TAGG informatique

Politique de Sécurité des Systèmes Informatiques de TAGG INFORMATIQUE (PSSI)

Chapitre I

Généralités sur la Sécurité

Version 1.2.1

MAJ le 30/01/2022

TABLE DES MATIERES

1 SECURITE PHYSIQUE

1.1 LOCAUX TECHNIQUES ET ESPACE BUREAU

1.1.1 DISPOSITIF D'ENREGISTREMENT ET DE CONTROLE DES VISITEURS

- Un protocole d'enregistrement des visiteurs permet le contrôle des personnes accédant aux locaux techniques, aux espaces de bureaux et aux zones de livraison/chargement : Enregistrement dans le logiciel de gestion des visiteurs « Kelio », signature de la clause de confidentialité, numéro de la CNA et mise à disposition d'un badge magnétique numéroté et enregistré au nom de la personne.

1.1.2 MECANISMES DE DETECTION AVEC JOURNALISATION DES INTRUSIONS PHYSIQUES

- Nos locaux sont équipés d'un système de caméras de surveillance, de radars volumétriques et de contrôles d'accès par biométrie. Les vidéos enregistrées sont sauvegardées et stockées 3 semaines sur une baie de stockage. Les journaux d'intrusions et d'accès sont consultables via un logiciel agréé.

1.1.3 ACCES AU BATIMENT

- Un dispositif d'authentification (par biométrie et badges) permet le contrôle des personnes accédant aux locaux techniques, aux espaces de bureaux et aux zones de livraison/chargement :
  - Mise à disposition de badges magnétique numérotés pour les prestataires, les intérimaires, les livreurs, ...
  - Enregistrement par biométrie du personnel de ménage et des collaborateurs.

1.2 LOCAUX TECHNIQUES INFORMATIQUES

1.2.1 HERBERGEMENT DES MOYENS TELECOMS ET INFORMATIQUES

- Les équipements informatiques et de télécommunication sont hébergés dans un local technique blindé. Il existe un deuxième local blindé pour le stockage des supports magnétiques et des documents sensibles. Les deux locaux sont protégés du feu par un système d'extinction automatique (gaz FE13).

1.2.2 ACCES AUX LOCAUX TECHNIQUES HEBERGEANT LES MOYENS TELECOMS ET INFORMATIQUES

- L'accès aux locaux techniques hébergeant les moyens télécoms et informatiques (éléments actifs de réseaux, commutateurs, routeurs, firewalls, serveurs, PABX...) est contrôlé par un dispositif biométrique d'authentification, d'habilitation et de journalisation des accès. Une porte blindée et une porte coupe-feu pouvant résister une heure à l'incendie (avec système de sas) protègent l'accès à ces locaux.

1.2.3 MAINTENANCE DES SYSTEMES DE CONTROLES D'ACCES, D'ALARME ET D'INCENDIE

- Tous les dispositifs de contrôle d'accès, d'alarme et d'incendie font l'objet d'une maintenance périodique (contrat d'entretien).
- Les alertes des systèmes d'alarmes et d'incendie sont reportées à une société de gardiennage.

1.2.4 MECANISME D'ALERTE

- La température et l'humidité des locaux techniques sont régulées et surveillées par un mécanisme d'alerte testé périodiquement. Ces locaux d'une importance majeure pour la continuité de services de l'entreprise sont équipés de climatisations redondantes pour une sécurité maximale.
- Un système de détection de fumée, de température, d'hydrométrie, d'inondation et de coupure électrique permet l'envoi de sms d'alerte sur les téléphones mobiles de plusieurs responsables techniques.

1.2.5 INFRASTRUCTURE ELECTRIQUE

- Deux onduleurs redondants et un groupe électrogène de 700KVA sont capables d'assurer une alimentation 24h/24 et 7j/7 des moyens informatiques et d'assurer le secours des sources d'énergie principales en cas d'interruption de ces dernières.

1.3 INSTALLATION DU SITE

1.3.1 CONTROLES DES INSTALLATIONS

- Les locaux sont régulièrement contrôlés et audités de manière à vérifier le respect des normes et standards d'installation (électricité, climatisation, détection incendie, ...)

1.4 PRATIQUES GENERALES

1.4.1 ACCES PHYSIQUE AUX POSTES DE TRAVAIL

- L'accès physique aux postes de travail utilisés pour l'administration et l'exploitation est protégé.

1.4.2 CONTROLE DES MOYENS DE PROTECTION PHYSIQUES : GESTION DES ALARMES, GESTION DES ACCES PHYSIQUES POUR ACCEDER AUX LOCAUX TECHNIQUES ET AUX ESPACES BUREAU

- Le directeur général adjoint a en charge la gestion des infrastructures, des systèmes de sécurité et de sauvegardes et du Système d'Information (télécom, réseaux, informatiques, accès, habilitations, ...)

2 SECURITE RESEAU

2.1 RESEAU INTERNE

2.1.1 REGLES D'ARCHITECTURE RESEAU

2.1.1.1 MAITRISE DE L'ARCHITECTURE RESEAU.

- Les points d'accès Internet mettent en œuvre une architecture à deux niveaux de technologies différentes : Firewalls redondants et DMZ
- Tous les flux avec l'extérieur passent systématiquement par des relais applicatifs du style proxy en DMZ.

2.1.1.2 CLOISONNEMENT DU RESEAU INTERNE

- Des zones de sensibilité différentes sont définies au sein du périmètre réseau en fonction des ressources hébergées.
- Les terminaux inconnus sont détectés et bloqués à l'aide d'une solution de contrôle d'accès au réseau, au niveau de notre firewall.

2.1.1.3 RESEAU D'ADMINISTRATION

- Un plan d'adressage IP dédié permet l'administration des équipements réseaux et systèmes.

