Vallée Sud Habitat

Politique de Sécurité des Systèmes d'Information (PSSI)

Objet :	Document regroupant l'ensemble des points de sécurité du système d'information de Vallée Sud habitat

Référence du Document :	
Version du document :	V.1
Date :	13/11/2024

Auteur du document :	DSI

Confidentialité

Ce document est strictement privé et confidentiel. Il ne peut être diffusé ou reproduit à l'extérieur de l'entreprise. Son contenu ne peut être utilisé sans l'accord de Vallée Sud Habitat.

Contacts

Toutes questions sur ce document peuvent être adressée à :

Nom ou Fonction	Téléphone	E-mail
DSI	06 28 46 48 21	
Responsable du contrôle Interne	06 26 08 39 69	Ines.allani@valleesudhabitat.fr

Validé par :

Suivi du document

Distribution Control

Nombre de Copies	Distribution
3	DSI
	Direction générale
	Conseil d'administration

Personnes impliquées dans la rédaction de ce document

Fonction	Nom
DSI	

Liste des relecteurs

Revu par	Date
Administrateurs réseau	13/11/2024
Direction générale	18/11/2024
Contrôle Interne	20/11/2024
Conseil d'administration	

Historique des versions

Version	Date	Description de la révision	Modifié par
V1	15/11/2024	Création du document	DSI

Abréviations utilisées dans le document

PSSI	Politique de sécurité du système d'information
VSH	Vallée Sud Habitat
PRA	Plan de reprise d'activité
VPN	Virtual Private Network

Sommaire

1 Description du projet

1.1 Présentation

La sécurité du système d'information est cruciale pour une entreprise car elle protège les données et les systèmes informatiques contre les menaces telles que le vol, la fraude, les cyberattaques et les pannes techniques :

1. **Protection des Données Sensibles** : Vallée Sud Habitat détient des informations confidentielles comme des données clients ou des informations financières et sociales. Une fuite ou une perte de ces données peut entraîner des pertes financières, des poursuites judiciaires et nuire à la réputation de l'entreprise.

2. **Conformité Réglementaire** : De nombreuses régulations, comme le RGPD (règlement général de protection des données), exigent des entreprises qu'elles protègent les données personnelles. Le non-respect de ces régulations peut entraîner des amendes importantes et des sanctions juridiques.

3. **Continuité des Activités** : Une cyberattaque ou une panne des systèmes peut interrompre le fonctionnement de l'entreprise, entraînant des pertes de revenus et des dommages à long terme. La sécurité de l'information assure la continuité des activités en prévenant ou en minimisant ces interruptions.

4. **Réputation et Confiance** : Les clients/locataires et les partenaires (Etat, collectivités locales, CAF, …) s'attendent à ce que leurs données soient sécurisées. Un incident de sécurité peut gravement ternir la réputation de l'entreprise et entraîner une perte de confiance.

1.2 Objectifs

Les objectifs d'une Politique de Sécurité des Systèmes d'Information (PSSI) sont de définir les lignes directrices et les mesures à suivre pour protéger les ressources informationnelles de l'entreprise. Les principaux objectifs sont :

- **Protéger la confidentialité**
- **Assurer l'intégrité des données**
- **Garantir la disponibilité des systèmes et des données**
- **Conformité aux réglementations**
- **Prévention des cybermenaces**
- **Sensibilisation et formation des utilisateurs**
- **Réduction des risques**
- **Réaction et gestion des incidents**
- **Amélioration continue**

Une PSSI permet de créer un cadre solide pour la protection des systèmes d'information, tout en assurant que l'entreprise peut fonctionner efficacement et en toute conformité avec les exigences légales et réglementaires.

2 Périmètre couvert par la PSSI

La PSSI De Vallée Sud Habitat couvre l'ensemble du système d'information et des utilisateurs. Cela inclut les réseaux, les applications, les dispositifs mobiles et les utilisateurs internes.

2.1 Description générale :

Description plus détaillée du périmètre concernant l'existant ou l'avenir :

Systèmes d'Information

- **Infrastructures Informatiques** : Serveurs, réseaux, systèmes de stockage, équipements de communication, etc.
- **Applications et Logiciels** : Tous les logiciels utilisés dans l'entreprise, y compris les systèmes de gestion d'entreprise (ERP) et les applications personnalisées.
- **Systèmes de Sécurité** : Pare-feu, systèmes de détection d'intrusion, antivirus, systèmes de gestion des identités et des accès, etc.
- **Dispositifs Mobiles** : Smartphones, tablettes, ordinateurs portables, et autres périphériques mobiles utilisés pour accéder aux systèmes d'information.

Données

- **Données Sensibles** : Informations financières, données clients, données personnelles des employés, données sociales, etc.
- **Bases de Données** : Tous les systèmes de gestion de bases de données qui stockent les informations de l'entreprise.
- **Documents et Fichiers** : Tous les fichiers numériques et documents, qu'ils soient stockés sur des serveurs locaux, dans le cloud, ou sur des périphériques mobiles.

Utilisateurs

- **Employés** : Tout le personnel de l'entreprise, y compris les dirigeants, les managers, et les employés.
- **Utilisateurs Externes** : Clients ou autres parties externes qui peuvent avoir un accès limité aux systèmes ou aux données (par exemple via un portail client).

Sites Physiques

- **Bureaux et Sièges Sociaux** : Tous les sites physiques où l'entreprise opère et où des systèmes d'information sont utilisés.
- **Centres de Données** : Lieux où les serveurs et autres infrastructures critiques sont hébergés.
- **Installations Distantes** : Sites distants, succursales, et bureaux mobiles.

Processus Métiers

- **Processus Critiques** : Activités clés de l'entreprise qui dépendent des systèmes d'information, telles que la gestion des locataires, la comptabilité, les RH, etc.
- **Flux de Travail** : Les flux de données et les procédures qui soutiennent les opérations quotidiennes.

Technologies et Outils

- **Technologies en place** : Toute technologie ou outil utilisé pour la gestion, le stockage, la transmission, et la protection des informations (y compris les solutions cloud, les plateformes de collaboration, etc.).
- **Outils de Développement** : Outils et environnements utilisés pour le développement interne de logiciels ou d'applications.

Composants Réseau

- **Réseaux Internes** : Tous les réseaux locaux (LAN, Local Area Network) utilisés au sein de l'entreprise.
- **Réseaux Externes** : Connexions internet, VPN (Virtual Private Network), et autres moyens de communication avec l'extérieur.
- **Périphériques Connectés** : Routeurs, commutateurs, points d'accès Wi-Fi, et autres dispositifs de réseau.

Environnement Cloud et Hébergé

- **Services Cloud** : Tous les services de « cloud computing » utilisés par l'entreprise, incluant le SaaS (Software as a Service), le PaaS (Platform as a Service), et l'IaaS (Infrastructure as a Service).
- **Hébergement Externe** : Données ou applications hébergées par des tiers.

3 Rôles et responsabilités

3.1 Direction Générale

Responsabilités :

- Définir l'orientation stratégique de la sécurité de l'information.
- Approuver la PSSI et les budgets alloués à la sécurité.
- Veiller à ce que la sécurité de l'information soit intégrée dans la culture de l'entreprise.

Rôles :

- Prendre les décisions finales concernant les politiques de sécurité.
- S'assurer que la PSSI est alignée avec les objectifs business et la conformité réglementaire.
- Nommer le Responsable de la Sécurité des Systèmes d'Information (RSSI) ou à défaut le Directeur des Systèmes d'Information (DSI).

3.2 DSI

Responsabilités :

- Élaborer, mettre en œuvre et surveiller la PSSI.
- Identifier et évaluer les risques en matière de sécurité de l'information.
- Mettre en place des mesures de sécurité techniques et organisationnelles.
- Coordonner la réponse aux incidents de sécurité.

