse à tout prestataire qui intègre un système informatique ou qui se trouve en interface avec le système d'information de la CTS.

Cette fiche thématique détaille les règles de sécurité applicables aux prestataires de la CTS, quel que soit le périmètre d'action du prestataire : infogérance, développement logiciel, assistance et expertise ...

Règles

Règle	Description	Niveau de sécurité
	Généralités	
PRE01	Tout contrat lié aux systèmes d'information signé avec un prestataire doit intégrer les règles de sécurité de la présente PSSI. Tout personnel du prestataire a l'obligation de prendre connaissance et de respecter la PSSI de la CTS.	1
PRE02	Tout contrat lié aux systèmes d'information doit contenir un responsable du contrat pour le prestataire et un responsable pour la CTS.	1
PRE03	À la fin de la collaboration, le responsable du contrat CTS valide la bonne clôture de celui-ci et il s'assure de la suspension de l'ensemble des accès et habilitations mis à disposition du prestataire	1
PRE04	Le prestataire peut sous-traiter une partie des prestations de services ou des travaux qui lui sont confiés uniquement avec l'accord formel et préalable de la CTS. L'ensemble des engagements pris par le prestataire en termes de sécurité s'applique aux sous-traitants. La responsabilité reste celle du prestataire et non celle du sous-traitant.	1
	Identification et accès au SI	
PRE05	L'interconnexion de tout ou partie du SI de la CTS avec un prestataire doit être approuvée par le RSSI ou le correspondant sécurité.	2
PRE06	Un inventaire exhaustif de l'ensemble des accès distants doit être constitué et maintenu à jour.	2
PRE07	Les interventions physiques sur les biens matériels du système d'information doivent être soumis à l'autorisation préalable du responsable du bien. Les prestataires ne doivent pas intervenir eux-mêmes sur les équipements sans un accord formel de ce responsable.	1

GC02-SQ419		Document associé à la procédure SQ419 Politique de Sécurité des Systèmes d'Information de la CTS	
Date : 28/09/2022	Indice : 01	PSSI-Thématiques	Page : 18 sur 18

	Services outsourcés	
PRE08	Dans le cas de services hébergés à l'extérieur de la CTS le prestataire doit être en possession d'une procédure de gestion des incidents	1
PRE09	Le prestataire doit être en possession d'une procédure de maintien en conditions opérationnelles (patch management etc ..).	1
	Contrôle d'accès	
PRE10	La CTS peut exiger certaines contraintes sur l'hébergement des données, en France ou dans l'Union Européenne	1