UES PSSI - Politique Sécurité ITS GROUP

SMIR

Système de Management Intégré Responsable

ISO 9001 - ISO 14001 - ISO 27001 - ISO 26000

Référence du document : UES_PSSI-POLITIQUE-SECURITE

42, Rue de Bellevue – 92100 Boulogne-Billancourt - Tél. : +33(0) 1 78 89 35 00 - Fax : +33(0) 1 78 89 93 95
www.itsgroup.com

Ce document exprime la politique sécurité mise en place au sein des infrastructures ITS Group et ses filiales pour garantir un niveau de sécurité convenable à ses clients. Cette politique sécurité est appliquée sur le système d'information interne mais ne représente pas un recueil des mesures mises en place sur les plateformes clientes.

SOMMAIRE

I. Les grands principes 5
II. S'engager : le maitre mot 6
III. Systématiser la sécurité auprès de tous 6
IV. Maintenir une architecture résiliente 7
4.1 Politique de Patch Management 7
4.2 Politique antivirale 8
4.2.1 Postes de travail des collaborateurs 8
4.2.2 Serveurs 8
4.2.3 Reporting / Alertes / Surveillance 8
4.3 Politique de sauvegardes 9
4.4 Gestion des traces 9
4.4.1 Généralités 9
4.4.2 Génération des traces 10
4.4.3 Collecte des traces 11
4.4.4 Hébergement de données de santé à caractère personnel 11
4.5 Gestion du temps 12
4.6 Gestion de la maintenance du matériel 12
4.7 Sécurité des serveurs 12
4.7.1 Sécurisation des serveurs Unix 12
4.7.2 Sécurisation des serveurs Windows 12
4.8 Les mesures du réseau 13
4.8.1 Isolation réseau 13
4.8.2 DDOS 14
4.8.3 Protection des applications publiques 14
4.9 Accès à la donnée 14
4.9.1 Politique de filtrage firewall 14
4.9.2 Règles de constitution des identifiants 14
4.9.3 Règles de constitution de mot de passe 15
4.9.4 Authentification 15
4.9.5 Transmission des données 16
4.9.6 Expiration de compte 16
4.10 Gestion de la sécurité logique 16
4.10.1 Gestion des privilèges 16

4.10.2 Habilitation 17
4.10.3 Réexamen des droits d'accès 18
4.10.4 Stockage des mots de passe 18
4.10.5 Transmission des identifiants et mots de passe 19
4.10.6 Déconnexion automatique des sessions inactives 19
4.10.7 Verrouillage automatique des sessions utilisateurs 19
4.10.8 Accès console 19
4.10.9 Accès VPN 19
4.11 Gestion de la sécurité physique 20
4.11.1 Datacenter 20
4.11.2 Bureaux 20
4.12 Exigences de sécurité pour les nouveaux équipements 20
4.12.1 Exigences liés aux matériels 20
4.12.2 Exigences liés aux logiciels 20
4.13 Norme de développement 21
4.13.1 Jeu d'essai 21
4.13.2 Mesures cryptographiques 21
4.13.3 Modification des logiciels 22
4.14 Gestion des incidents de sécurité 22
4.14.1 Définition 22
4.14.2 Traitement et résolution 22
V. Garantir notre continuité de service 22
5.1 Périmètre 23
5.2 Indisponibilité d'un site physique 23
5.2.1 Indisponibilité temporaire 23
5.2.2 Indisponibilité permanente 23
5.3 Indisponibilité humaine 24
5.4 Indisponibilité services vitaux 24
5.5 La cellule de crise PCA 24
5.5.1 Composition 24
5.5.2 Mission de la cellule de crise 24
5.5.3 Principe de réunion 24
5.5.4 Test de constitution de la cellule de crise 25
VI. Annexe 1 : Indicateurs SSI 25

Niveau de confidentialité :

 ◉ Public  ○ Interne  ○ Confidentiel  ○ Restreint

CARTOUCHE DE SUIVI							
Version	Rédacteur	Date	Objet	Date de transmission	Vérificateur	Date de transmission	Approbateur
V01	Céline FERREIRA	21/10/14	Création d'une politique sécurité	21/10/14	Florian PERRIN	29/10/14	Jean Claude BEAUJOT
V02	Margaux CHAUVET	0/04/15	Modification et ajout de nouvelles politiques	15/05/15	Florian PERRIN	18/05/15	Céline FERREIRA
V03	Margaux CHAUVET	16/07/15	Ajustements dossier HDS	29/07/15	Florian PERRIN	11/08/15	Geoffroy de LAVENNE
V04	Margaux Chauvet	22/12/15	Ajout des indicateurs de la PSSI	22/12/15	Florian PERRIN	22/12/15	Céline FERREIRA
V05	Florian PERRIN	11/04/16	Ajout gestion du temps et WAF	11/04/2016	Margaux CHAUVET	11/04/16	Geoffroy de LAVENNE
V06	Florian PERRIN	05/08/16	Ajout détail politique habilitation / exigence sur l'achat de matériel / Annexe indicateur SSI	17/08/2016	Margaux CHAUVET	17/08/2016	Geoffroy de LAVENNE
V07	Florian PERRIN	11/10/16	Ajustement dossier HDS	11/08/2016	Margaux CHAUVET	12/08/2016	Geoffroy de LAVENNE

CARTOUCHE DE DIFFUSION				
Date de transmission	Destinataire(s)	Moyen de transmission	Date de retour	Accord oui/non
04/11/14	ALL en document public	Mail, mise à disposition sur serveur et GED	/	/
18/05/15	ALL en document public	Mail, mise à disposition sur serveur et GED	/	/
21/08/15	ALL en document public	Mail, mise à disposition sur serveur et GED	/	/
17/08/2016	ALL en document public	mise à disposition sur serveur et GED	/	/
14/10/16	ASIP Santé	Format papier et clé USB	/	/