Rôles :

- Superviser les initiatives de sécurité à l'échelle de l'entreprise.
- Conseiller la direction sur les questions de sécurité.
- Organiser des audits de sécurité réguliers et assurer le suivi des actions correctives.
- Définir les action correctrices à mettre en œuvre.

3.3 Equipe IT

Responsabilités :

- Mettre en œuvre les mesures de sécurité définies par le DSI.
- Maintenir l'infrastructure technique sécurisée (réseaux, systèmes, applications).
- Gérer les accès, les sauvegardes, et les mises à jour des systèmes.
- Surveiller les systèmes pour détecter les incidents de sécurité.

Rôles :

- Administrer les systèmes d'information en suivant les politiques de sécurité.
- Réaliser des tests de sécurité (tests de pénétration, scans de vulnérabilité).
- Participer aux réponses aux incidents en fournissant un support technique.

3.4 Utilisateurs

Responsabilités :

- Adhérer à la charte informatique, aux politiques de sécurité et aux bonnes pratiques établies par la PSSI.
- Signaler toute activité suspecte ou incident de sécurité au service compétent.
- Participer aux formations de sensibilisation à la sécurité de l'information.

Rôles :

- Utiliser les systèmes d'information de manière responsable et sécurisée.
- Suivre les procédures pour la gestion des mots de passe, le traitement des données, etc.
- Éviter les comportements à risque, comme l'ouverture de courriels suspects ou le partage non autorisé d'informations sensibles.
- Accepter de mettre en œuvre les actions correctrices.

3.5 Responsables de service

Responsabilités :

- Intégrer les exigences de sécurité dans les processus métiers.
- S'assurer que les employés de leur département comprennent et respectent la PSSI.
- Collaborer avec le DSI pour identifier les risques spécifiques à leurs activités.

Rôles :

- Communiquer les attentes en matière de sécurité aux membres de leur équipe.
- Veiller à ce que les projets et les nouvelles initiatives respectent les politiques de sécurité.
- Contribuer à l'évaluation des risques pour leur domaine de responsabilité.
- Contribuer à mettre en œuvre les actions correctrices au sein de leurs services et s'assurer de la participation de leurs équipe.

4 Gestion des risques

Une cartographie des risques a été réalisée conjointement entre la DSI et la responsable du Contrôle Interne. Cette cartographie en Annexe 1 comporte les éléments suivants indispensables à une PSSI :

- Une liste des risques (intitulé, univers du risque).
- Evaluation du risque brut : Probabilité et Impact brut (financier, image, juridique, sécurité des personnes).
- Evaluation de la maitrise : évaluation du dispositif de maitrise et éléments de maitrise.
- Priorisation.

Cette cartographie sera régulièrement mise à jour et systématiquement réinterrogée lors d'éventuels incidents.

5 Mesures de sécurité

5.1 Contrôles d'accès

Windows

La gestion de l'authentification Windows est renforcée au sein de Vallée Sud Habitat par l'utilisation de l'outil « Specops ». Cet outil analyse la force des mots de passes utilisés par calcul d'entropie comme recommandé par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Les utilisateurs ont le choix entre un mot de passe ou une « pass phrase ». L'outil possède une base de données mise à jour régulièrement de tous les mots de passe déjà compromis et refuse l'utilisation de ceux-ci. De plus nous avons ajouté les mots clés suivant en liste rouge : Clamart, Chatillon, Habitat, Vallée, Sud, Bourg la reine, Bagneux.

Les utilisateurs sont plus autonomes sur la complexité des mots de passe avec un système de « récompense » : plus le mot de passe est robuste, plus sa validité sera longue.

Office 365

L'accès à « Office 365 » est protégé par la multi authentification pour les personnes ayant un smartphone d'entreprise.

Mot de passe

En interne l'outil « Vaultwarden » est disponible pour l'ensemble du personnel comme gestionnaire de mot de passe. Cet outil remplace « Keypass » devenu obsolète. La base de données cryptée des mots de passe est sauvegardée en interne.

Fichiers d'entreprise

L'accès aux fichiers d'entreprise est sécurisé par des groupes d'accès géré par Windows Serveur. Les utilisateurs au sein de Vallée Sud Habitat n'ont accès qu'aux fichiers qui leur est nécessaire pour travailler. De plus les utilisateurs ne voient que les dossiers auxquels ils doivent avoir accès grâce à un paramétrage avancé de l'énumération sur le serveur de fichier.

Accès administrateur

Les administrateurs systèmes et réseaux de l'entreprise ainsi que le directeur des systèmes d'information utilisent des comptes nominatifs dédiés en tiers pour l'administration des serveurs.

Il existe 3 comptes par administrateur (T0, T1 et T2) avec 3 niveaux d'habilitation. Le compte T2 est seulement administrateur des postes de travail, ce compte existe aussi pour les techniciens informatiques. Le compte T1 a le rôle d'administrateur des serveurs non critique (serveurs métier). Le compte T0 est un compte administrateur des serveurs les plus important (AD, DNS, Serveur de fichiers, AD Connect et Specops).

Les identifiants « administrateurs du domaine » ou « administrateur local des serveurs » ne sont utilisés qu'en dernier recours.

WIFI : interne et invité

VSH propose un système de wifi pour les utilisateurs ainsi que pour les invités de l'entreprise qui en auraient besoin. Le Wifi d'entreprise, appelé VSH-Corp est sécurisé par le protocole 802.1X qui permet une authentification par l'active directory. Il permet aux utilisateurs de travailler avec les mêmes accès qu'une connexion filaire.

Le Wifi invité, appelé VSH-Guest, n'est accessible qu'avec un compte temporaire crée sur le pare-feu à la demande d'un salarié. La création de ce compte relève de la DSI et est soumis à la vérification de l'identité de l'utilisateur invité. Ce Wifi donne accès seulement à internet.

5.2 Sécurisation des réseaux

Pare-feux

Des pare-feux physiques de marque Fortinet se trouvent dans chacune des antennes de Vallée Sud Habitat. Sur ces pare-feux sont activés les protocoles : Webfiltering, IDS, IPS.

L'accès au réseau d'entreprise par VPN est possible avec l'application Forticlient qui permet la connexion distante pour les utilisateurs nomades ou en télétravail. Le protocole de protection des connexions SSL est activé pour ces connexions.

Les pare-feux des différentes agences communiquent avec ceux du siège par VPN site-à-site afin de permettre aux utilisateurs des agences de communiquer avec le réseau d'entreprise.

Filtrage Web

L'accès à internet est filtré depuis les pare-feux et bloque l'accès à plusieurs catégories de site internet (ex : arme, drogue, jeu, …). De plus, la politique interne de Vallée Sud Habitat ajoute le blocage des sites de création de PDF (ex : ilovepdf.com, pdf24.com, …) et de transferts de fichiers non-souverains (ex : wetransfer.com, …) afin d'éviter la fuite de données. Ces fonctionnalités sont accessibles avec des outils internes.