2.1.1.4 INTERCONNEXIONS AVEC L'EXTERIEUR

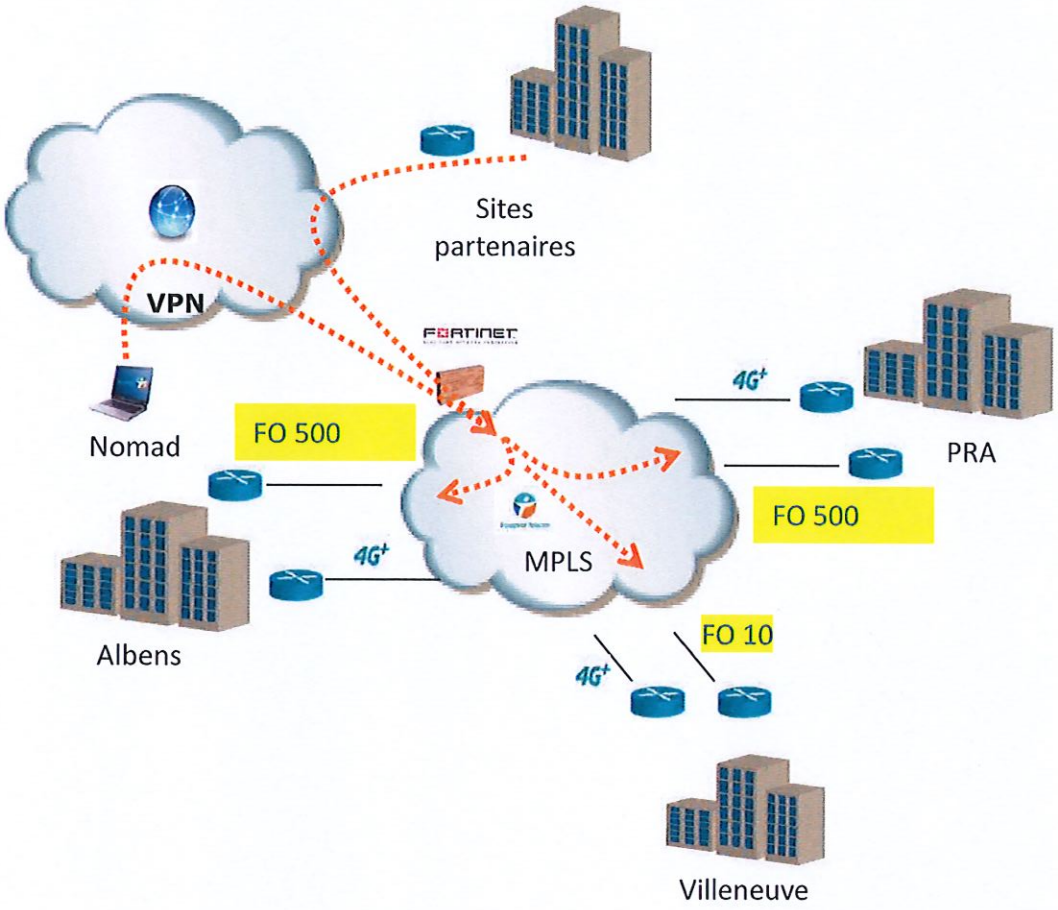
- Les bornes WIFI sont connectées au réseau via les firewalls. Des campagnes périodiques de détection de réseau WIFI sont menées dans les bâtiments.

2.1.1.5 GESTION DES COMPTES ET DES DROITS

- Chaque compte d'accès peut être révoqué en cas de perte d'authentifiant.

2.2 INTERCONNEXIONS AUTRES RESEAUX

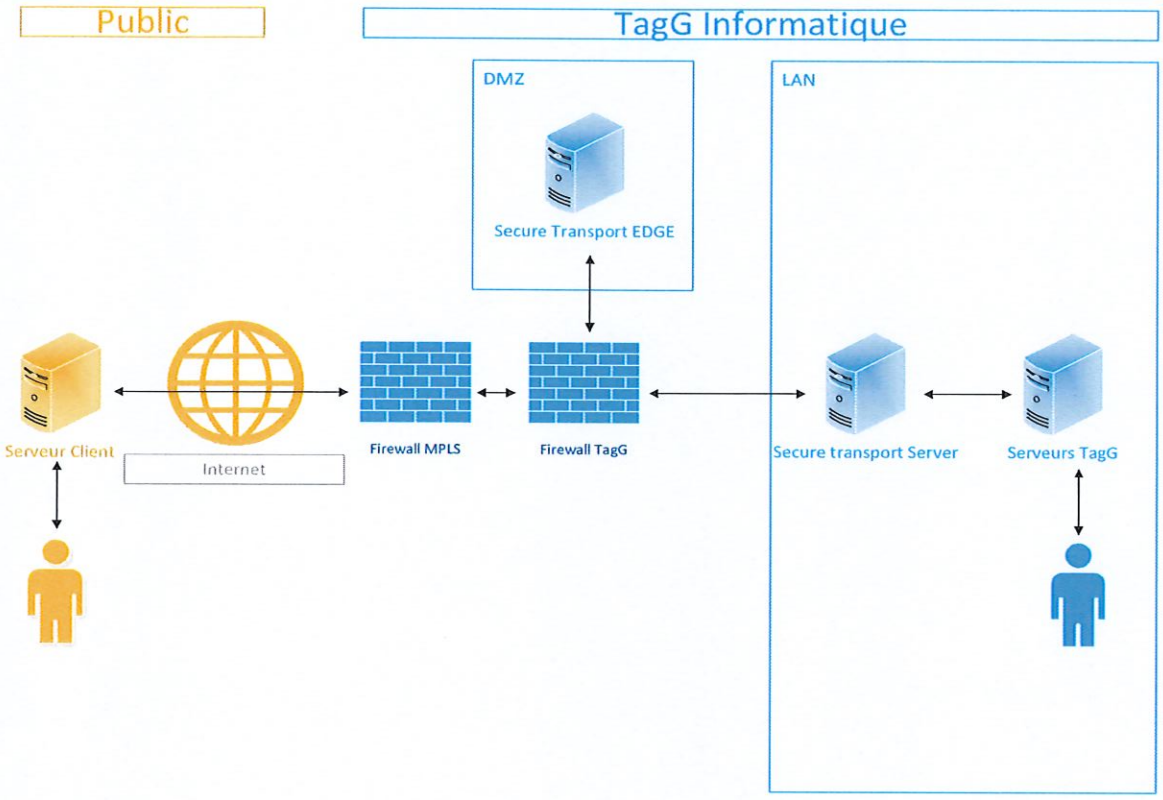
2.2.1 SCHEMA DES POINTS D'INTERCONNEXION AVEC LES RESEAUX EXTERNES



2.2.1.1 INTERCONNEXION AVEC L'EXTERIEUR

- Les données transitant sur les liaisons réseaux sont chiffrées (VPN).
- Les flux d'échange avec les partenaires sont protégés par une solution de détection d'intrusion au niveau du firewall.
- Les points d'interconnexion avec les tiers a lieu 24h/24 grâce aux outils du firewall.