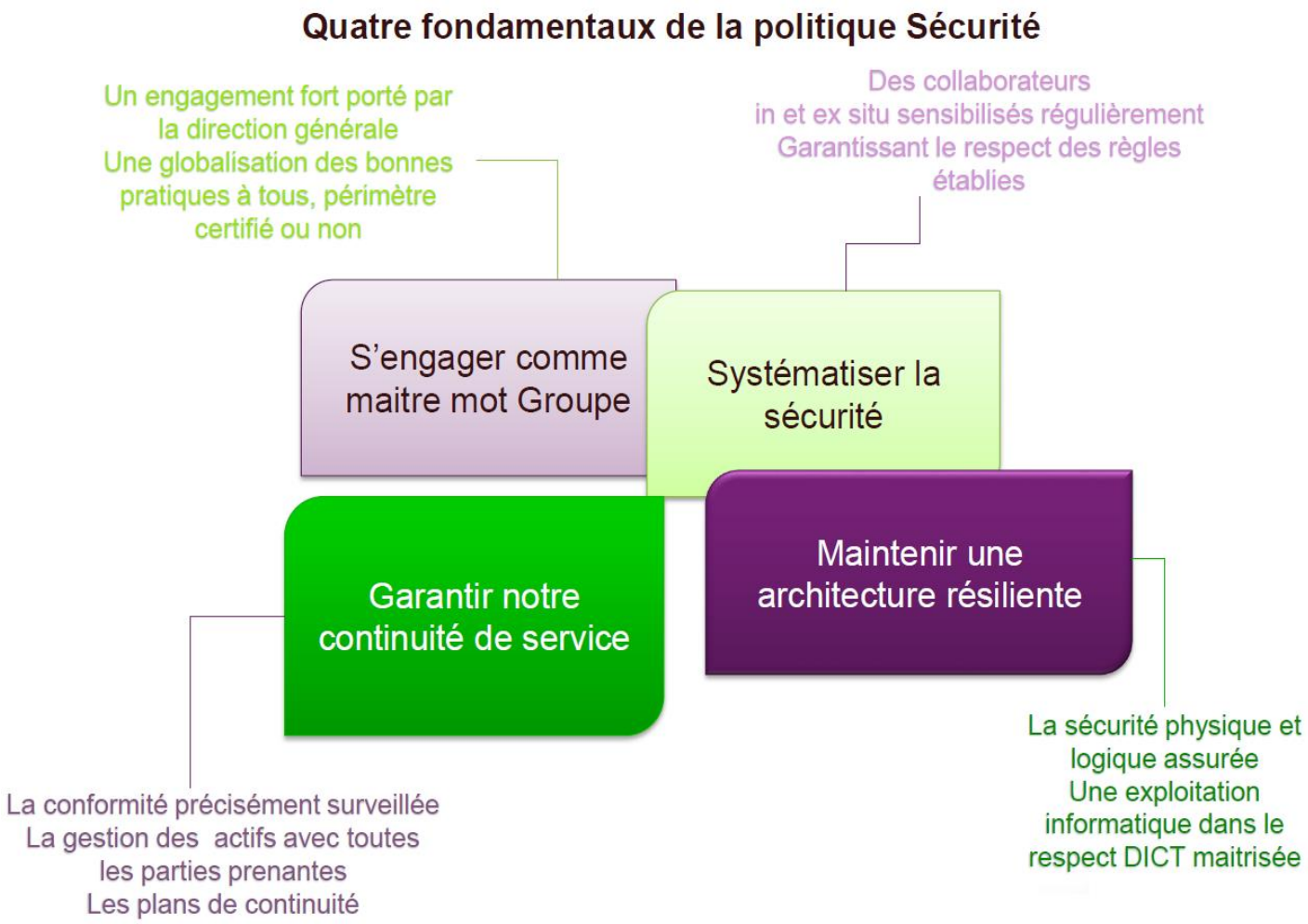
I. Les grands principes

ITS Group s'engage à assurer une qualité de service optimale, en rendant disponibles les applications confiées, et aussi en garantissant une réactivité importante lorsqu'un incident survient, ou que le client émet une demande.

Afin de préserver la disponibilité, l'intégrité, la confidentialité et la traçabilité (DICT) de l'information, ITS Group intègre dans ses activités une politique de sécurité de l'information, dans laquelle est présenté l'ensemble des mesures de sécurité ainsi que les règles de bonnes pratiques, applicables aux activités de l'entreprise.

Les activités de Cloud Computing, d'infogérance outsourcée et hébergement à valeur ajoutée sont d'ores et déjà certifiées ISO 27001. Cet engagement démontre l'intérêt du groupe à s'engager dans cette politique, et la volonté de respecter les règles de l'art en matière de sécurité de l'information.

Nos objectifs fondamentaux sont :



II. S'engager : le maitre mot

Basée sur le respect de l'ISO 27005, l'appréciation des risques en matière de sécurité de l'information se déroule à minima annuellement et est pilotée par le Responsable Sécurité des Systèmes d'Informations (RSSI). Cette analyse peut également être déclenchée en cas de changements impactant, tant organisationnels que techniques.

Les résultats sont présentés en revue de direction et la décision quant au seuil d'acceptabilité des risques est décidée puis annoncée dans la lettre d'engagement rédigée par le dirigeant, à l'attention de toutes les parties prenantes.

En découlent des actions qui sont identifiées et validées dans le Plan de Traitement des Risques (PTR) garant du suivi et du déroulement des initiatives en matière de réponse à l'appréciation des risques.

Une déclaration d'applicabilité nous permet de présenter les dispositions établies pour répondre aux 113 exigences de l'ISO 27002 conformément à notre certification.

Une veille réglementaire et technologique précise assurée par les leaders sécurité ainsi que notre collaboration avec des organismes tels que la Commission Nationale de l'Informatique et des Libertés, le Syntec, l'Agence Nationale de la Sécurité Informatique nous permettent de mettre en œuvre des actions supplémentaires, de les piloter et de les contrôler dans le temps.

Ainsi, les mesures instaurées sont applicables à différentes activités :

- Accès logiques et physiques
- Charte informatique
- Classification et transmission de la donnée
- Contrôle des accès aux données
- Identifiant unique, gestion des privilèges
- Implication du personnel
- Management des actifs
- Usage réseau

La force de notre engagement réside dans la globalisation des pratiques sécurité, quel que soit le périmètre même non certifié. Cette généralisation est assurée en transverse grâce au service QSE Groupe.

III. Systématiser la sécurité auprès de tous

La charte informatique (Charte ITCom), ainsi que l'engagement de confidentialité, permettent à ITS Group d'impliquer les collaborateurs dans la démarche de sécurité de l'information globale. Au-delà du périmètre certifié, ITS Group fait le choix également de diffuser les bonnes pratiques à l'ensemble de ses collaborateurs.

La charte informatique constitue un élément d'engagement et de responsabilisation des salariés. Ce document garantit que le collaborateur connait les règles générales à appliquer, afin de protéger l'accès aux données à travers le matériel qui lui est confié, mais aussi afin de garantir la préservation des dispositifs de sécurité en place et la valeur de la confidentialité de l'information

L'engagement de confidentialité, comme la charte informatique, est présenté lors de la signature du contrat de travail, en annexe. L'engagement de confidentialité peut être transmis sur demande aux clients lors des audits.

La nomination de leaders sécurité permet d'accompagner la mise en œuvre, dans chaque service, des bonnes pratiques, en étant l'interface entre le RSSI et les collaborateurs.

Par ailleurs, les collaborateurs sont régulièrement conviés à des ateliers dans le but de les informer et de les sensibiliser aux nouveaux outils de sécurité, à l'évolution des exigences réglementaires et aux bonnes pratiques. La newsletter interne est également un support essentiel de la communication sur les aspects sécurité. Enfin, le plan de formation annuel permet de répondre aux besoins des collaborateurs en termes de compétences, et d'anticiper les évolutions de l'environnement.

IV. Maintenir une architecture résiliente

Lors de l'appréciation des risques, une liste des actifs est dressée selon le périmètre technique certifié. Il est précisé pour chaque actif son propriétaire, et la politique applicable à son utilisation.

De plus, chaque donnée est soumise à une classification, qui a pour but de définir les conditions de manipulation, de criticité, selon les exigences légales. Pour les données contenues dans des supports amovibles, tels que les ordinateurs portables, une procédure est mise en place afin de déterminer précisément les conditions de mise à disposition, et de transfert.

Les politiques essentielles de sécurité sont :

- Patch management
- Antivirus
- Sauvegardes
- Gestion des traces
- Gestion maintenance matériel
- Gestion du réseau
- Contrôles accès aux données
- Contrôles accès logiques
- Contrôles accès physiques
- Normes nouvelles applications
- Normes de développementGestion des incidents
- Capacity Planning

4.1 Politique de Patch Management

ITS procède à la mise à jour complète des systèmes. Cela regroupe les mises à jour de sécurité et les mises à jour d'applications (correction de bugs). Les mises à jour sont effectuées de façon automatique et quotidienne. L'horaire des mises à jour est compris dans une plage horaire (même principe que les sauvegardes).

Les systèmes disposent ainsi de l'ensemble des correctifs relatifs aux applications.

Les serveurs compromis au niveau sécurité et entraînant des désagréments sur le réseau sont susceptibles d'être isolés afin de garantir la pérennité des infrastructures.