Plan d'adressage réseau

Début plage IP	Fin plage IP	MASQUE	Nom	ID VLAN	PASSERELLE
172.24.0.1	172.24.0.254	255.255.255.0	SIEGE-SERVERS-HISTORIQUE	60	172.24.0.254
172.24.10.1	172.24.10.254	255.255.255.0	SIEGE-USERS	10	172.24.10.254
172.24.4.1	172.24.4.254	255.255.255.0	SIEGE-SERVERS	4	172.24.4.254
172.24.12.1	172.24.12.254	255.255.255.0	SIEGE-WIFI-CORPORATE	12	172.24.12.254
172.24.14.1	172.24.14.254	255.255.255.0	SIEGE-WIFI-PUBLIC	14	172.24.14.254
172.24.20.1	172.24.20.254	255.255.255.0	MGMT	15	172.24.20.254
			BACKUP	55	172.24.55.254

Début plage IP	Fin plage IP	MASQUE	Nom	ID VLAN	PASSERELLE
172.25.10.1	172.25.10.254	255.255.255.0	CLAMART-USERS	110	172.25.10.254
172.25.4.1	172.25.4.254	255.255.255.0	CLAMART-SERVERS	104	172.25.4.254
172.25.12.1	172.25.12.254	255.255.255.0	CLAMART-WIFI-CORPORATE	112	172.25.12.254
172.25.14.1	172.25.14.254	255.255.255.0	CLAMART-WIFI-PUBLIC	114	172.25.14.254
172.25.20.1	172.25.20.1	255.255.255.0	MGMT	115	172.25.20.254

Début plage IP	Fin plage IP	MASQUE	Nom	ID VLAN	PASSERELLE
172.26.10.1	172.26.10.254	255.255.255.0	CHATILLON-USERS	210	172.26.10.254
172.26.4.1	172.26.4.254	255.255.255.0	CHATILLON-SERVERS	204	172.26.4.254
172.26.12.1	172.26.12.254	255.255.255.0	CHATILLON-WIFI-CORPORATE	212	172.26.12.254
172.26.14.2	172.26.14.255	255.255.255.0	CHATILLON-WIFI-PUBLIC	214	172.26.14.254
172.26.20.1	172.26.20.254	255.255.255.0	MGMT	215	172.26.20.254

5.3 Protection des systèmes et des d'applications

Gestion des correctifs

Les mises à jour des postes de travail sont configurées en automatique.

Les salariés de la DSI consacrent un samedi par mois aux mises à jour des éléments suivant :

- Serveurs virtuels Windows et Linux,
- Hyperviseurs,
- ERP Aravis,
- Pare-feux,
- Bornes wifi,
- Switch.

EDR

Les postes de travail et les serveurs sont protégés par un EDR (Endpoint Detection and Response) qui fonctionne en collaboration avec l'antivirus Windows defender. Un EDR est une solution de cybersécurité conçue pour surveiller, détecter et bloquer les activités malveillantes des terminaux. Il est aussi capable d'isoler un terminal du réseau local en cas de compromission.

De plus, l'EDR crée une base de données des IP malveillantes relevées depuis les terminaux afin de les interdire directement depuis les pare-feux.

5.4 Gestion des incidents de sécurité

La notion d'incident est très large et couvre des domaines variés : incident technique, incident fonctionnel, incident social, incident de sécurité, incident de communication, incident de paiement, incident financier, etc. D'une manière générale, un incident peut être défini comme un événement causant des dommages ou susceptible de le faire à des personnes ou à des organisations.

Quelle que soit l'approche, la gestion des incidents a pour objectif la détection et le traitement des incidents (à priori et à posteriori). Le processus de gestion des incidents inclut en général la détection de l'incident, les analyses et diagnostics, la résolution de l'incident et/ou le rétablissement du service affecté. Un aspect important de la gestion des incidents est le suivi (reporting) de ce processus et la capitalisation (bilan).

La qualité de service et la performance des organisations exigent la mise en place d'une gestion efficace des incidents et des problèmes. La gestion des incidents est également un dispositif essentiel du Plan de Reprise d'Activité (PRA), car elle définit les procédures d'escalade qui permettent d'être plus réactif pour le déclenchement des plans de secours.

5.4.1 Définition d'un incident de Sécurité du Système d'Information

Dans ce document nous désignerons par incident SSI (Sécurité du Système d'Information) un événement, potentiel (au sens « signes précurseurs ») ou avéré, indésirable et/ou inattendu, impactant ou présentant une probabilité forte d'impacter la sécurité de l'information dans ses critères de Disponibilité, d'Intégrité, de Confidentialité et/ou de Preuve.

Un incident SSI correspond à une action malveillante délibérée, au non-respect d'une règle de la Politique de Sécurité du Système d'Information (PSSI) 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. Concernant la disponibilité, on fera la différence entre les sinistres majeurs (incendie, inondation, etc.) nécessitant l'activation d'une cellule de crise et les autres incidents (panne d'un serveur). Une atteinte à la disponibilité pourra être considérée comme étant un incident de sécurité (déni de service suite à une intrusion) ou non (panne de serveur suite à une défaillance d'un composant), après analyse des causes.

5.4.2 Organisation de la gestion des incidents SSI

Une politique de gestion des incidents de sécurité passe par la définition de deux objectifs majeurs :

- Assurer que les événements et failles de sécurité sont signalés rapidement pour permettre des actions correctives ou complémentaires dans les meilleurs délais.
- Garantir une approche cohérente et efficace dans le traitement des incidents de sécurité de l'information.

Une fois l'incident qualifié en tant qu'incident de sécurité il doit être confié à l'équipe adéquate pour l'analyse, l'évaluation d'impact, les actions correctives et la remise en fonction du service affecté.
Ces équipes sont :

- La cellule Helpdesk constitué de techniciens micro et réseau
- L'équipe d'administration système et réseau

La cellule Helpdesk intervient en premier lieu lors d'un incident déclaré. Il convient à cette cellule de faire la première analyse et la qualification de l'incident. Si l'incident dépasse les capacités de résolution de cette cellule il sera escaladé à l'équipe d'administration système et réseau.

Indépendamment du modèle d'organisation les membres de chaque équipe doivent disposer des moyens fiables et sécurisés de communication interne, mais également externe pour collaborer avec les équipes concernées dans le cadre de leur activité.
Un autre aspect de l'organisation de moyens de gestion d'incidents de sécurité est la décision du mode de gestion des ressources humaines et des services.

Dans le cas le plus simple l'équipe est constituée d'employés de l'entreprise ou de l'organisme et prend en charge l'ensemble des services. Nous avons pris la position de nous faire épauler d'une équipe externe (SOC : Security Operation Center) qui gère la qualification des incidents relevé par le logiciel FortiEDR.

Une équipe de réponse aux incidents de sécurité doit répondre à différents objectifs imposés par son environnement. Parmi ses objectifs on peut lister :

- La rationalisation de la veille dans l'entreprise ou l'organisme,
- La nécessité de traiter rapidement tout type d'incident de sécurité par du personnel qualifié habilité et avec des modes opératoires éprouvés,
- La nécessité d'avoir une vue du risque d'exposition du SI de l'entreprise ou de l'organisme.

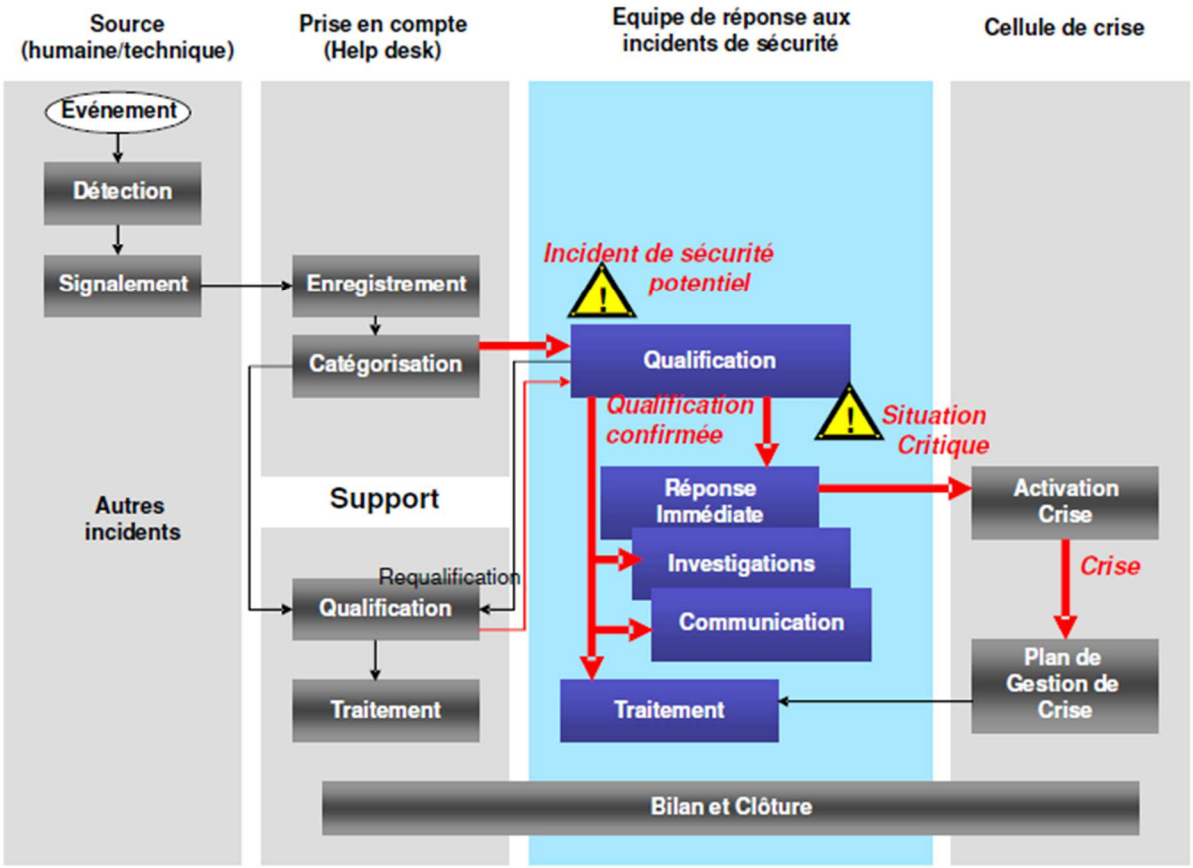
Ces objectifs répondent aux stratégies de l'entreprise.