2.2.1.2 TRANSFERT DE DONNEES SECURISE ENTRE LES CLIENTS ET TAGG



2.2.1.3 CONTROLES

- Une revue systématique de la cohérence des droits d'accès donnés aux tiers est appliquée au niveau du système grâce à nos applications métiers (base de données).

2.3 ACCES NOMADES

2.3.1.1 INTERCONNEXION AVEC L'EXTERIEUR

Les points d'accès nomade mettent en œuvre une architecture qui protège le réseau interne et les équipements du point d'accès vis à vis des réseaux externes (par VPN sécurisé, voir le schéma d'interconnexions réseau)

2.3.1.2 CONFIGURATION DES EQUIPEMENTS

- Tout accès nomade externe au réseau interne met en œuvre une authentification par double authentification (mot de passe + token) ainsi qu'une demande de réauthentification au-delà d'une période.
- Tous nos postes nomades sont administrés et ont des droits limités.

2.3.1.3 JOURNALISATION

- Les accès nomades sont journalisés (identifiant de connexion, date et heure de connexion)

3 SECURITE SYSTEME

3.1 POSTES DE TRAVAIL

3.1.1 CONFIGURATION DES EQUIPEMENTS

- Chaque poste est configuré pour demander une authentification lors de l'ouverture de session.
- Tous les postes sont installés dans des locaux sécurisés.
- Chaque poste de travail est configuré pour ne pas démarrer sur un support amovible (CD-ROM, clé USB, disquette)
- L'ensemble des interfaces de communication IP des PC portables sont protégées par un firewall local.
- La configuration sécurité du poste de travail est protégée vis à vis de l'utilisateur par une stratégie de groupe
- Un mot de passe est demandé pour accéder au BIOS du poste.
- Chaque poste est configuré pour empêcher la désactivation de l'antivirus.

3.1.2 GESTION DES COMPTES ET DES DROITS

- Tout utilisateur ayant accès à un poste de travail est pourvu d'un identifiant personnel et unique pour accéder à ce poste (sauf production).
- Tout poste de travail connecté au réseau de production est identifié et administré.

3.1.3 GESTION DES EVOLUTIONS ET VEILLE

- Chaque poste de travail connecté au réseau interne dispose d'un antivirus actif et à jour.
- Les logiciels installés sur le poste de travail (y compris l'OS) ont tous une version à jour supportée par l'éditeur.
- Les correctifs de sécurité sont appliqués en moins d'une semaine sur les postes de travail (serveurs = une fois par mois).

3.1.4 PROTECTION DES BIENS

- Des outils de chiffrement orientés fichiers sont mis à disposition sur le poste de travail pour protéger les éventuelles informations confidentielles.

3.1.5 CONTROLE

- Le contenu logiciel du poste de travail virtualisé est régulièrement contrôlé.

3.1.6 JOURNALISATION

- Majeure partie des interventions d'administration sont tracées par le système d'exploitation.

3.2 UTILISATION DES RESSOURCES INFORMATIQUES

3.2.1 PROTECTION DES BIENS

- Les données des équipements réseau, des serveurs et des postes de travail (fichiers, comptes, URLs, etc.) sont supprimées à la suite du départ de collaborateurs.
- Le protocole TLS est implémenté sur les serveurs Web.

3.2.2 ACCES AUX EQUIPEMENTS

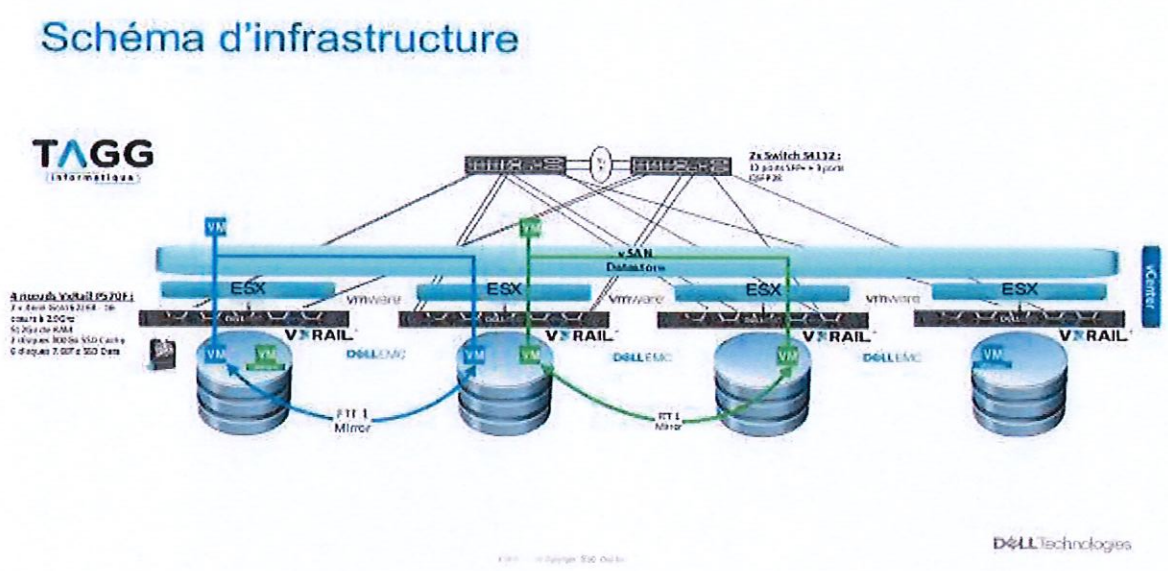
- Le poste de travail dispose d'une mise en veille protégée par mot de passe en cas d'inactivité prolongée.
- Aucunes données sensibles (ex : données clients, données bancaires, etc.) ne sont stockées sur les postes de travail.

3.2.3 CONFIGURATION DES EQUIPEMENTS

- Les outils de protection contre des logiciels malveillants (virus, chevaux de Troie ···) sont activés et maintenus à jour sur les moyens informatiques (serveur dédié).

3.3 SERVEURS INTERNES

3.3.1 SCHEMA DE L'INFRASTRUCTURE SERVEURS



3.3.2 GESTION DU MATERIEL

- Il existe un inventaire à jour des serveurs (automatiquement géré par l'outil de virtualisation).

3.3.3 PROTECTION DES BIENS

- Les serveurs applicatifs et les serveurs de partage de ressources mettent en œuvre une protection antivirale.