Les mises à jour de sécurité nécessitent parfois les redémarrages des machines, des plages de maintenance doivent être prévues (au moins une fois par semaine).

Taux moyen de réussite des patchs pour ITS Integra

Quantité de patchs disponibles

Taux d'équipements compatibles avec la politique de MAJ

4.2 Politique antivirale

Dans le cadre de la lutte antivirale, ITS met en œuvre les procédures suivantes :

4.2.1 Postes de travail des collaborateurs

L'ensemble des postes de travail des collaborateurs doit disposer d'un logiciel antivirus avec des mises à jour régulières.

Les postes doivent procéder à une mise à jour quotidienne de la base de signatures antivirus et effectuer au moins une fois par semaine un scan complet de façon automatique.

En cas de détection d'un fichier malveillant, les actions suivantes sont réalisées de façon automatique, dans l'ordre :

- Tentative de réparation du fichier
- Tentative de mise en quarantaine du fichier
- Tentative de suppression du fichier

En cas d'échec des différentes actions automatiques, l'équipe sécurité prend en charge le nettoyage du poste.

Les postes de travail Windows étant fortement exposés, il est procédé de façon biannuelle à un scan antivirus avec un outil tiers. Celui-ci est réalisé avec un outil en ligne afin de garantir son intégrité vis-à-vis de la machine.

Le RSSI définit les périodes où seront réalisés les tests complémentaires ainsi que la procédure.

Le résultat des tests complémentaires est consigné sur l'outil de GED.

4.2.2 Serveurs

Les serveurs ITS doivent disposer d'un antivirus mis à jour à minima quotidiennement. Un scan global est réalisé une fois par semaine la nuit.

Concernant les anti-virus en temps réel, afin que l'impact sur les performances soit limité, les mesures suivantes sont prises:

- La protection active ne concerne que les créations ou modifications de fichiers
- Les partitions systèmes sont exclues de la surveillance active en dehors du /tmp sous Linux
- Une liste de répertoires standards est exclue (logs / Fichiers BDD par exemple)

Le traitement des fichiers malveillants suit la même procédure que celle appliquée aux postes de travail des collaborateurs.

4.2.3 Reporting / Alertes / Surveillance

Les différents outils doivent être configurés afin d'envoyer des alertes par mail au service sécurité.

Le bon fonctionnement de la mise à jour des signatures est surveillé en temps réel par l'outil de monitoring.

Une alerte visuelle est levée dans la console de monitoring si la date de la dernière mise à jour des signatures est supérieure à 3 jours.

Taux d'agent antivirus à jour 

4.3 Politique de sauvegardes

ITS applique en interne une sauvegarde de ses données sur son architecture de sauvegarde mutualisée, selon les modalités de notre politique de sauvegarde 'standard', précisées dans le tableau suivant :

Périmètre de sauvegarde	Type	Fréquence	Rétention	Fenêtre
Ensemble des composants du SI (système, configuration, données applicative, traces de sécurité)	Incrémental	Quotidienne	Deux semaines	De minuit à 9 heures
	Complète	Hebdomadaire	Deux mois	Dimanche, début à minuit
	Complète	Mensuel	Un an	Dimanche, début à minuit

Pilotés depuis un réseau d'administration dédié, les back-ups sont répliqués sur le data center distant (celui n'hébergeant pas les serveurs en question) via notre réseau MAN 10Gb/s redondé en fibre noire reliant les centres de La Courneuve et Saint-Denis. La réplication utilise un transfert disque à disque.

Les systèmes de stockage sur disques (SATA en Raid6) composant cette architecture sont basés sur deux équipements EMC Data Domain DD670 fortement évolutives, une sur chaque site d'hébergement principal- PAR5 (ITC5) et PAR7 (ITC7).

Les DD670 permettent nativement la déduplication; c'est-à-dire la factorisation des données sauvegardées en stockant une information une seule fois au lieu de recopier toutes les données à chaque nouvelle sauvegarde complète.

Le pilotage des tâches de sauvegarde est réalisé grâce à la solution Evault.

Un test de restauration est réalisé systématiquement à la fin de chaque intégration, avant la mise en production de la plateforme et aléatoirement toutes les semaines sur l'architecture globale.

Lors de l'installation des systèmes, des tests de sauvegarde et de restauration sont réalisés automatiquement afin de valider le processus complet. Des tests de restaurations réguliers sont ensuite mis en place durant le cycle de vie du système.

Taux de réussite des sauvegardes

Taux de réussite des tests de restauration

4.4 Gestion des traces

4.4.1 Généralités

L'ensemble des équipements ITS ainsi que les équipements administrés par sa filiale ITS Integra transfèrent leurs traces techniques en temps réel sur des serveurs dédiés à cette tâche :

- Applications conformément aux contrats et demandes des clientsBases de données
- Certains composants logiciels standards (serveurs web, java, middleware, EAI, ETL…)
- Outil de gestion des sauvegardes
- Outils d'administration (notamment bastion d'administration et stockage)
- Réseaux (tout dispositif de filtrage et notamment pare-feu de cloisonnement)
- Systèmes (physiques et virtuels)

Sont également tracés toutes intrusions physiques par le biais de caméras et de cahier de visites permettant la journalisation des passages.

4.4.2 Génération des traces

. Les évènements de sécurité à tracer sont les suivants :

- Opération sur les habilitations
  - La création/suppression/modification/désactivation/activation d'un compte
  - L'attribution/suppression/modification de droits

- Opération pouvant avoir un impact sur la sécurité du SI
  - L'accès aux interfaces d'administration (ajout, modification, suppression)
  - L'accès technique ou applicatif à des données de santé (lecture, ajout, modification, suppression)
  - L'accès technique ou applicatif à des données personnelles (lecture, ajout, modification, suppression)
  - Les modifications de configuration
  - L'accès au système de gestion des évènements lui-même

- Accès tiers
  - Connexions à l'infrastructure d'hébergement
  - Une fois connecté, toute opération, en traçant les mêmes évènements de sécurité que pour le personnel interne
  - Accès physique

Les traces permettent une surveillance des opérations et d'investiguer dans le cas d'un incident de sécurité. Elles permettent d'identifier :

- L'action journalisée
  - Tentative d'authentification (succès et échec)
  - Connexion à un environnement/déconnexion
  - Création/suppression/modification/activation/désactivation d'un compte
  - Attribution/suppression/modification de droits
  - Action technique (ajout d'une règle pare-feu…)
  - Motif de la visite, date, heures et intervenants pour un accès physique

- La source de l'action
  - Identifiant de la personne
  - Equipement (IP, hostname)

- La date et l'heure de l'action, provenant d'une source de temps unique

- Le statut de l'action
  - Réussite/échec
  - Alerte
  - Erreur
  - NA si impossible

Les traces applicatives sont générées conformément aux exigences spécifiées dans les contrats avec les clients.

Les traces applicatives ne peuvent contenir de données de santé, sans quoi les traces elles-mêmes seront soumises à l'agrément pour l'hébergement de données de santé. A cet effet, les traces sont générées de façon à être strictement dissociables des données de l'application, notamment les données de santé.

S'il est spécifié dans le contrat avec un client que les traces applicatives sont collectées par ITS, alors les traces sont générées dans un format communément admis de gestion des traces. Ainsi les traces seront compatibles avec le système de centralisation, et seront exploitables si nécessaire. Ces formats sont les suivants : syslog, format Microsoft, fichiers csv ou texte.

4.4.3 Collecte des traces

Les traces de sécurité générées sont centralisées de façon à garantir qu'elles ne peuvent être supprimées ou modifiées. Si des traces ne peuvent être centralisées, l'exception est validée par le RSSI.