Cet environnement complexe requiert d'être maintenu à jour pour assurer une pleine capacité de réaction à l'équipe de réponse aux incidents. Une veille permanente et attentive aux nouvelles tendances et méthodes d'attaques est également nécessaire.
Pour être contactée rapidement, l'équipe de réponse aux incidents bénéficie d'une bonne visibilité en interne comme en externe.

La cellule Helpdesk est joignable facilement par une adresse e-mail générique : hotline@valleesudhabitat.fr ainsi qu'un numéro unique joignable depuis le softphone interne au 400. Ce numéro fait sonner une file d'appel constituée comme suivant : La cellule helpdesk, puis les administrateurs réseau et enfin le Directeur des systèmes d'information.

Processus de traitement des incidents

Le processus de gestion des incidents de sécurité est représenté par le schéma ci-dessous. La particularité du traitement des incidents de sécurité tient à l'intervention de l'équipe de réponse aux incidents de sécurité. Les autres volets du processus appartiennent, soit au processus général de gestion des incidents (prise en compte de l'incident, catégorisation, qualification, traitement), soit au processus de gestion de crise.



Le signalement d'un événement susceptible d'être qualifié d'incident de sécurité est réalisé soit par une personne (utilisateur, administrateur, etc.), par des moyens techniques (outils de surveillance, etc.) ou par le SOC.
La prise en compte est réalisée en général par la cellule Helpdesk. D'autres circuits peuvent exister.
Dans tous les cas, il est nécessaire que l'événement soit enregistré de manière à pouvoir en faire un suivi donc dans le logiciel de suivi de ticket : GLPI.
C'est à ce stade de la prise en compte que l'événement peut être catégorisé : « incident à risque ».
Ces incidents sont immédiatement soumis à l'équipe d'administration système. Les autres types d'incident restent traités par la cellule Help Desk.
L'équipe d'administration système après analyse, confirme ou infirme la catégorisation « incident de sécurité » (qualification). Les incidents non confirmés « incident de sécurité » sont retransmis aux équipes support si cela relève de leur compétences. Les incidents qualifiés « de sécurité » font alors l'objet d'un traitement spécifique dont les particularités sont développées plus bas dans le document. Outre les investigations complémentaires, le traitement des incidents de sécurité peut nécessiter des actions spécifiques telles que la préservation des preuves ou des actions adaptées de communication.
Lorsque l'équipe d'administration système n'est plus à même de gérer la situation, ou lorsque les conséquences potentielles sont à un niveau trop important, la cellule de crise est alertée et juge de l'opportunité de passer en mode « gestion de crise ».

Au sein de Vallée Sud Habitat la cellule de crise est constituée des administrateurs systèmes et réseau, du directeur des systèmes d'information, de la responsable du contrôle interne et d'un membre de la direction générale.

5.4.3 Dans le cas d'un incident

Détection et signalement

La détection peut avoir pour origine :

- Toute personne qui a connaissance d'un fait ou d'une menace pour l'organisme (par exemple comportement anormal d'un équipement, d'une application ou d'une personne),
- Un administrateur lorsqu'il est informé par un dispositif de supervision ou lorsqu'il constate une anomalie lors de contrôles,
- Un membre du SOC lorsqu'il est informé par l'outil de surveillance (détection d'intrusion ou d'action frauduleuse) ou lorsqu'il constate une anomalie lors de contrôles.

L'anomalie doit pouvoir être signalée à une personne compétente dans les plus brefs délais. Le contact habituel pour l'utilisateur est le helpdesk. Cependant, il doit également être possible de contacter directement un responsable de la sécurité en toute discrétion si la situation l'exige. Les utilisateurs doivent être sensibilisés et informés sur les différents niveaux d'alerte. Dans tous les cas, on doit s'assurer que les moyens d'alerte sont suffisamment rapides, y compris en dehors des heures ouvrées, pour permettre une réponse adaptée (empêcher que l'incident se poursuive, préserver les preuves, etc.).

Des mesures immédiates peuvent être associées à la détection par l'activation automatique de mécanismes de protection contenu dans l'outil EDR ou XDR (actuellement : FortiEDR).

Enregistrement de l'incident

Comme indiqué précédemment, un incident supposé de sécurité peut être signalé à différentes personnes, en général le helpdesk, selon des procédures devant être connues de tous. Dans tous les cas, la personne qui réceptionne l'appel ou l'alerte doit en accuser réception.

L'événement doit immédiatement être enregistré dans une base de données des incidents (logiciel support : GLPI).

A ce stade de la procédure, l'événement n'est pas encore qualifié d'incident de sécurité mais il est catégorisé. L'enregistrement de l'événement doit comporter à minima la date et l'heure de l'alerte, son origine (personne ou dispositif technique), les coordonnées du déclarant, une description aussi précise que possible de l'événement et sa catégorisation. Comme pour tout incident, un numéro de dossier est généré et communiqué par mail de façon automatique.

La personne qui enregistre l'événement doit également mentionner l'action immédiate déclenchée (par exemple transmission à l'équipe d'administrateurs système pour qualification).

L'enregistrement de l'événement est essentiel à plusieurs titres. Il permet de garder une trace de chaque événement et d'en effectuer un suivi dans toutes les phases ultérieures, d'analyse ou de traitement, jusqu'à la fermeture du dossier.

La base des événements constitue également un outil d'analyse a posteriori dans le cadre d'analyses de risques, pour évaluer l'efficacité des dispositifs en place ou pour identifier des incidents récurrents pouvant être qualifiés de « problème ».

Par exemple : l'équipe d'administrateurs système peut également être sollicitée à chaque fois qu'une équipe support ou qu'un membre du personnel pense être face à un événement susceptible d'avoir un impact fort sur l'organisation.

Les consignes peuvent éventuellement spécifier que tout incident susceptible d'être d'origine malveillante ou concernant certains équipements ou logiciels ou encore signalé par certains dispositifs techniques, doit être transmis à l'équipe d'administrateurs système.