3.3.4 MISE A JOUR DU PARC

- Les mises à jour des serveurs et postes de travail sont effectuées et gérées par un serveur dédié.
- Les patchs de sécurité sont appliqués automatiquement à l'ensemble du parc informatique pour les systèmes d'exploitation.
- Des périodes de maintenance sont planifiées mensuellement pour finaliser au besoin l'application de ces patchs.
- Les failles critiques sont traitées dès leur apparition et l'application du correctif se fait en dehors des maintenances planifiées afin de corriger le risque au plus tôt.
- Les mises à jour de qualité sont soumises à une validation manuelle après avoir été testées sur des serveurs pilotes.
- Les applications tierces sont gérées de manière biannuelle sauf pour les patchs critiques qui sont appliqués immédiatement.

3.3.5 GESTION DES EVOLUTIONS ET VEILLE

- Les logiciels installés sur les serveurs internes (y compris l'OS) ont tous une version à jour supportée par l'éditeur.

- La procédure d'installation des serveurs (logiciels, configuration sécurité, OS) est facilitée grâce aux outils de virtualisation.

3.3.6 CONTROLES

- Des tests de vulnérabilités et un audit de configuration a été réalisé sur un échantillon de serveurs (serveurs Web) en 2015.
- Depuis mars 2018, des tests de vulnérabilités potentielles sont fait chaque mois par notre opérateur sur notre pare-feu en fonction des règles que nous avons créées sur ce dernier. Ces tests mettent en avant les points critiques à corriger ou des avertissements suivant le niveau de risque encouru.

3.3.7 ACCES AUX EQUIPEMENTS

- Les flux d'administration distante des ressources réseaux et systèmes sont chiffrés.
- L'administration des ressources réseaux et systèmes passe par un serveur de rebond centralisé au niveau du firewall.
- Les administrateurs utilisent des comptes d'administration nominatifs différents de leur compte utilisateur.

3.4 ACCES LOGIQUES

3.4.1 GESTION DES COMPTES ET DES DROITS

- Le compte administrateur possédant le privilège le plus élevé du système est déposé dans une enveloppe scellée dans un coffre de banque.
- Les mesures de sécurité suivantes sont imposées techniquement pour protéger les mots de passe : longueur de 20 caractères minimum ; combinaison d'au moins trois des critères suivants : majuscules, minuscules, chiffres et caractères spéciaux ;
- Blocage systématique du compte et temporisation de 30 min avant toute nouvelle tentative au bout de 3 saisies erronées.
- Renouvellement tous les six mois et non réutilisation des 3 derniers mots de passe (sauf compte de service)
- Les comptes inutilisés pendant une période de plus de 60 jours sont systématiquement désactivés.
- Les accès aux BIOS sont verrouillés par mot de passe

3.4.2 CONFIGURATION DES EQUIPEMENTS

- Aucun mot de passe n'est stocké en clair sur les serveurs

3.4.3 JOURNALISATION

- Les actions d'administration sont enregistrées dans les journaux du système.
- Les journaux d'évènements des équipements réseaux et systèmes sont analysés fréquemment.

3.4.4 CONTROLES

- Une liste centralisée des droits attribués aux utilisateurs sur les données métier est tenue à jour dans un classeur (Fiches personnelles « Sécurité de l'accès au bâtiment et à l'informatique »).

3.5 VIRTUALISATION

- La virtualisation des environnements systèmes respecte les préconisations des éditeurs logiciels en termes de performance (suite à audit société spécialisée).

3.6 MESSAGERIE

- Le relais SMTP dispose d'une protection antivirale à jour, pour l'analyse des messages, avec mise à jour automatique du fichier des signatures.
- Dispositif de défense contre les spams.
- La boîte aux lettres d'un utilisateur qui a quitté l'entreprise est systématiquement supprimée puis relayée à un collaborateur.
- Les utilisateurs ont la possibilité de chiffrer les courriels confidentiels. Ils ont la connaissance de l'obligation d'utiliser, pour l'envoi de leurs messages confidentiels, cette fonction de chiffrement.
- Les collaborateurs disposent de la solution NetExplorer pour le partage des documents et l'envoi des pièces jointes.

4 SECURITE APPLICATIVE

4.1 ACCES INTERNET

- Un contrôle antivirus des flux HTTP est réalisé au niveau des points d'interconnexion.
- Les accès web sortants sont limités par un dispositif de contrôle visant à interdire l'accès à des sites réputés illégaux ou dangereux (filtrage de contenus).
- Les journaux de connexion Internet sont conservés à titre de preuve sur les durées minimales et maximales conformes à la législation (URL visitées, date et heure, identifiant de l'utilisateur).
- Les enregistrements stockés dans les journaux sont protégés contre une suppression et/ou une altération non-autorisée.

4.2 APPLICATION WEB

- Le site Internet hébergé a fait l'objet d'un scan de vulnérabilités en 2015 (scan interne depuis le réseau interne, scan externe depuis Internet)
- Le site Internet a fait l'objet de tests d'intrusion (applicatif) en 2015 suite à un audit client.
- Des tests sur notre pare-feu sont réalisés par notre FAI tous les mois
- La disponibilité du service et de la bande passante font l'objet d'un engagement contractuel : 20 Mb/s garanti (réseau MPLS)
- Deux serveurs redondants (actif/passif) hébergent les sites WEB
- L'accès à l'application Web nécessite une authentification préalable de l'utilisateur (authentification forte)
- Les données saisies par l'utilisateur de l'application sont contrôlées.
- L'application enregistre les traces de l'activité des utilisateurs (action, responsable et date)

4.3 PRATIQUES GENERALES

- Des mesures rigoureuses sont mises en œuvre, pour s'assurer de l'intégrité des logiciels en production (impression et mise sous plis)
- Les données confidentielles en production sont protégées : chiffrement, droits d'accès, ...
- Les données de production sont protégées et séparées de celles des autres environnements : pré-production, tests, ... (outils ProdInformation)

4.4 SECURITE DANS LES PROJETS

4.4.1 REGLES DE SECURITE DANS LES PROJETS SI

- Des mesures de sécurité sont prises pour ne pas réutiliser les fichiers de production à des fins de tests
- Nous disposons de normes de développement et de règles de codage pour assurer la sécurité des produits développés (validation des données en entrée et en sortie, validation du traitement, contrôle des modifications)
- Les développements font l'objet d'une documentation de conception et d'une documentation d'exploitation.

- Dans les cas d'externalisation de développements, des mesures de sécurité spécifiques sont mises en œuvre en fonction de la sensibilité des applications (engagement de confidentialité)
- Les équipements et environnements de développement, de tests et d'exploitation sont séparés.