Les traces de sécurité doivent être centralisées de façon synchrone (temps réel) afin qu'une analyse puisse être réalisée.

Les traces sont horodatées et la source de temps de tous les équipements générant des traces est unique. Le service de temps retenu est le service NTP fourni par ITS Integra.

Les traces sont conservées pour une durée de 1 an et uniquement 1 an sauf en cas de nécessité (procédure judiciaire). Au-delà de cette durée définie, les traces sont supprimées définitivement.

L'accès aux traces s'effectue à distance à travers une connexion sécurisée et une authentification nominative par identifiant / Mot de passe.

L'accès en lecture seule est possible à l'ensemble des collaborateurs du pôle technique dans le cadre de leur travail.

L'accès en écriture aux serveurs de centralisation des traces est restreint à la direction sécurité afin d'empêcher :

- La modification des types de messages
- La modification ou la suppression des fichiers de traces

De plus, une surveillance active est positionnée dans l'outil de supervision afin d'éviter une saturation de la partition qui bloquerait l'écriture des traces et donc la récolte de celles-ci.

Toutes les traces collectées sont sauvegardées de façon à garantir que les traces sont disponibles, même en cas de destruction du support physique.

Les traces sont intégrées au processus de sauvegarde propre à l'infrastructure d'hébergement de données de santé. Les sauvegardes qui garantissent la complétude, l'intégrité et la confidentialité des traces sont réalisées et sont externalisées.

Les traces récoltées font l'objet d'une analyse afin de détecter toutes défaillances ou tentatives d'intrusions. Cette analyse est réalisée par le SIEM de ITS Integra qui est en charge de faire de la corrélation et de l'analyse plus poussée des traces. Cette analyse a pour objectif le déclenchement d'alerte en cas de comportement suspect.

Pour les traces physiques, elles sont gérées par notre fournisseur de Datacenter.

4.4.4 Hébergement de données de santé à caractère personnel

Dans le cadre de l'hébergement de données de santé à caractère personnel, en plus des dispositions habituelle, la solution Wallix Admin Bastion est systématiquement mise en œuvre. Cette solution permet une traçabilité complète des actions des administrateurs systèmes, qu'ils soient Linux / Unix ou Windows. Elle permet d'enregistrer les sessions d'administration et de les visionner ultérieurement en cas de besoin (audit, incident, forensics, …). Elle permet également de garantir à la fois l'imputabilité des connexions et l'imputabilité des actions.

Dans l'architecture d'Hébergement des Données de Santé, cette solution de traçabilité est placée dans la DMZ d'administration réservée à ITS Integra.

Taux de déploiement du Syslog 

4.5 Gestion du temps

Chaque serveur et chaque équipement réseaux ou sécurité doivent synchroniser leurs horloges sur une source de temps stable et redondée. Cette source doit se synchroniser elle-même sur au minimum 2 sources de strate 1 sur Internet.

Un potentiel décalage horaire sur les équipements doit être supervisé pour permettre une correction rapide.

4.6 Gestion de la maintenance du matériel

Lors de l'achat de nouveau matériel, une garantie initiale auprès du constructeur est systématiquement souscrite. Celle-ci est généralement de 1 ou 3 ans. Pour les équipements dits sensibles et si cela est possible, un support en 24/7 avec intervention en 4h est souscrit. Pour les autres équipements, le support reste en heures ouvrées et le remplacement est fait en J+1.

Le renouvellement du support à la fin de la période initiale est réalisé uniquement sur les équipements sensibles.

ITS dispose d'un stock avec des composants de secours permettant de palier à des défaillances matérielles pour les équipements dont le support est à échéance.

4.7 Sécurité des serveurs

4.7.1 Sécurisation des serveurs Unix

La sécurité des serveurs Unix / Linux au sein d'ITS Integra s'applique en deux temps :

- Application d'un script de post installation lors de l'installation automatique du serveur
- Application des classes Puppet.

Les points suivants sont mis en œuvre dans le cadre de leur sécurisation :

- Arrêt des services inutiles
- Suppression des packages système inutiles
- Création de comptes locaux de secours
- Intégration de la machine dans l'authentification Active Directory
- Configuration de l'externalisation des logs
- Configuration des sauvegardes
- Configuration du monitoring
- Configuration de l'agent Puppet permettant un maintien de conformité
- Configuration de l'inventaire automatique
- Configuration de la synchronisation temporelle
- Configuration de la politique de mise à jour
- Configuration de la politique de mot de passe
- Configuration des accès distants
- Mise en place de droits spécifiques sur l'arborescence.

Par la suite, des scripts de sécurisation standards sont mis en œuvre en fonction du rôle du serveur (serveur Web, serveur BDD, serveur applicatif).

4.7.2 Sécurisation des serveurs Windows

La sécurité des serveurs Windows au sein d'ITS Integra s'applique en deux temps :

- Application d'un script de post installation lors de l'installation du serveur
- Application des stratégies de groupe lors de l'intégration au sein d'un domaine AD.

Les points suivants sont mis en œuvre dans le cadre de la sécurisation des serveurs Windows :

- Arrêt des services inutiles
- Suppression des packages système inutiles
- Création de comptes locaux de secours et renommage du compte Administrateur
- Intégration de la machine dans l'authentification Active Directory
- Configuration de l'externalisation des logs
- Configuration des sauvegardes
- Configuration du monitoring
- Configuration de l'inventaire automatique
- Configuration de la synchronisation temporelle
- Configuration de la politique de mise à jour
- Configuration de la stratégie de mot de passe
- Configuration des accès distants
- Mise en place de droits spécifique sur l'arborescence.

Par la suite, des scripts de sécurisation standards sont mises en œuvre en fonction du rôle du serveur (serveur Web, serveur BDD, serveur applicatif).

Taux de serveurs intégrés dans l'AD

4.8 Les mesures du réseau

De nombreuses mesures afin de sécuriser les réseaux de l'entreprise sont mises en œuvre et répondent à l'annexe 27002 dans le document de déclaration d'applicabilité.

Les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation. Dans ce cadre, différentes mesures sont en place au niveau réseau et applications.

Les services dédiés à l'administration des systèmes et l'exécution du métier d'ITS sont réservés à la population technique de l'entreprise.

Dans le cas où de tels services doivent être accessibles par une population non technique, des profils utilisateurs doivent être en place afin d'interdire toutes modifications des données.

4.8.1 Isolation réseau

L'isolation des plateformes de chacun des clients est obligatoire et il peut exister, pour une même plateforme, plusieurs types de sous-réseaux. Les différents sous réseaux sont tous isolés les uns des autres par des firewalls qui font soit partie de la production, soit du réseau d'administration ITS Integra. Cela assure une étanchéité et un contrôle minutieux des différents flux de données.

Les différents sous-réseaux sont les suivants :

- ITC : Le réseau ITC est de coloration jaune et représente le réseau d'administration, de supervision et de sauvegarde. Son accès est réservé aux administrateurs ITS et sa configuration est en PVLAN
- PROD : Le réseau PROD est de coloration verte et représente le réseau de production pour les accès des utilisateurs. Son accès est réservé aux utilisateurs et sa configuration peut être en PVLAN ou en VLAN en fonction de la conception de la plateforme
- BKE : Le réseau BKE est de coloration bleue et représente le réseau d'interconnexion entre les serveurs d'une même plateforme. Son accès est restreint aux uniques serveurs connectés sur ce réseau, il ne contient pas de GW (sauf exception avec une isolation de niveau 3 entre différents réseau BKE) et sa configuration est en VLAN
- STO : Le réseau STO est de coloration rouge et représente le réseau dédié d'interconnexion entre les serveurs et l'équipement de stockage en réseau (ISCSI, NFS, CIFS). Son accès est

restreint aux uniques serveurs connectés sur ce réseau, il ne contient pas de GW et sa configuration est en VLAN

- DRAC : Le réseau DRAC est de coloration blanche et représente le réseau d'accès aux consoles de managements des équipements (ILO, DRAC, MM etc.). Son accès est réservé aux administrateurs ITS INTEGRA et sa configuration est en VLAN.