Qualification par l'équipe de réponse aux incidents de sécurité

Une première analyse, conduite par l'équipe d'administrateurs système, confirme ou infirme la catégorisation « incident de sécurité ». Les incidents non confirmés « incident de sécurité » sont transmis aux équipes support pour traitement. L'équipe d'administrateurs système procède si nécessaire à des investigations complémentaires pour qualifier l'événement. Les critères d'évaluation d'impact prenant en compte différents axes d'analyse (impacts financiers, impacts sur l'image, impacts sur les clients ou partenaires, risques de poursuite judiciaire, etc.) doivent être préétablis et mis à la disposition de l'équipe. Typiquement ces critères sont issus de l'analyse de risque.

5.4.4 Réponse à l'incident SSI

Mesures de réponses immédiates

Suite à la qualification, des mesures d'urgence peuvent être prises pour limiter les impacts et préserver les traces. En effet, même sans connaître précisément la nature de l'incident, son origine ou son impact réel qui seront l'objet de la phase d'analyse, le simple fait d'identifier le type de danger peut déclencher des actions palliatives, comme par exemple :

- Un confinement (ex : débranchement du réseau d'un poste infecté pour le mettre dans un VLAN de quarantaine),
- Une isolation (ex : couper tous les flux de messagerie Internet),
- Une communication ciblée de recommandations.

Certaines de ces mesures peuvent être prévues à l'avance dans des procédures du support et de l'équipe sécurité.

Si ces mesures s'avèrent insuffisantes ou/et si la situation n'est pas maitrisée ou/et si le niveau d'impact de l'incident le justifie, au regard des critères d'évaluation, la cellule de crise doit être activée.

Investigations

L'analyse de l'incident a pour objectif de préciser les éléments suivants :

- La nature de l'incident,
- Le fait générateur,
- Le périmètre concerné,
- L'impact.

Ces éléments permettront de définir les actions à entreprendre. Dans certains cas les conclusions de l'investigation peuvent conduire à l'activation de la cellule de crise.

Préservation des traces

Certaines précautions doivent être prises. En particulier, en cas de piratage par exemple, si le but de l'analyse est de remonter à la source de la manipulation frauduleuse et de prendre des mesures légales à l'encontre des auteurs des faits, il est nécessaire de préserver les informations d'origines (logs, etc.) afin de conserver le contexte de preuve.

En effet, l'analyse peut, dans certains cas modifier (le travail d'analyse génère lui-même des traces qui se confondent ensuite avec les traces laissées par l'agresseur), voire effacer, les traces du passage d'un 'attaquant'. De fait, il est nécessaire de sauvegarder (par exemple via une copie intégrale, de type bit à bit) les informations avant d'entreprendre toute action susceptible de nuire à l'intégrité des données sur le support d'origine.

Si une copie complète des disques n'est pas réalisable ou l'est difficilement, il faut au moins conserver une copie des logs (journaux de connexions au système). Toutefois, cette sauvegarde n'est pas toujours simple à mettre en œuvre et peut nécessiter des outils et/ou des compétences particulières.

Enfin, les données ainsi sauvegardées doivent être protégées physiquement et un cadre opératoire doit être mis en œuvre qui précisera notamment par qui ces sauvegardes ont été effectuées, à quel moment, comment elles ont été protégées et qui y a eu accès. En fonction des enjeux, il peut être recommandé de faire appel à un huissier de justice.

Le travail d'investigation pourra alors commencer, si possible sur les copies de sauvegarde, les disques durs d'origine étant rangés en lieu sûr (une procédure pouvant durer des mois, voire des années). Ces derniers ainsi que la sauvegarde des logs, pourront servir de preuves en cas de poursuites judiciaires.

Durant l'investigation il est important de déterminer le périmètre concerné :

- Système d'exploitation,
- Réseau et téléphonie,
- Serveurs,

- Applications,
- Locaux,
- Groupe de personnes,
- Données,
- Services,
- Clients, fournisseurs, partenaires, …

Ces actions de recherche et d'identification de l'origine de l'attaque, de la panne ou de recherche de 'l'attaquant' étant très spécifique et nécessitant des compétences particulière il conviendra de faire appel à une société spécialisé dans ce domaine.

Identification du fait générateur et analyse de l'impact

L'objet principal de l'analyse de l'incident proprement dit permet de répondre à plusieurs questions qui se posent, comme par exemples :

- Quelle est la vulnérabilité ou la faiblesse qui a rendu possible l'incident ? C'est la question la plus importante ! En effet, si aucune réponse claire n'est trouvée à cette question, le système restera vulnérable une fois remis en service ; il pourrait être attaqué à nouveau,
- Quel est l'inventaire des dégâts ou quel est l'impact de l'incident ? (Déni de service, baisse de la qualité du service, perte de donnée, divulgation d'information confidentielle, risque sur la réputation, etc.).

5.4.5 Traitement

Mesures pour éviter l'aggravation des conséquences

En complément des mesures de réponses immédiates déjà prises dès la qualification de l'incident, des mesures peuvent être prises pour éviter l'aggravation des conséquences.
Disposant à ce stade des informations obtenues lors des investigations, ces mesures seront plus ciblées que les réponses conservatoires d'urgence :

- Activation de la Cellule de Crise : si elle n'a pas été activée lors de la phase de réponse immédiate, la gestion de crise peut être déclenchée à ce stade, si la situation s'est dégradée entre temps et l'impose,
- Restrictions temporaires d'accès aux réseaux ou/et aux applications : ces restrictions peuvent être, suivant les cas, des blocages ou des simples filtrages. (Exemple : interdiction d'accès à certains sites Web),
- Communications ciblées : pour adapter la communication, il faut évaluer très rapidement la durée de la perturbation (exemple : évaluer la durée de restauration par rapport au volume de données à restaurer en cas de pertes de données). On identifie trois types de communication :
    - Communication vers les utilisateurs. Le communiqué contient en règle générale à minima :

- Les faits qui doivent être édulcorés dans certains cas,
- Les activités impactées du fait des restrictions temporaires en place,
- Des consignes de comportements (exemple : ne pas ouvrir les pièces jointes),
- L'heure prévisionnelle de retour à la normale,

- Communication technique entre homologues (vers les prestataires) :
  - Les faits précis,
  - Les recommandations d'actions,
  - Une proposition d'actions coordonnées,
- Communication vers les externes (locataires, assureurs, fournisseurs, etc.). On peut utiliser si besoin la communication de crise ou des partenaires.

Déclarations du sinistre

Procéder aux déclarations de sinistres en faisant attention à :

- La tenue des délais : généralement 48 heures pour le vol, 5 jours ouvrés au maximum dans la plupart des autres cas auprès de notre assureur.
- Ne rien « toucher » avant la venue de l'expert en assurances ou des forces de polices sauf nécessité.
- En cas de violation de données il faut notifier la CNIL dans les 72H en utilisant le téléservice de notification de violations.

En cas d'urgence, on peut remplacer le matériel et mettre le matériel endommagé de côté (cette mesure ne peut être prise qu'en cas d'urgence, afin d'éviter l'arrêt de l'exploitation). Si le sinistre est important, des photos peuvent ne pas suffire, il faudra procéder à un constat par un commissaire de police et faire mettre toutes les preuves sous scellés.

Résolution de l'incident

Sans être exhaustifs, les quelques points ci-dessous nécessitent une attention particulière.

Appels aux supports externes

L'entreprise ou l'organisme peut avoir besoin en urgence de compétences externes qui interviendront à distance ou sur site et qu'il faut réserver en priorité en raison des délais d'intervention.

Éradication

L'éradication du problème dépend du type d'incident rencontré.
On peut noter deux grandes tendances entre lesquelles il faudra choisir :

- Le mode « réparation », souvent manuel,
- Le mode « restauration ou réinstallation » en repartant d'une sauvegarde.

Les critères de choix entre ces deux méthodes sont :

- Le temps total (estimation) pour éradiquer l'incident,
- Le niveau de certitude d'avoir bien identifié tous les impacts précis liés à l'incident,
- Le niveau de perte de données acceptable.

Dans les cas complexes, il peut être important d'écrire le plan d'action correctif pour bien ordonnancer les étapes.