4.4.2 RECETTE DES LOGICIELS

- Les recettes et tests de bon fonctionnement des logiciels sont effectués sur des plateformes dédiées avant installation en production.

5 MANAGEMENT SECURITE

5.1 ORGANISATION

- Les rôles et responsabilités en matière de sécurité sont définis dans une Fiche Individuelle de Sécurité
- En cas d'incident de sécurité ayant un impact sur la prestation, un processus général (fiches d'incidents) permet de traiter la non-conformité.
- Des fiches d'incidents permettent de mesurer la bonne application des mesures correctives.
- Le Directeur QSE est le correspondant avec les autorités légales et les organismes de réglementation (Ex : CNIL)

5.2 ACCES LOGIQUES

- Des procédures « Fiches individuelles de Sécurité » sont appliquées pour l'attribution de compte, à l'arrivée d'un utilisateur, lors d'un mouvement ou d'un changement de fonction d'un utilisateur et lors de départ d'un utilisateur.

5.3 PRATIQUES GENERALES

5.3.1 GESTION DU MATERIEL

- Une procédure de destruction ou d'effacement définitif des données sur les supports de stockage (disque dur, cartouche de sauvegarde ···) est systématiquement réalisée avant mise au rebut, réaffectation ou cession des supports contenant des informations sensibles.

5.3.2 MISE EN PRODUCTION

- Des mesures sont mises en œuvre, pour s'assurer que les versions mises en exploitation sont les versions recettées.

5.3.3 GESTION DES EVOLUTIONS ET VEILLE

- Une qualification est réalisée avant mise en production d'un système, d'un service, d'une application ou d'un correctif.
- Tous les logiciels système et matériels utilisés en production font l'objet d'un suivi d'obsolescence de versions.

5.3.4 TELEMAINTENANCE

- Les mesures de sécurité sont formalisées dans un contrat entre l'entité et le fournisseur du service de télémaintenance.
- Lors des périodes de non-utilisation de la télémaintenance, la liaison vers l'extérieur est désactivée.
- Pour tout accès de télémaintenance, le paramétrage de nos firewalls garantit que le télémainteneur n'a accès qu'à la ressource télémaintenue.

- Les personnes chargées de la télémaintenance sont nommément désignées.

5.3.5 GESTION DES INCIDENTS

- Nous utilisons une procédure formalisée de remontée d'incident (fiches d'incidents).
- Les horloges serveurs sont synchronisées afin de pouvoir corréler les informations provenant de différentes sources.
- Nous disposons d'une procédure de collecte des preuves utilisables devant les tribunaux en cas d'incident grave.
- Grace aux fiches d'incidents, les décisions prises par une cellule de crise sont conservées, exploitées et gérées comme les autres traces de sécurité du système d'information.

5.4 DOCUMENTATION

- Une stratégie de groupe sur un serveur sécurisé permet le partage et la protection des documents techniques (informatique, réseau, télécom ...).
- Avant d'être mis au rebut, tous les documents utilisés sont détruits de façon irréversible et définitive (broyeur de papiers dans chaque bureau, broyeurs de documents industriels dans l'atelier, protection des déchets avant leur enlèvement).
- Les déchets papiers des documents personnalisés ou non personnalisés sont rendus inutilisables grâce à un destructeur papier situé à l'intérieur du bâtiment et sont ensuite stockés dans une benne fermée. Cette benne est régulièrement récupérée par une entreprise agrée pour la certification de la bonne destruction des documents enlevés.

5.5 GESTION DES CHANGEMENTS

- Les changements de configuration sur les infrastructures informatiques font l'objet d'une procédure de qualification et de validation avant mise en œuvre.

5.6 SECURITE DU MATERIEL

- Il existe un stock de matériels de secours, en cas de panne, pour de nombreux équipements.

5.7 R.H.

- Le personnel est sensibilisé à la sécurité informatique (y compris les mesures disciplinaires en cas de non-respect, le respect de la confidentialité étant inscrit dans les contrats de travail)
- A la demande des clients, les membres de l'équipe d'exploitation peuvent signer un engagement individuel et contractuel de sécurité.
- A la demande des clients, les membres de l'équipe d'exploitation peuvent fournir une copie du bulletin N°3 du casier judiciaire.

5.8 POSTES DE TRAVAIL

- Par l'intermédiaire de la fiche individuelle, les utilisateurs sont sensibilisés sur les règles d'usage du poste de travail (respect de la configuration du poste, arrêt du poste de travail le soir, mesures de protection du poste, non-divulgation du mot de passe, verrouillage des sessions utilisateurs, ...).

5.9 UTILISATION DES RESSOURCES INFORMATIQUES

5.9.1 OBLIGATIONS LEGALES ET REGLEMENTAIRES

- Les utilisateurs ont-ils pris connaissance, grâce au contrat de travail qui y fait référence, de l'existence de documents spécifiant les conditions d'utilisation des équipements informatiques (charte d'utilisation, règlement intérieur).

5.9.2 PROTECTION DES BIENS

- Les utilisateurs sont sensibilisés aux risques liés à l'utilisation d'Internet ou de la messagerie (virus ou chevaux de Troie dans des fichiers téléchargés ou reçus par messagerie, niveau de confiance à accorder aux messages reçus par Internet, ...)
- Les utilisateurs sont informés de leur responsabilité en matière de protection et de sauvegarde des données stockées sur leur poste de travail en l'absence de sauvegarde automatique.
- Les utilisateurs ont l'obligation de conserver leurs données sur les disques serveurs ou à l'aide des moyens mis à disposition sur les portables, plutôt que sur leur poste en local.

5.9.3 USAGE DES RESSOURCES DU SI

- Les utilisateurs sont informés que l'utilisation des ressources doit être réservé à un seul usage professionnel et que les connexions au réseau et à l'internet sont tracées (clause du contrat de travail et disposition du RI)

5.9.4 REGLES D'ADMINISTRATION

- Les utilisateurs valident toujours la prise de main à distance de leur poste par l'administrateur en cas de demande de dépannage.

5.9.5 POLITIQUE DE SECURITE

- Le processus de diffusion, de réévaluation et d'amélioration de la politique de sécurité est réévalué aux cours des comités de CIP.