4.8.2 DDOS

ITS Integra a choisi Arbor Networks, l'un des principaux fournisseurs de solutions de gestion et de sécurité réseau pour les entreprises et les fournisseurs de services. Une solution globale (Arbor Peakflow SP), permettant de surveiller et de sécuriser infrastructures et trafics, est utilisée. Devenu un standard international, Arbor Peakflow SP protège aujourd'hui plus de 70% du trafic Internet mondial.

L'ensemble des services fournis sur internet doit bénéficier de la protection Anti DDOS afin de garantir la disponibilité et la visibilité de nos infrastructures.

Taux de services configurés en protection DDOS 

4.8.3 Protection des applications publiques

Les différentes applications publiques (sites web, portail client, évènementiel) doivent faire l'objet d'une attention particulière. En effet, celles-ci sont plus largement exposées aux risques externes. De fait, les différents services disponibles sur Internet doivent être protégés par un firewall applicatif (WAF) permettant de bloquer les attaques.

4.9 Accès à la donnée

4.9.1 Politique de filtrage firewall

Par défaut, l'ensemble des flux réseau est bloqué au niveau des différents firewalls. Pour faire transiter un nouveau flux, il est nécessaire d'en faire la demande au service sécurité qui effectue certains contrôles puis procède à l'ouverture en suivant scrupuleusement la procédure décrite dans le Wiki.

Dans le cadre d'une demande d'ouverture firewall concernant un flux sensible, l'équipe sécurité doit obtenir l'approbation du RSSI avant de réaliser l'ouverture.

4.9.2 Règles de constitution des identifiants

Les identifiants de connexion sont normés de la forme : pnom (première lettre du prénom suivi du nom complet) pour les collaborateurs internes et pnom-ext pour les prestataires externes à l'entité.

Exemple : Michel Nom - mnom

Deux cas particuliers sont à prendre en compte :

Dans le cas de prénoms composés, les premières lettres de chacun des prénoms suivis du nom sont utilisées

Exemple : Jean-Pierre Nom - jpnom

Dans le cas de noms composés, il faut les concaténer en un seul nom.

Exemple : Jean-Pierre du Nom - JPdunom

4.9.3 Règles de constitution de mot de passe

La constitution d'un mot de passe doit respecter les règles suivantes, à savoir il :

- Doit être composé d'une longueur supérieure ou égale à 10 caractères
- Doit avoir obligatoirement une durée de vie maximale de 180 jours
- Ne doit pas être composé d'aucun terme propre à l'utilisateur ou à l'entreprise
- Ne doit pas être enregistré en clair (au sein d'un fichier), ni pouvoir être déduit par une fonction quelconque ou d'une chaîne de caractères
- Doit être différent des 10 derniers mots de passe
- Doit être construit d'au moins une minuscule, une majuscule, un chiffre.

Info : Un générateur de mots de passe est disponible ici.

4.9.4 Authentification

- AUTHENTIFICATION FORTE

L'authentification forte d'ITS Integra s'effectue à travers deux voies différentes, et est basée sur un certificat et un mot de passe. Les certificats électroniques sont uniques et personnels, ils attestent de l'identité de l'administrateur. Le mot de passe de l'administrateur est stocké sur l'annuaire de l'entreprise et est associé à son login personnel. Pour s'authentifier, il est indispensable d'être en possession du certificat et du mot de passe. Cette authentification forte correspond à une première authentification obligatoire pour l'ensemble des collaborateurs.

Les certificats sont attribués personnellement pour un membre de l'équipe Sécurité, lors de la procédure INOUT. Chaque demande de nouveau certificat doit être validée par un manager. Seuls les membres de l'équipe sécurité peuvent attribuer et révoquer un certificat.

- AUTHENTIFICATION SIMPLE

L'authentification simple est gérée par un unique facteur :

- Par mot de passe : politique des mots de passe présentée au paragraphe précédent
- Par SSO : basée sur les principes de kerberos, cette authentification permet aux administrateurs de se connecter aux architectures clients. Cette technologie permet d'éviter la transmission de mots de passe sur le réseau en privilégiant l'utilisation de jetons.

- AUTHENTIFICATION DES COMPOSANTS

Les postes des utilisateurs ITS sont authentifiés avec l'adresse MAC de leur ordinateur. Le service DHCP est configuré pour attribuer une adresse IP fixe spécifique en fonction de l'adresse MAC de l'ordinateur.

Les authentifications mises en œuvre sont réparties de la façon suivante :

Composants	Type d'authentification	Architecture
Système d'exploitation	Identifiant / Mot de passe	Authentification centralisée
Bases de données	Identifiant / Mot de passe	Authentification locale
Applications	Authentification forte	Authentification locale ou centralisée
Composants réseaux	Identifiant / Mot de passe	Authentification centralisée
Composants de sécurité	Identifiant / Mot de passe	Authentification centralisée
Composants de sauvegarde	Identifiant / Mot de passe	Authentification locale
Composants de supervision	Identifiant / Mot de passe	Authentification centralisée

Composants d'exploitation ou d'administration	Identifiant / Mot de passe	Authentification centralisée
Accès distants	Authentification forte	Authentification centralisée

- CONTROLE DE L'AUTHENTIFICATION

Un contrôle des authentifications Identifiant / Mot de passe est réalisé annuellement. Lors de ce contrôle, des tests de complexité de mot de passe sont réalisés sur quelques comptes aléatoirement.

4.9.5 Transmission des données

La transmission de données doit respecter la politique de classification des documents.

- Transmission de mots de passe

La transmission de mots de passe doit être faite via 2 canaux différents (téléphone, SMS, mail, Shareit)

- Transmission de documents numériques

La transmission de documents numérique doit respecter les règles suivantes :

- Respecter les règles de classification de l'information
- Être réalisée au maximum par l'application de partage sécurisé : Shareit
- Être réalisée dans un format non modifiable, il faut privilégier le format PDF plutôt que Word, Excel, etc ...

- Transmission électronique

Les courriels émis par la société doivent contenir la signature numérique qui est fournie au collaborateur.

En cas de transmission de données sensibles via courriel, il peut être nécessaire de chiffrer celui-ci à l'aide du certificat, en accord avec la politique de classification des documents.

4.9.6 Expiration de compte

Un processus d'expiration des comptes est en place au niveau de l'annuaire centralisée Active Directory.

Tous comptes inactifs depuis plus de 30 jours sont automatiquement verrouillés. Cette mesure concerne aussi bien les comptes utilisateurs que les comptes de machines.

Taux de mots de passe avec expiration 

4.10 Gestion de la sécurité logique

4.10.1 Gestion des privilèges

Toutes applications ou systèmes au sein d'ITS doivent disposer d'une gestion des privilèges. Pour les applications, les privilèges doivent définir au moins 2 profils. Un en lecture seule et un en lecture-écriture.

Les privilèges sont attribués sur demande du manager et après validation du RSSI lors notamment du déroulement de la procédure INOUT.

Toujours dans le cadre de cette procédure, les privilèges sont supprimés lors du départ d'un collaborateur. Une désactivation automatique devra être programmée pour les contrats à durée déterminé (CDD, Stage, Prestataire).