Détermination du point zéro de l'incident

Les éléments permettant de déterminer le point zéro sont (entre autres) :

- Le recueil des preuves et journaux,
- Le témoignage des utilisateurs,
- Tous les outils de supervision et reporting.

Cette compréhension de l'origine de l'incident permet de vérifier la pertinence des mesures correctives et de réduire le risque de reproduction.

Délai de Réapprovisionnement de matériel

Même si l'organisme utilise le matériel de secours, il n'est pas recommandé de « rouler trop longtemps sans roue de secours ». C'est pourquoi le réapprovisionnement du matériel est également une priorité.

Retour à la normale

Le retour à la normale doit être associé à une communication spécifique tant en interne qu'en externe.

Méthodes et outils

Du début à la fin de l'incident, les outils indispensables sont :

- Outil d'enregistrement des évènements (centralisation des logs des serveurs AD et Fichiers avec une rétention de 6 mois) ainsi que les moyens d'accès associés (téléphone, messagerie, etc.),
- Outil de supervision.

D'autres outils peuvent être utiles ou nécessaires :

- Outils de diagnostic,
- Outils de confinement :
  - VLAN de confinement,

  - Blocage au niveau de l'annuaire d'entreprise ou des comptes locaux des équipements,
  - Blocage ou filtrage sur tout équipement de sécurité (pare-feu, switch, relais SMTP, etc.),
  - etc.,
- Outils de réparation :
  - Antivirus / kit de décontamination antiviral (exemple : clé USB bootable) contenant des anti-malwares et outils systèmes basées de préférence sur un OS différent de celui qui est installé et pouvant prendre en charge de façon fiable le système de fichier à examiner (exemple : LINUX pour examiner NTFS).
  - Outils de déploiement de patchs systèmes et/ou d'applications,
  - Outils de restauration d'images systèmes, de données ou d'environnement virtuel,
  - etc.

Enfin, l'accès aux moyens de communication téléphoniques et informatiques et à Internet est indispensable pour communiquer ou s'informer.

En cas d'incident empêchant l'accès à ces outils, les équipes d'intervention doivent bénéficier de dispositifs alternatifs.

5.4.6 Revues post-incident

Investigation post-incident

Une fois l'incident maîtrisé, il est possible qu'il soit nécessaire de lancer des investigations complémentaires pour bien comprendre comment cet incident a pu avoir lieu. Si tel est le cas, il ne faut pas hésiter à consacrer le temps nécessaire à cette étape qui viendra enrichir le dossier de synthèse.

Si des éléments de preuve sont encore présents et que l'incident a vocation à être présenté devant un tribunal, la collecte des indices devra être particulièrement précise et se conformer aux bonnes pratiques techniques en adéquation avec les obligations légales.

Ce travail de recherche est fait par des ingénieurs qui ont des compétences spécifiques dans ce domaine dont l'investigation sera un des points du dossier de restitution demandé.

Rapport de synthèse

Chaque incident de sécurité doit être accompagné d'un dossier de suivi et si possible d'un rapport de synthèse. Ce rapport doit être rédigé par l'équipe en charge de la résolution de l'incident. Il peut servir de cadre directeur lors d'une revue post-incident.

Le rapport de synthèse doit pouvoir répondre aux questions suivantes :

- Éléments techniques :
  - Quel est l'objet de l'incident ?
  - Quand a eu lieu l'incident ?
  - Où a-t-il eu lieu ?
  - Comment l'incident s'est-il produit ?
  - Comment l'incident a-t-il été maîtrisé ?
- Bilan processus :
  - Qu'est-ce qui n'a pas fonctionné ?
  - Qu'est-ce qui a bien fonctionné ?
  - La communication aux parties concernées a-t-elle été bien faite ?
- Bilan financier :
  - Quel est le coût de l'incident en matière de perturbation du SI (impact métier) ?
  - Quel est le coût induit de l'incident en matière d'incapacité de travailler pour le personnel ?
  - Quel est le coût de l'incident en matière de temps de résolution passé par les différentes équipes ?
  - Quel est le coût de la contre-mesure mise en place ?
  - Quelles pertes ont pu être économisées grâce à l'équipe de réponse à incident ?

Le rapport de synthèse doit être rédigé au plus près de la date de résolution de l'incident afin d'éviter que le temps n'efface dans la mémoire des acteurs des éléments ou des détails importants pour la compréhension et l'analyse de l'incident.

Le rapport doit prioritairement présenter des conclusions claires compréhensibles par les responsables.

Ce rapport doit être conservé dans un espace dédié servant de base de connaissance aux incidents de sécurité. Cette base d'information pourra par la suite être mise à profit pour une meilleure anticipation des incidents, pour définir les contremesures les plus appropriées ou encore pour vérifier si les décisions actées ont été suivies d'effets.

Analyse post-incident

L'analyse post-incident s'inscrit dans une démarche d'amélioration continue et de qualité permettant de prendre connaissance des éléments qui doivent évoluer dans le Système d'Information.

Cette analyse post-incident doit impliquer les responsables pour que les engagements soient pris rapidement en matière d'évolution du Système d'Information. Celle-ci peut prendre la forme d'un comité de pilotage ou tout autre type de réunion impliquant les décideurs adéquats.

Un compte-rendu de l'analyse post-incident doit être rédigé pour acter des évolutions du Système d'Information.

5.4.7 Actions post-incident

Bilan de l'incident

Les informations et les mesures déterminées lors du traitement de l'incident doivent être conservées et permettre d'enrichir la base de connaissances.

Dans le traitement d'un incident majeur, il est important d'analyser avec recul, ce qui a bien fonctionné et ce qui a moins bien fonctionné.

Cela doit se traduire par la rédaction d'un bilan adressé aux directions concernées.

La mise en place des mesures du bilan, de préférence sous forme de plan d'actions précis, devra être suivie par le responsable sécurité.

Le Recours

Dans le cas d'une attaque, la responsabilité de l'auteur de celle-ci est d'abord d'ordre pénal.

La loi française réprime certains actes commis ou tentés, notamment :

- L'accès illégal à un système,
- La modification ou la suppression illicite de données,
- L'entrave au fonctionnement d'un système,
- L'association de malfaiteurs informatiques (en tant qu'élément aggravant).

La France dispose d'une législation précise sur le sujet (Articles 323-1 à 323-7 du Code pénal relatifs au piratage informatique) et les pirates sont passibles de sanctions parfois conséquentes. C'est pourquoi, il ne faut pas hésiter à l'utiliser en cas d'attaque, que l'attaquant réussisse ou non à la mener à bien. Il existe également un Parquet spécialisé (à Nanterre) compétent en ces matières.

Il faudra alors réunir les éléments suivants :

- Les faits énoncés clairement, de manière chronologique, en incluant tout détail utile,
- Une liste, la plus complète possible, de tous les préjudices subis (dommages, préjudice financier, perte de temps pour vérification de l'intégrité du site ou des données, perte de crédibilité auprès des internautes ou des locataires, etc.),
- Les éléments de preuve constitués lors de l'analyse de l'incident (pour que ces éléments aient une valeur juridique leur collecte et leur conservation doivent obéir à des règles très strictes).

Dans un second temps, il faut identifier auprès de qui porter plainte, en gardant en tête que c'est généralement le lieu des faits qui est l'élément déterminant.

5.5 Gestion des sauvegardes et continuité d'activité

La sauvegarde des données au sein de VSH se fait par le biais du logiciel VEEAM Backup. Ce logiciel est actuellement une référence dans le milieu pour la sauvegarde de machines virtuelles. En plus de ce logiciel la fonction « versions précédentes » est activée sur les serveurs pour plus de facilité et d'autonomie des utilisateurs.

Enfin pour la sauvegarde de l'AS400 un autre système de sauvegarde est mis en place.

L'ensemble est détaillé dans le plan de sauvegarde qui se trouve en annexe 2.