6 SAUVEGARDE

6.1 SAUVEGARDE ET ARCHIVAGE

6.1.1 REGLES D'EXPLOITATION

6.1.1.1 MISE EN PRODUCTION

- Nos serveurs sont sauvegardés automatiquement tous les jours par sauvegarde incrémentale cryptée, une fois par semaine en sauvegarde cryptée totale et une fois par mois en sauvegarde cryptée totale.
- Les cartouches du mois précèdent sont stockées dans un coffre-fort loué à l'une de nos banques. Nous conservons un archivage des données sur un an.
- Les sauvegardes restant sur le site de production sont entreposées dans des locaux d'accès protégé et éloignés des salles machines (local ignifuge blindé).
- Les sauvegardes sont protégées des risques physiques courants (incendie, inondation, intrusion).

6.1.1.2 CONTROLES

- Procédure de tests périodiques de validité des sauvegardes : Réalisation d'une restauration réelle au moins une fois par mois.
- Le journal des incidents de sauvegarde est quotidiennement analysé.

6.1.2 PLAN DE SECOURS INFORMATIQUE

- Il est prévu que les postes de travail sensibles soient en pris en charge par le Plan de Secours Informatique.

6.2 ACCES LOGIQUES

- Les journaux d'évènements et d'évènements sécurité de tous les équipements réseau, système et applicatif sont sauvegardés et archivés.

6.3 POSTES DE TRAVAIL

- En cas de réaffectation ou de mise au rebut des équipements (postes de travail, des serveurs, des systèmes de stockage, disque dur, supports amovibles, ...), le matériel fait l'objet d'un effacement préalable définitif des données.

6.4 ORGANISATION

- Les données archivées sont supprimées au bout du délai légal de conservation ou selon les termes contractuels.

7 BACK-UP PRODUCTION/PRA/PCA

7.1 LEXIQUE

- BACK-UP production : Système de redondance des équipements métiers liés à la production : machines de mises sous plis, imprimantes, matériel de façonnage, ...
- PCA : Plan de continuité d'activité, plan qui doit permettre de fonctionner même en cas de panne majeure quitte à ce que ce soit en mode dégradé.
- PRA : Plan de reprise d'activité, plan qui permet d'assurer, en cas de crise majeure la reconstruction de l'infrastructure et la remise en route des applications.

7.2 REPLICATION ET BACK-UP PRODUCTION SUR LE SITE PRINCIPAL

7.2.1 TRAITEMENT INFORMATIQUE

- Les applications clientes sont traitées dans un environnement de serveurs VMWARE, la redondance des traitements étant assurée par la virtualisation.
- Un Datacenter abrite l'ensemble de l'infrastructure informatique. C'est un local très sécurisé (porte d'entrée et murs blindés, porte sas coupe-feu, détection vol, contrôle biométrique, détection et extinction automatique, ...)
- Tous les serveurs sont répliqués, de manière synchrone, dans une armoire informatique séparée. Au total ce sont 55 serveurs, 36 postes de travail et toute l'infrastructure réseau qui sont dupliqués et immédiatement opérationnels en cas de panne d'un des éléments de l'armoire informatique principale.
- La réplication temps réel est assurée par des serveurs redondants.
- L'outil de backup, VEEAM référence sur le marché, permet de sauvegarder la totalité de l'infrastructure. Les cartouches de sauvegardes sont stockées dans un coffre ignifugé (sauvegarde journalière) et dans le coffre d'une banque (sauvegarde mensuelle).

7.2.2 EDITION

- La redondance de l'édition est assurée par plusieurs équipements d'impression en back-up dans l'atelier d'impression.

7.2.3 MISE SOUS PLIS

- La redondance de la mise sous pli est assurée par plusieurs équipements de mise sous plis automatiques en back-up dans l'atelier de routage.

7.3 BACK-UP PRODUCTION CHEZ NOTRE PARTENAIRE ET ASSOCIE DATAONE (SITE DE GAILLON-EURE)

7.3.1 QUI EST DATAONE ?

- DATAONE est une société coactionnaire du groupe mais indépendante de TAGG INFORMATIQUE. Les deux entreprises, néanmoins concurrentes, se connaissent bien et travaillent sur de nombreux dossiers communs depuis de plusieurs années. Cette union forte est liée à la bonne entente entre ses différents coactionnaires depuis les années 1990.

7.3.2 BACK-UP PRODUCTION CHEZ DATAONE

- Bien que cette solution ayant vocation à servir, nous n'avons pas eu à y recourir dans le cadre d'une situation réelle. Elle n'a fonctionné que sur demande de certains clients afin de vérifier le bon fonctionnement de leur back-up.

7.3.3 LES DIFFERENTS CAS DE DECLENCHEMENTS DU BACK-UP « DATAONE »

7.3.3.1 BACK-UP EN CAS DE SINISTRE MAJEUR SUR NOTRE SITE PRINCIPAL (HORS DATACENTER)

- La distance entre les deux sites permet de s'affranchir d'un risque dont l'étendue est supérieure à une région entière comme dans le cas d'un incident climatique.

7.3.3.2 BACK-UP EN CAS DE SURCHARGE PONCTUELLE NE POUVANT ETRE ABSORBEE PAR LE SITE SECONDAIRE.

- Cette option permet limiter les risques de décalage de planning trop important dont les raisons sont aussi bien du côté Prestataire que du côté Client. Cette option est plutôt réservée pour des dossiers dont le volume dépasse 500.000 plis avec un délai restreint.

7.3.3.3 BACK-UP EN CAS DE GREVE GENERALISEE DANS LE GROUPE

- Bien que ce cas ne se soit jamais présenté chez TAGG INFORMATIQUE, le risque existe. Les deux entreprises, TAGG et DATAONE sont indépendantes du point de vue social.

7.3.3.4 BACK-UP EN CAS DE DEFAILLANCE FINANCIERE

- Ce cas ne s'est jamais présenté dans notre Groupe, mais compte tenu de la situation financière mondiale, personne ne plus prétendre que ce risque n'existe pas. Les deux entreprises étant indépendantes financièrement, le back-up reste viable même en cas de défaillance financière de TAGG INFORMATIQUE.

7.3.3.5 BACK-UP EN CAS DE PROBLEMES TECHNOLOGIQUES

- Les solutions de gestion des flux de données mise en place par nos deux structures sont différentes et s'appuient sur des solutions softwares réalisées par des éditeurs de logiciels différents. Bien que le cas soit peu courant, nul ne peut être à l'abri d'un problème logiciel, dont le délai de débogage mettrait en péril le planning prévu pour l'application.