4.10.2 Habilitation

a. Principes d'habilitation interne

Chaque utilisateur dispose d'un identifiant unique et personnel lui permettant d'accéder aux ressources de l'entreprise et aux ressources des clients de l'entreprise dans le cas de l'activité d'hébergement.

Les identifiants sont créés selon les règles exposées au paragraphe « Règles de constitutions des identifiants ».

L'utilisation de comptes génériques sur les systèmes, composants, journaux ou applications est strictement interdite. L'identification d'éventuels comptes génériques est réalisée par le biais de la surveillance active des systèmes (SIEM) et par le contrôle des habilitations et des profils présent sur les différentes applications.

Les habitations sont fournies à durée indéterminée tant que l'utilisateur ne change pas de rôle dans l'entreprise ou en cas d'absence exceptionnelle.

La révision des habilitations a lieu lors de l'émission d'un changement au niveau de la fiche INOUT (changement de service, départ).

L'attribution d'un utilisateur à un groupe est donc réalisée via la procédure INOUT sous contrôle du RSSI (contrôles trimestriels aléatoires).

Par précaution, les utilisateurs ne peuvent accéder que aux applications dont ils ont besoin pour travailler, pas plus, pas moins.

En cas d'absence exceptionnelle de plus de 30 jours (maladie, vacances), les différents accès du collaborateur peuvent être suspendus jusqu'à son retour afin d'éviter tout acte d'usurpation d'identité sur son compte.

b. Principes d'attribution des groupes

D'une façon générale, il existe plusieurs profils d'utilisateurs. Les groupes utilisateurs correspondent à divers profils d'accès tant au niveau système qu'au niveau applicatif.

Les groupes sont créés selon la convention de nommage des groupes AD.

Au sein de la filiale ITS Integra, cinq grands profils d'utilisateurs sont utilisés :

- N1-Public : Accès utilisateurs sans accès administrateur aux serveurs, il dispose néanmoins d'accès sur des applicatifs. Ce profil est attribué aux utilisateurs standards (Commerciaux / Chef de projet / Administratifs).
- N2-Interne : Accès administrateur aux systèmes clients autorisant l'intervention de sous traitants. Profil attribué à la prestation
- N3-Confidentiel : Accès administrateur aux systèmes clients n'autorisant pas l'intervention de sous traitant. Profil initial des collaborateurs internes techniques.
- N4-Restreint : Accès administrateur aux systèmes internes de la société. Profil attribué au cas par cas en fonction des besoins.
- N5-Secret : Accès administrateur aux systèmes internes sensibles de la société (équipements de traçabilité / coffre fort numérique). Ce profil est attribué à un nombre très limité de collaborateurs de forte confiance.

On retrouve ensuite des profils d'habilitation liés aux compétences de l'individu et de sa fonction, par exemple :

- Accès sur les équipements réseaux et les équipements de sécurité (Firewall, IDS, etc.)
- Accès à la gestion des baies de stockage
- Accès administrateur virtualisation (ESX, vcenter)
- Accès aux équipements de sauvegarde
- Etc …

La liste exhaustive des différents groupes de sécurité est maintenue par le RSSI qui valide en concertation avec les managers l'affectation du personnel dans les différents groupes d'utilisateurs.

c. Principes d'habilitation HDS

Dans le cadre de l'hébergement des données de santé à caractère personnel (HDS), les différentes habilitations font l'objet d'une validation de la part du médecin hébergeur. Pour des raisons d'impartialité, le médecin hébergeur valide les habilitations en fonction des profils. L'attribution du personnel nominativement sur les profils ainsi validé est à la charge du RSSI.

4.10.3 Réexamen des droits d'accès

Un réexamen trimestriel est réalisé afin d'identifier tout écart dans les droits d'accès ou des accès qui ne sont plus pertinents. Le réexamen est réalisé par les leaders sécurité ou le RSSI et sont étudiés lors des comités sécurité.

Le réexamen a lieu sur l'ensemble des applications et dans la gestion des identités ITS (Active directory).

Sont étudiés :

- La liste des comptes actifs
- L'appartenance aux groupes
- Les profils associés aux groupes

A l'issu du réexamen, les actions correctives sont consignées dans le rapport d'audit et la correction des droits est réalisée dans les plus brefs délais. Si nécessaire, une vérification auprès du manager peut être effectuée.

Lors du réexamen des droits d'accès, il est contrôlé par la même occasion la présence de comptes illégitimes sur les différents équipements. Si des comptes illégaux sont découverts, leur désactivation est immédiate.

4.10.4 Stockage des mots de passe

L'ensemble des mots de passe doit être stocké dans un environnement sécurisé, à savoir :

- keepass (un par client) pour l'activité d'infogérance
- Passi concernant l'activité hébergement et l'usage interne

L'écriture d'un mot de passe au sein d'un script ou d'une application doit être faite dans un format non réversible (qui ne permet pas de le restituer).

Attention : Le stockage de mots de passe, sans exception, est strictement interdit sur les postes utilisateurs.

4.10.5 Transmission des identifiants et mots de passe

En interne, les identifiants et mots de passe sont transmis par le biais des coffres forts numériques (cf stockage des mots de passe).

La transmission des accès à un client doit être réalisée par le biais de 2 canaux différents, 3 possibilités existent :

- Transmission de l'identifiant par mail et du mot de passe par SMS via l'interface client
- Transmission de l'identifiant par mail et du mot de passe par téléphone
- Transmission des identifiants dans un fichier chiffré en fonction des accords de chiffrement préalablement établis avec les clients.

4.10.6 Déconnexion automatique des sessions inactives

Les sessions utilisateurs sur les serveurs Microsoft et Linux sont déconnectées automatiquement après **2 heures** d'inactivité.

4.10.7 Verrouillage automatique des sessions utilisateurs

Les sessions graphiques sont configurées pour se verrouiller automatiquement après 5 minutes d'inactivité.

4.10.8 Accès console

Les accès console sont réalisés à distance au travers des cartes de contrôle à distance (DRAC, ILO, UCS, etc…). Cet accès console est systématiquement protégé par utilisateur / mot de passe. Dans la mesure du possible, l'accès utilise l'authentification nominative centralisée.

4.10.9 Accès VPN

Au sein de la filiale ITS Integra, l'utilisation d'un accès VPN est obligatoire sur l'ensemble des postes quel que soit leur emplacement physique ou leur type (fixe et portable). L'accès VPN est nécessaire aussi bien depuis les locaux d'ITS qu'en situation de nomadisme.

Cet accès est réalisé à l'aide d'une authentification forte composée de certificats X509 et d'un couple identifiant / mot de passe. Les certificats ainsi que les identifiants sont nominatifs et ne peuvent être utilisés qu'une seule fois en simultanée.

Il existe 3 types de VPN donnant accès à des ressources différentes (segmentation au niveau réseau) :

- Accès Administratif permettant l'accès aux outils internes uniquement
- Accès Technique permettant l'accès aux outils internes et à l'ensemble des serveurs hébergés et infogérés
- Accès Prestataire permettant d'accéder à des ressources prédéfinies en fonction du besoin.

Afin de garantir un accès permanent, la solution VPN est redondée sur 2 sites physiques différents.

Seuls les accès technique et prestataire permettent d'accéder aux serveurs. Dans le cadre de l'hébergement de données de santé, les accès prestataire ne sont pas autorisés

Taux d'écarts lors de la revue des droits	

4.11 Gestion de la sécurité physique

ITS gère la sécurité physique de ses locaux au niveau du siège et des agences. L'accès physique aux datacenters est garantie par des fournisseurs de colocation spécialisés certifiés notamment ISO 27001. Une procédure d'accès physique est disponible pour chaque site en Ile-de-France.