5.5.1 Politique de sauvegarde

La politique de sauvegarde des serveurs virtuel est la suivante :

- Les versions précédentes permettent un snapshot des données 2 fois par jour : à 10h, et à 16h.
- Une première partie des serveurs (critiques) est sauvegardée avec une sauvegarde complète tous les samedis et une incrémentielle du lundi au vendredi.
- La deuxième partie des serveurs est sauvegardée avec une sauvegarde complète tous les 4 samedis et une incrémentielle du lundi au samedi.
- Une sauvegarde complète mensuelle est faite chaque mois avec 4 mois de rétention.
- Une sauvegarde complète immuable est faite chaque mois.
- Une sauvegarde complète immuable en ligne dans un Bucket S3 est faite chaque mois.
- Une copie de notre infra est faite chaque jour sur un serveur de PRA dans une agence.

La politique de sauvegarde de l'AS400 est la suivante :

- Une sauvegarde complète est faite 2 fois par semaine les mardis et vendredis soir sur une bande. Cette bande est changée tous les lundis et mercredis matin avec un roulement de 4 jeux de bande.
- Une box WOOXO est utilisé pour une sauvegarde incrémentielle des données tous les jours. Deux box WOOXO sont présentes, une dans la salle serveur principale et une deuxième dans la salle de secours de l'agence de Clamart.

5.5.2 Localisation

Les sauvegardes incrémentielles et complètes du logiciel VEEAM sont stockées sur un NAS qui est situé dans la salle serveur.

Les sauvegardes immuables sont stockées sur un serveur dédié qui se trouve dans le pavillon informatique. Ce pavillon n'est pas attenant au locaux de Vallée Sud Habitat.

Le serveur de PRA se trouve dans l'agence de Clamart à 3.5km du siège et avec un dénivelé de 61m supérieur.

La sauvegarde sur bande de l'AS400 du mercredi est transportée par le technicien informatique dans l'agence de Clamart afin de déporter ce jeu de sauvegarde. Cette bande est stockée dans la salle serveur de l'agence.

5.5.3 Chiffrement

Les sauvegardes dites immuable sont des sauvegardes cryptées.

Un jeu existe dans le pavillon informatique et un jeu se trouve dans le cloud, stocké par la société Leviia (société de cloud française).

5.5.4 Test de restauration

Des tests de restauration de données sont effectués chaque année pendant la période estivale.

Un test de restauration de fichier et un test de restauration de VM est fait.

5.6 Plan de Reprise d'Activité (PRA)

Un PRA est un plan qu'on exécute dans le cas d'un incident critique du système d'information. Ce plan a pour but de restaurer les services critiques de Vallée Sud Habitat dans les meilleurs délais.

Pour ce faire un serveur est installé dans l'agence de Clamart et reçoit quotidiennement une réplique du système principal.

Exemple de mise en place du PRA

Premièrement il convient d'identifier l'état du serveur IBM AS400 qui n'a pas de serveur de réplication pour la reprise d'activité.

Cas n°1 : il est en état de fonctionner alors il sera déplacé dans la salle serveur de secours de l'agence de Clamart.

Cas n°2 : il est inutilisable, il faut contacter ACG Synergie (éditeur de l'ERP Aravis) afin qu'il nous amène l'AS400 de secours prévu dans le contrat.

Liste des actions à mener pour mettre en place le PRA :

- Eteindre ou couper du réseau tous les serveurs du système d'information principal.
- Mettre en route toutes les VM du serveur de PRA
- Faire un test de connexion interne pour s'assurer du bon fonctionnement des VM.
- Relier la fibre IELO au port WAN1 du pare-feu dédié au PRA et relier le serveur de PRA au port Lan 1 ce pare-feu.
- Faire un test de connexion externe via VPN.

A ce stade les utilisateurs peuvent travailler en mode dégradé en VPN, avec la même qualité de travail que le télétravail. Ils n'auront pas encore accès à l'ERP « Aravis », logiciel développé par « ACG Synergie » auquel nous sommes adhérents.

Une fois que ACG Synergie sera présent (sous 3 jours) ils pourront réinstaller le serveur AS400 à partir de la sauvegarde sur bande pour le système et le paramétrage et de la box WOOXO de l'agence de Clamart pour les données les plus à jour de la base de données. L'ERP sera opérationnel à partir de ce moment-là.

Dans le cas n°1 le temps d'inactivité est estimé à 8h ouvrées. Les données du système d'information reviendront à leur état J-1 avant l'incident de sécurité.

Dans le cas n°2 le temps d'inactivité dépend de la réactivité d'ACG Synergie. Une partie des fonctions du système d'information sera opérationnel comme décrite dans le cas n°1 sous 8h ouvrées, en revanche l'ERP ne sera opérationnel qu'après une estimation raisonnable de 4 jours.

Les utilisateurs devront travailler à travers le VPN jusqu'à ce que le système d'information principal soit de nouveau entièrement opérationnel.

5.7 Sécurité physique

Les salles serveurs du siège et de l'agence de Clamart ne sont pas situées en zone inondable, à risques sismiques ou industriels.

Salle serveur principale :

La salle serveur principale se situe au premier étage du siège. Cette pièce dédiée est climatisée par 2 systèmes de climatisation indépendants. Aucune conduite d'eau ne passe au-dessus de cette pièce. Elle est constamment fermée à clef, la clef se trouve dans une boite à clefs dans le pavillon informatique, elle-même fermée à clef. La clé de la boite à clef est cachée. Une clé supplémentaire de la salle serveur est confiée au DSI. Le bâtiment du siège est protégé par une alarme anti-intrusion.

Salle serveur secondaire dans l'agence de Clamart :

La salle serveur secondaire se situe au sous-sol de l'agence. Cette pièce dédiée est climatisée et constamment fermée à clef. Un jeu de clé se trouve dans la boite à clefs du pavillon informatique et un double se trouve dans le bureau du responsable de la Régie au premier étage de l'agence de Clamart. Le bâtiment est aussi protégé par une alarme anti-intrusion.

Baie de brassage dans l'agence de Chatillon :

La baie de brassage de l'agence de Chatillon se trouve d'une pièce à l'étage, fermée à clef. La clé est en possession de la responsable d'agence. Un double est conservé dans la boite à clef du pavillon informatique.

5.8 Sensibilisation à la sécurité

Les utilisateurs de Vallée Sud Habitat sont régulièrement sensibilisés à la sécurité sur plusieurs aspect : mails, phishing, mot de passe, …

Phishing : Grâce au partenariat fait avec la société « Avant de cliquer » les utilisateurs suivent une formation initiale sous forme de e-learning, rendue obligatoire par la direction, pour les sensibiliser au phishing, puis reçoivent des faux mails de phishing régulièrement tout au long de l'année. Cette campagne annuelle permet de voir l'évolution de l'attention des utilisateurs au contenu des mails qu'ils reçoivent. Dans l'optique de leur donner de l'autonomie ils peuvent alerter depuis leur boite mail s'ils pensent recevoir du phishing.

Mails : Vallée Sud Habitat protège ses boites mails avec la solution de « Mail In Black ». Cette solution permet aux utilisateurs de se rendre compte des typologies de mails qu'ils reçoivent grâce au tri intelligent fait par la solution.

Mot de passe : Vallée Sud Habitat est passé au calcul des forces de mot de passe par entropie comme recommandé par l'ANSSI. Pour se faire le logiciel « Specops » donne à tous les utilisateurs la possibilité de créer des mot de passe classique mais aussi des « Pass phrase ». Chaque utilisateur voit la force de son mot de passe en direct en le tapant et avec le système de récompense mis en place le mot de passe choisi par l'utilisateur à une durée de vie en fonction de sa complexité.