7.4 PRA ET PCA DANS NOTRE DATACENTER

- Une infrastructure informatique simplifiée mais dont les fonctionnalités sont identiques à celles de notre site de Savoie est installée dans le Datacenter de BOUYGUES - 78180 Montigny le Bretonneux. Elle permet une réplication totale de l'informatique du site d'Albens, utilisable dans le cadre d'un PCA ou d'un PRA.

7.4.1.1 PCA (PLAN DE CONTINUITE D'ACTIVITE) DANS LE DATACENTER

- Les serveurs principaux de production (fichiers clients, base de données, sites extranet, télétransmission, ...) sont répliqués en temps réel, dans une armoire informatique dédiée au PCA, afin de répondre à une panne de courte ou de longue durée de l'informatique du site principal. Dans ce cas, la réception (plateforme SECURE TRANSPORT) et le traitement des fichiers clients se fait via le Datacenter jusqu'au retour à la normale du site principal.

7.4.1.2 PRA (PLAN DE REPRISE D'ACTIVITE) DANS LE DATACENTER DATAONE

- Dans le cadre d'un PRA, l'ensemble de l'informatique du site principal peut redémarrer dans un délai de 1 heures, dans une infrastructure virtualisée, sur le site de secours. Une armoire informatique spécifique est dédiée à la gestion du PRA (4 ESX DELL) dans le Datacenter.
- Le PRA peut être déclenché dans l'hypothèse d'une indisponibilité totale de notre site de Savoie. Le back-up métier (paragraphe 2) est bien évidemment valable dans le contexte du PRA.

TAGG informatique

Politique de Sécurité des Systèmes Informatiques de TAGG INFORMATIQUE (PSSI)

Chapitre II

Règles de sécurité générales et spécifiques

Rôles et responsabilités de chacun à appliquer par les salariés

Version 2.0.4

MAJ le 2/03/2021

TABLE DES MATIERES

1 SECURITE PHYSIQUE

1.1 LOCAUX TECHNIQUES ET ESPACE BUREAU

- Service accueil
  - Les visiteurs (prestataires, clients, ...) souhaitant accéder aux locaux techniques, aux espaces de bureaux et aux zones de livraison/chargement doivent être enregistrés dans le logiciel « Kélio » : Signature de la clause de confidentialité, digitalisation de la CNA et mise à disposition d'un badge magnétique numéroté.
- Service administration des Systèmes & Réseaux
  - Les enregistrements vidéo, les journaux d'intrusions et d'accès doivent être contrôlés régulièrement (vérification du bon fonctionnement).
  - Les collaborateurs ainsi que les intervenants extérieurs doivent obligatoirement être enregistrés par biométrie.
  - Les données biométriques (droits d'accès) doivent être supprimées suite au départ de collaborateurs.
- Service atelier de production
  - Les intérimaires doivent obligatoirement être munis d'un badge magnétique.
- Tous les services
  - Interdiction de laisser entrer toute personne sans autorisation sur le site (notamment au niveau du tambour de l'entrée personnelle ou du magasin).

1.2 LOCAUX TECHNIQUES INFORMATIQUES

- Service administration des Systèmes & Réseaux
  - Parmi les collaborateurs, seuls les administrateurs, le responsable d'atelier et la direction ont le droit d'accès à ce local.
  - Les intervenants extérieurs doivent être enregistrés par biométrie.
  - Les systèmes de détection de température, d'humidité, d'inondation, de courant secteur et de fumée des locaux techniques doivent être testés périodiquement (tous les 6 mois).
  - La climatisation de secours doit être testée périodiquement (tous les mois).
- Service technique
  - Le groupe électrogène doit être testé périodiquement à vide et en charge (essai réel) :
    En charge : tous les 6 mois
    A vide : tous les mois

2 SECURITE RESEAU

2.1 RESEAU INTERNE

- Service administration des Systèmes & Réseaux
  - Des campagnes périodiques de détection de réseau WIFI doivent être menées dans les bâtiments (tous les 6 mois).

2.2 INTERCONNEXIONS AUTRES RESEAUX

- Service administration des Systèmes & Réseaux
  - Une revue systématique de la cohérence des droits d'accès donnés aux tiers doit être effectuée de manière périodique (tous les 6 mois).

2.3 ACCES NOMADES

- Aux administrateurs des Systèmes & Réseaux :
  - Tous les accès nomades externes au réseau interne doivent mettre en œuvre une double authentification par mot de passe et token ainsi qu'une demande de réauthentification périodique en cas de connexion de longue durée.

3 SECURITE SYSTEME

3.1 POSTES DE TRAVAIL

- Service administration des Systèmes & Réseaux
  - Chaque poste doit être configuré pour demander une authentification lors de l'ouverture de session locale ou réseau.
  - Tous les postes doivent être installés dans le local sécurisé (sauf impératif lié à la production).
  - Chaque poste de travail doit est configuré pour ne pas démarrer sur un support amovible (CD-ROM, clé USB, disquette)
  - L'ensemble des interfaces de communication IP des PC portables doivent être protégées par un firewall local.
  - La configuration sécurité du poste de travail doit est protégée vis à vis de l'utilisateur par une stratégie de groupe
  - Un mot de passe doit est demandé pour accéder au BIOS du poste.
  - Chaque poste doit est configuré pour empêcher la désactivation de l'antivirus.
  - Tout utilisateur ayant accès à un poste de travail doit être pourvu d'un identifiant personnel et unique pour accéder à ce poste (sauf production).
  - Tout poste de travail connecté au réseau de production doit être identifié et administré.
  - Chaque poste de travail connecté au réseau interne doit disposer d'un antivirus actif et à jour.
  - Les correctifs de sécurité doivent être appliqués en moins d'une semaine sur les postes de travail (serveurs = une fois tous les 3 mois lors des redémarrages planifiés le WE).
  - Des outils de chiffrement orientés fichiers doivent être mis à disposition sur le poste de travail des programmeurs de production pour protéger les éventuelles informations confidentielles.
  - Le contenu logiciel des postes de travail virtualisés doit être régulièrement contrôlé.