- Datacenter de La Courneuve
- Datacenters de Saint-Denis
- Siège social de Boulogne-Billancourt

Les accès sont essentiellement contrôles par la biométrie au siège d'ITS à Boulogne, et par badge personnel et incessible aux datacenters.

4.11.1 Datacenter

Les bâtiments type Datacenter doivent répondre à minima aux protections suivantes :

- Détection et extinction incendie automatisées
- Environnement climatique redondé
- Environnement électrique double alimenté et secouru (onduleurs et générateurs)
- L'accès à un serveur nécessite un contrôle d'accès à minimum 4 niveaux (exemple : parking, PC sécurité, zone technique, suite, baie)
- Murs renforcés
- Portes et issues de secours sous alarme
- Présence d'une équipe sécurité 24/7/365
- Présence de vidéo surveillance
- Procédure d'accès sur accréditations.

4.11.2 Bureaux

Les bâtiments type bureaux doivent disposer à minima des protections suivantes :

- Alarme intrusion
- Contrôle d'accès par biométrie
- Détection incendie automatisée
- Existence d'une procédure d'accès visiteur
- Murs en dur
- Présence de vidéo surveillance.

4.12 Exigences de sécurité pour les nouveaux équipements

4.12.1 Exigences liés aux matériels

Lors de l'acquisition de matériel physique destiné à un environnement datacenter, il est nécessaire de respecter les exigences suivantes :

- Présence d'une double alimentation électrique (ou possibilité de mise en place de STS le cas échéant),
- Présence d'une carte de contrôle à distance type Drac ou ILO pour les serveurs
- Présence d'une redondance matérielle au niveau du stockage de la donnée (raid)
- Présence à minima de 2 cartes réseaux pour la séparation des flux.

4.12.2 Exigences liés aux logiciels

Lors de l'acquisition de nouveaux logiciels ou lors de la modification de logiciels, il est important de tenir compte des exigences de sécurité en termes de Disponibilité, Intégrité, Confidentialité et Traçabilité.

Cette identification est faite lors de la phase projet, c'est à dire avant l'acquisition ou le changement.

Critères de disponibilité

Le système hébergeant l'application doit être suffisamment dimensionné pour que l'application puisse fonctionner normalement.

Dans le cas d'applications liées aux systèmes sensibles, celles-ci doivent permettre la mise en place d'une redondance.

Il est également important d'étudier la possibilité de souscrire à un support auprès de l'éditeur.

Critères d'Intégrité

Les solutions doivent pouvoir gérer plusieurs paramètres :

- Les communications doivent pouvoir être chiffrées par SSL (ldaps, https, etc).
- L'application doit pouvoir gérer une historisation des accès.
- Dans le cas d'une application publique, un WAF doit être mis en place.

Critères de confidentialité

Les solutions retenues doivent à minima permettre la mise en place des exigences suivantes :

- Gérer une authentification
- Permettre une authentification sur le système de gestion d'identité (si possible SSO)
- Pouvoir gérer des profils utilisateurs avec restrictions de droits (profils admin et profils lecteur).

Critères de Traçabilité

La preuve au sein de l'application doit permettre à minima de :

- Historiser les authentifications (Date/Heures IP sources, login, Succès/Echec)
- Historiser les accès (log web par exemple)
- Exporter les logs au format syslog (au travers du système si l'application ne le gère pas nativement)
- Non répudiation.

4.13 Norme de développement

4.13.1 Jeu d'essai

Sur la plateforme de test, aucune donnée de production n'est exploitée. Pour effectuer des développements ou faire des recettes d'applications, ITS crée un jeu d'essai avec des données anonymisées. Ainsi les environnements de production ne contiennent jamais d'information de production identifiables.

4.13.2 Mesures cryptographiques

ITS met en œuvre différentes mesures cryptographiques afin de protéger les données sensibles de l'entreprise.

Le besoin de chiffrement des documents est défini par les exigences du tableau de classification.

Les mesures cryptographiques sont également utilisées dans les cas suivants :

- Chiffrement des postes nomades
- Chiffrement des communications mails tant au niveau transport (SMTPS/IMAPS) que contenu (X509)
- Création de conteneurs sécurisés

Des moyens de recouvrement sont mis en œuvre avec le stockage des clefs au niveau du coffre-fort numérique.

4.13.3 Modification des logiciels

ITS ne modifie pas les logiciels propriétaires. Si par nécessité, ITS a besoin d'effectuer une modification, celle-ci est étudiée par le pôle développement et sécurité. Si elle est retenue, elle sera mise en œuvre en partenariat avec le fournisseur de façon à veiller au bon déroulement de cette modification sans altération du niveau des performances, de la sécurité et du contrat de service du fournisseur (notamment garanties).

Une phase de recette avec le fournisseur permettra la meilleure exécution.

4.14 Gestion des incidents de sécurité

4.14.1 Définition

Un incident SSI est un évènement, potentiel ou avéré, indésirable et/ou inattendu, impactant ou présentant une probabilité forte d'impacter la sécurité de l'information dans les critères de Disponibilité, de Confidentialité, d'Intégrité ou de Traçabilité.

Il correspond à une action malveillante délibérée ou d'une manière générale à toute atteinte aux informations, toute augmentation des menaces sur la sécurité des informations ou toute augmentation de la probabilité de compromission des opérations liées à l'activité.

4.14.2 Traitement et résolution

Tout incident de sécurité observé ou suspecté doit être signalé à l'équipe sécurité dans les plus brefs délais par les collaborateurs. Les prestataires sont également tenus à cette obligation. La suite à donner est définie à partir des critères d'évaluation d'impacts, qui permettent la détermination du niveau de l'incident : mineur, sévère, majeur, critique.

Suite à la qualification, des mesures d'urgence peuvent être prises pour limiter les impacts et préserver les traces, tels qu'un confinement, une isolation, une communication ciblée.

Une investigation est ensuite effectuée afin de préciser les caractéristiques de l'incident, et peut conduire au déclenchement d'une cellule de crise. L'incident est enfin résolu, soit par le biais d'une solution de contournement, soit par l'application d'un correctif.

Une revue mensuelle des incidents de sécurité est effectuée par l'équipe sécurité, afin de dégager et globaliser des plans d'action correctifs pérennes.

Temps moyen de résolution des incidents de sécurité
Quantité d'incidents SWAT

V. Garantir notre continuité de service

Conformément aux exigences ISO 27002 et aux besoins internes, ITS procède régulièrement à la revue et à l'audit technique de son infrastructure. Ces contrôles permettent de maîtriser au mieux la conformité avec ce qui a été défini et est connu de tous notamment dans le cadre du Plan de Continuité d'Activité (PCA).

Pour ce faire, ITS a défini une organisation et des modes opératoires associés ayant pour but de garantir la survie de l'entreprise lors un sinistre important. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

5.1 Périmètre

Lors de l'appréciation des risques réalisée dans le cadre de la norme ISO 27001, il a été identifié trois types de risques nécessitant la mise en place du plan de continuité.

- LA PERTE OU L'INDISPONIBILITE D'UN SITE PHYSIQUE.

Ce risque regroupe l'ensemble des problèmes liés aux bâtiments. Le risque peut être temporaire (perte de sources d'énergie) ou définitif dans le cas d'une destruction du bâtiment. On distingue également 2 types de bâtiments : les datacenters d'une part et les bureaux d'autre part.

- L'INDISPONIBILITE D'UN NOMBRE IMPORTANT DE SALARIES.