3.2 UTILISATION DES RESSOURCES INFORMATIQUES

- Service administration des Systèmes & Réseaux
  - Les données des équipements réseau, des serveurs et des postes de travail (fichiers, comptes, URLs, compte de messageries, etc.) doivent être supprimées suite au départ de collaborateurs.
  - Les postes de travail doivent disposer d'une mise en veille protégée par mot de passe en cas d'inactivité prolongée.
- Service Programmation et Fabrication
  - Aucunes données sensibles (ex: données clients, données bancaires, etc.) ne doivent être stockées sur les postes de travail

3.3 ACCES LOGIQUES

- Service administration des Systèmes & Réseaux
  - Le compte administrateur possédant le privilège le plus élevé du système doit être déposé dans une enveloppe scellée dans un coffre de banque.
  - Les mesures de sécurité suivantes doivent être imposées techniquement pour protéger les mots de passe : longueur de 8 caractères minimum; combinaison d'au moins trois des critères suivants : majuscules, minuscules, chiffres et caractères spéciaux;
  - Imposer aux utilisateurs le blocage systématique du compte avec une temporisation de 30 min avant toute nouvelle tentative au bout de 3 saisies erronées.
  - Imposer aux utilisateurs le renouvellement tous les trois mois et non réutilisation des 3 derniers mots de passe (sauf compte de service)
  - Les comptes inutilisés pendant une période de plus de 60 jours doivent être systématiquement désactivés.
  - Aucun mot de passe ne doit être stocké en clair sur les serveurs.
  - Les journaux d'évènements des équipements réseaux et systèmes doivent être analysés fréquemment.
  - La liste des droits attribués aux utilisateurs doit être tenue à jour dans le classeur des fiches personnelles « Sécurité de l'accès au bâtiment et à l'informatique ».

3.4 MESSAGERIE

- Service administration des Systèmes & Réseaux
  - La boîte aux lettres d'un utilisateur qui a quitté l'entreprise doit être systématiquement supprimée ou relayée à un collaborateur.
- Service Programmation et Fabrication
  - Les programmeurs ont l'obligation d'utiliser, pour l'envoi de leurs messages confidentiels, la fonction de chiffrement.

4 SECURITE APPLICATIVE

4.1 ACCES INTERNET

- Service administration des Systèmes & Réseaux
  - L'accès à des sites réputés illégaux ou dangereux doit être interdit.
  - Les journaux de connexion Internet doivent être conservés à titre de preuve sur les durées minimales et maximales conformes à la législation (URL visitées, date et heure, identifiant de l'utilisateur).

4.2 APPLICATION WEB

- Service Développement
  - L'accès à l'application Web de l'entreprise doit nécessiter une authentification préalable de l'utilisateur (authentification forte)
  - Les données saisies par l'utilisateur de l'application doivent être contrôlées.
  - Les applications doivent enregistrer les traces de l'activité des utilisateurs

5 MANAGEMENT SECURITE

5.1 ACCES LOGIQUES

➢ Service RH

- Des procédures « Fiches individuelles de Sécurité » sont appliquées pour l'attribution de compte, à l'arrivée d'un utilisateur, lors d'un mouvement ou d'un changement de fonction d'un utilisateur et lors de départ d'un utilisateur.

5.2 PRATIQUES GENERALES

➢ Service administration des Systèmes & Réseaux

- La procédure de destruction ou d'effacement définitif des données sur les supports de stockage (disque dur, cartouche de sauvegarde ···) doit être systématiquement réalisée avant mise au rebut, réaffectation ou cession des supports contenant des informations sensibles.
- Lors des périodes de non-utilisation de la télémaintenance, la liaison vers l'extérieur doit être désactivée.

5.3 DOCUMENTATION

➢ Tous les services

- Avant d'être mis au rebut, tous les documents utilisés doivent être détruits de façon irréversible et définitive (broyeur de papiers dans chaque bureau, broyeurs de documents industriels dans l'atelier).

5.4 R.H.

➢ Service RH

- Le personnel embauché ou intérim doit fournir une copie du bulletin N°3 du casier judiciaire.
- Le personnel doit être sensibilisé à la sécurité informatique (y compris les mesures disciplinaires en cas de non-respect, le respect de la confidentialité étant inscrit dans les contrats de travail)
- Le personnel s'engage à ne pas divulguer les informations dont il peut avoir connaissance en raison de ses fonctions ou du seul fait de son appartenance à la société. Il s'interdit en conséquence d'en conserver des copies, de les transmettre à des tiers sans l'accord exprès de la Direction et à plus forte raison, de les utiliser pour son usage personnel.
- Le personnel s'engage à prendre toutes les précautions conformes aux usages et à l'état de l'art dans le cadre de ces attributions afin de protéger la confidentialité des informations auxquelles il a accès et d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

5.5 POSTES DE TRAVAIL

- Tous les services
  - Les utilisateurs sont informés sur les règles d'usage du poste de travail (respect de la configuration du poste, arrêt du poste de travail le soir, non-divulgation du mot de passe, verrouillage des sessions utilisateurs, ...).

5.6 UTILISATION DES RESSOURCES INFORMATIQUES

- Service RH
  - Les utilisateurs doivent prendre connaissance, grâce au contrat de travail qui y fait référence, de l'existence de documents spécifiant les conditions d'utilisation des équipements informatiques (charte d'utilisation, règlement intérieur).
- Tous les services
  - Les utilisateurs sont informés des risques liés à l'utilisation d'Internet ou de la messagerie (hameçonnage, virus ou chevaux de Troie dans des fichiers téléchargés ou reçus par messagerie, niveau de confiance à accorder aux messages reçus par Internet, ...)
  - Les utilisateurs sont informés de leur responsabilité en matière de protection et de sauvegarde des données stockées sur leur poste de travail en l'absence de sauvegarde automatique.
  - Les utilisateurs ont l'obligation de conserver leurs données sur les disques serveurs ou à l'aide des moyens mis à disposition sur les portables, plutôt que sur leur poste en local.
  - Les utilisateurs sont informés que l'utilisation des ressources doit être réservé à un seul usage professionnel et que les connexions au réseau et à l'internet sont tracées (disposition du RI)
  - Les utilisateurs doivent valider la prise de main à distance de leur poste par l'administrateur en cas de demande de dépannage.

6 SAUVEGARDE ET ARCHIVAGE

- Service administration des Systèmes & Réseaux
  - Les supports physiques de sauvegarde du mois précèdent doivent être stockées dans le coffre-fort loué à l'une de nos banques.
  - L'archivage des données doit être conservé deux mois (hors spécificité contractuelle).
  - Une restauration réelle doit être réalisée au moins une fois par mois.
  - En cas de réaffectation ou de mise au rebut des équipements (postes de travail, des serveurs, des systèmes de stockage, disque dur, supports amovibles,...), le matériel doit faire l'objet d'un effacement préalable définitif des données.