Il s'agit de l'indisponibilité d'un nombre important de salariés ou dans l'incapacité de se rendre au travail. Cette indisponibilité pourrait avoir des origines diverses comme des grèves massives, une pandémie virale…

- LA PERTE OU LA CORRUPTION D'UN SERVICE VITAL (CORE SERVICE)

Le bon fonctionnement des services de cœurs de réseaux étant vital, ils entrent dans le PCA afin que des mesures de redondance adéquates soient mises en place.

5.2 Indisponibilité d'un site physique

5.2.1 Indisponibilité temporaire

a) Sites de bureaux

L'indisponibilité temporaire indique que le site est toujours existant mais ne permet plus de travailler ou accueillir les collaborateurs. L'indisponibilité est relativement courte et ne dépasse généralement pas 24 heures. Ce cas peut se présenter lors de la perte des sources d'énergie, la perte des moyens de communications ou un besoin d'évacuation.

Cette indisponibilité déclenche le PRA utilisateur simple pour le site concerné dans un délai de 1 heure suivant le début de l'indisponibilité.

Dans le cas de la plateforme technique ITS Integra, les sites de Boulogne Billancourt et de Montpellier sont prévus pour se seconder l'un l'autre afin d'assurer une continuité de traitement.

b) Sites datacenter

Les sites de datacenters étant pleinement redondés ceux-ci ne subissent pas de coupures temporaires ou alors très courtes, la résolution est traitée comme un incident classique.

5.2.2 Indisponibilité permanente

a) Sites de bureaux

L'indisponibilité permanente d'un site hébergeant des bureaux est déclarée en cas de destruction du site. La destruction indique que le site sera indisponible pendant une longue durée.

Cette indisponibilité déclenche le PRA utilisateur complet pour le site concerné dans les plus brefs délais.

b) Sites de datacenter

L'indisponibilité permanente d'un datacenter est la situation la plus critique possible pour ITS. Ce cas peut se présenter en cas de catastrophe naturelle, d'attentats, incendie.

Cette indisponibilité déclenche immédiatement l'ensemble des PRA Clients ayant souscrits à cette offre ainsi que les PRA internes. L'ordre de déclenchement des PRA clients est défini en fonction de 2 critères :

- Le RTO (Recovery Time Objective) qui correspond au temps maximum de coupure admissible selon l'engagement de service convenu
- Le volume financier du client

Concernant les clients ne disposant pas d'offre de PRA, conformément aux contrats clients, une mise à disposition des données externalisées sera réalisée.

5.3 Indisponibilité humaine

L'indisponibilité massive d'employés lors d'épisodes viraux sévères (grippe saisonnière, grippe aviaire) représente un risque pour ITS. Il peut être nécessaire de mettre en place de mesures de sauvegarde du personnel. Selon le niveau d'alerte virale et en accord avec les autorités sanitaires, les mesures suivantes peuvent être prises :

- Actions de communication interne spécifiques
- Mise à disposition d'un gel désinfectant et/ou masque de protection
- Remplacement des essuies mains en tissu par du papier jetable
- Confinement en télétravail

En cas de dépassement d'un taux d'absentéisme de 30%, le confinement en télétravail est mis en place pour les utilisateurs vitaux.

5.4 Indisponibilité services vitaux

Les services vitaux présents sur les systèmes sensibles doivent subir un minimum de coupures. Ceux-ci sont donc systématiquement configurés en haute disponibilité sur plusieurs sites physiques. Ils doivent pouvoir fonctionner en mode dégradé sans intervention particulière.

La redondance des services vitaux est testée de façon périodique en accord avec le plan d'audit.

5.5 La cellule de crise PCA

Si un des incidents couverts par le périmètre du PCA se présente, une cellule de crise est immédiatement mise en place.

5.5.1 Composition

La cellule de crise PCA est composée de :

- La direction générale
- La direction financière
- Les directeurs de services opérationnels
- Le médecin hébergeur, dans le cadre de l'hébergement des données de santé.

5.5.2 Mission de la cellule de crise

La cellule de crise PCA est chargée des missions suivantes :

- Validation du déclenchement du PCA
- Prise de décision et ajustement sur l'orchestration des PRA liés au PCA
- Prise de décision sur les mesures et investissements immédiats.

5.5.3 Principe de réunion

La cellule de crise se concerte en réunion à toutes les étapes clés du PCA (déclenchement / PRA vitaux / fin) et à minima toutes les 3 heures.

Pour ce faire, la grande salle de réunion des locaux de Boulogne-Billancourt est réquisitionnée d'office.

5.5.4 Test de constitution de la cellule de crise

Des tests de constitution de la cellule de crise sont réalisés une fois par an. Il s'agit d'un exercice assurant que l'ensemble des acteurs peuvent être joint rapidement.

Taux de tests PRA effectués 

VI. Annexe 1 : Indicateurs SSI

Thème	Nom de l'indicateur	Référentiel	Formule de calcul	Fréquence	Objectif
Patch Management	Taux moyen de réussite des patchs	Outil de patch management windows et linux	$\left(\frac{\text{Nb patch ok}}{\text{Nb patch lancé}}\right) * 100$	Mensuelle	95%
	Quantité de patchs disponible	Outil de patch management windows et linux	N/A	Mensuelle	
	Taux d'équipements compatible avec la politique de MAJ	Outil de patch management windows et linux	$\left(\frac{\text{Nb poste config ok}}{\text{Nb poste total}}\right) * 100$	Mensuelle	100%
Code Malveillant	Taux d'agent antivirus à jour	Logiciel antivirus	$\left(\frac{\text{Nb agent à jour}}{\text{Nb agent}}\right) * 100$ Mise à jour inférieure à 3 jours entre la date de dernière connexion et la date de définition de virus	Mensuelle	95%
Sauvegardes	Taux de réussite des sauvegardes	Logiciel de sauvegarde	$\left(\frac{\text{Nb job réussi}}{\text{Nb job total}}\right) * 100$	Mensuelle	95%
	Taux de réussite des tests de restauration	Tableau de suivi des tests	$\left(\frac{\text{Nb test réussi}}{\text{Nb test total}}\right) * 100$	Mensuelle	95%
Gestion des traces	Taux de déploiement du Syslog	Serveurs syslogs	$\left(\frac{\text{Nb poste dans syslog}}{\text{Nb poste total}}\right) * 100$	Trimestrielle	95%
Durcissement	Taux de serveurs intégrés dans l'AD	Inventaire	$\left(\frac{\text{Nb poste dans AD}}{\text{Nb poste total}}\right) * 100$	Trimestrielle	100%
	Taux de services configurés en protection DDOS	Solution de protection anti DDOS	$\left(\frac{\text{Nb service configure}}{\text{Nb service publique}}\right) * 100$	Trimestrielle	100%
Comptes logiques	Taux de mots de passe avec expiration	Active Directory	$\left(\frac{\text{Nb compte avec expiration}}{\text{Nb compte}}\right) * 100$	Trimestrielle	100%
	Taux d'écarts lors de la revue des droits	Tableau de suivi des revus des droits	$\left(\frac{\text{Nb compte erreur}}{\text{Nb compte controlé}}\right) * 100$	Trimestrielle	<2%

Gestion des incidents	Temps moyen de résolution des incidents de sécurité	Outil de ticketing	$\frac{\sum \text{temps de résolution}}{\text{Nb incident fermé}}$	Mensuelle	
	Quantité d'incidents SWAT	Outil de ticketing	N/A	Mensuelle	
PRA	Taux de tests PRA effectués	Tableau de suivi des PRA	$\left(\frac{\text{Nb PRA testé}}{\text{Nb PRA existant}}\right) * 100$ PRA testé = PRA testé au cours des 365 jours précédents	Trimestrielle	