6 ANNEXES

6.1 Annexe 1 : Cartographie des risques

En Annexe 1, la cartographie des risques rédigée conjointement par la responsable du contrôle interne et le DSI regroupe l'ensemble des risques, leur probabilité et leur impact.
Cette cartographie se trouve dans le fichier Cartographie des risques informatiques.xlsm

6.2 Annexe 2 : plan de sauvegarde

Tableau des Jobs de sauvegarde du système d'information

JOB	TYPE	SERVEURS	INCREMENTIEL	FULL	RETENTIONS (jours)	EMPLACEMENT
BKP-CL01	VMware Backup	**SRV-AD-01** (172.24.4.200) **SRV-ARAFIC** (172.24.4.200) **SRV-ARAGRC** (172.24.4.200) **SRV-ARAPRT01** (172.24.4.200) **SRV-AWZZ** (172.24.4.200) **SRV-FTP01** (172.24.4.200) **SRV-GLPI** (172.24.4.200) **SRV-RADIUS01** (172.24.4.200) **SRVAWSVC01** (172.24.4.200) **SRVAWSVCZZ01** (172.24.4.200) **SRV-DHCP** (172.24.4.200) **SRVINFOCENTRE** (172.24.4.200) **SRV-SUPERVISION** (172.24.4.200)	Lundi @ 01:30AM Mardi @ 01:30AM Mercredi @ 01:30AM Jeudi @ 01:30AM Vendredi @ 01:30AM	Samedi @ 01:30AM	14	NAS-SYNO-01
BKP-CL01-LEVIIA	VMware Backup	**SRV-AD-01** (172.24.4.200) **SRV-ARAFIC** (172.24.4.200) **SRV-ARAGRC** (172.24.4.200) **SRV-ARAPRT01** (172.24.4.200) **SRVAWSVC01** (172.24.4.200) **SRVAWSVCZZ01** (172.24.4.200) **SRV-AWZZ** (172.24.4.200) **SRV-DHCP** (172.24.4.200) **SRV-FTP01** (172.24.4.200) **SRV-GLPI** (172.24.4.200) **SRVHARRY** (172.24.4.200) **SRV-RADIUS01** (172.24.4.200) **SRV-RDS-01** (172.24.4.200) **SRV-RDS-03** (172.24.4.200) **SRV-RDS-04** (172.24.4.200) **SRV-SUPERVISION** (172.24.4.200) **SRV-VEEAM-01** (172.24.4.200)		Dimanche @ 01:00AM	30	Leviia S3
BKP-CL02	VMware Backup	**SRV-AD-02** (172.24.4.210) **SRV-ADCONNECT** (172.24.4.210) **SRVARAGED01** (172.24.4.210) **SRVARALAD** (172.24.4.210) **SRV-ARAMOT01** (172.24.4.210) **SRVARAPRT** (172.24.4.210) **SRVARASYSTENCI** (172.24.4.210) **SRV-AWAPACHE** (172.24.4.210) **SRV-AWLIFERAY** (172.24.4.210) **SRV-AWMYSQL** (172.24.4.210) **SRV-AWWILDFLY** (172.24.4.210) **SRV-BDD-SQL** (172.24.4.210) **SRV-IMPRESSION01** (172.24.4.210) **SRV-NEOVACOM** (172.24.4.210) **SRV-SPECOPS01** (172.24.4.210) **SRV-SQL** (172.24.4.210) **SRV-AC** (172.24.4.210) **SRV-HARRY** (172.24.4.210) **SRV-INFOCENTRE** (172.24.4.210)	Lundi @ 01:30AM Mardi @ 01:30AM Mercredi @ 01:30AM Jeudi @ 01:30AM Vendredi @ 01:30AM Samedi @ 01:30AM	Samedi @ 01:30AM	14	NAS-SYNO-01

BKP-CL02-LEVIIA	VMware Backup	**FR-CLU01-VC** (172.24.4.210) **SRV-AC** (172.24.4.210) **SRV-AD-02** (172.24.4.210) **SRV-ADCONNECT** (172.24.4.210) **SRVARAGED01** (172.24.4.210) **SRVARALAD** (172.24.4.210) **SRV-ARAMOT01** (172.24.4.210) **SRVARASYSTENCI** (172.24.4.210) **SRV-AWAPACHE** (172.24.4.210) **SRV-AWLIFERAY** (172.24.4.210) **SRV-AWMYSQL** (172.24.4.210) **SRV-AWWILDFLY** (172.24.4.210) **SRV-HARRY** (172.24.4.210) **SRV-IMPRESSION01** (172.24.4.210) **SRV-INFOCENTRE** (172.24.4.210) **SRV-NEOVACOM** (172.24.4.210) **SRV-RDS-02** (172.24.4.210) **SRV-RDS-BROKER** (172.24.4.210) **SRV-RDS-SALVIA** (172.24.4.210) **SRV-SPECOPS01** (172.24.4.210) **SRV-SQL** (172.24.4.210)		A la fin du Job : BKP-CL01-LEVIIA (Dimanche @ 01:00AM)	30	Leviia S3
BKP-IMMU-CL01	VMware Backup	**SRV-AD-01** (172.24.4.200) **SRV-ARAFIC** (172.24.4.200) **SRV-ARAGRC** (172.24.4.200) **SRV-ARAPRT01** (172.24.4.200) **SRVAWSVC01** (172.24.4.200) **SRVAWSVCZZ01** (172.24.4.200) **SRV-AWZZ** (172.24.4.200) **SRV-DHCP** (172.24.4.200) **SRV-FTP01** (172.24.4.200) **SRV-GLPI** (172.24.4.200) **SRVHARRY** (172.24.4.200) **SRVINFOCENTRE** (172.24.4.200) **SRV-PROXYBKP01** (172.24.4.200) **SRV-PROXYBKP02** (172.24.4.200) **SRV-PROXYBKP03** (172.24.4.200) **SRV-RADIUS01** (172.24.4.200) **SRV-RDS-01** (172.24.4.200) **SRV-RDS-03** (172.24.4.200) **SRV-RDS-04** (172.24.4.200) **SRV-SUPERVISION** (172.24.4.200) **SRV-VEEAM-01** (172.24.4.200)		Samedi @ 08:00AM	14	HARDENED REPOSITORY

BKP-IMMU-CL02	VMware Backup	**SRV-AC** (172.24.4.210) **SRV-AD-02** (172.24.4.210) **SRV-ADCONNECT** (172.24.4.210) **SRVARAGED01** (172.24.4.210) **SRVARALAD** (172.24.4.210) **SRV-ARAMOT01** (172.24.4.210) **SRVARAPRT** (172.24.4.210) **SRVARASYSTENCI** (172.24.4.210) **SRV-AWAPACHE** (172.24.4.210) **SRV-AWLIFERAY** (172.24.4.210) **SRV-AWMYSQL** (172.24.4.210) **SRV-AWWILDFLY** (172.24.4.210) **SRV-BDD-SQL** (172.24.4.210) **SRV-FICHIER** (172.24.4.210) **SRV-HARRY** (172.24.4.210) **SRV-IMPRESSION01** (172.24.4.210) **SRV-INFOCENTRE** (172.24.4.210) **SRV-NEOVACOM** (172.24.4.210) **SRV-RDS-02** (172.24.4.210) **SRV-RDS-BROKER** (172.24.4.210) **SRV-RDS-SALVIA** (172.24.4.210) **SRV-SPECOPS01** (172.24.4.210) **SRV-SQL** (172.24.4.210)		Samedi @ 10:00AM	14	HARDENED REPOSITORY
BKP-RDS	VMware Backup	**SRV-RDS-01** (172.24.4.200) **SRV-RDS-03** (172.24.4.200) **SRV-RDS-04** (172.24.4.200) **SRV-RDS-02** (172.24.4.210) **SRV-RDS-BROKER** (172.24.4.210) **SRV-RDS-SALVIA** (172.24.4.210)	Lundi @ 23:00 Mardi @ 23:00 Mercredi @ 23:00 Jeudi @ 23:00 Vendredi @ 23:00	Samedi @ 23:00	7	NAS-SYNO-01
BKP-SRV-FICHIER	VMware Backup	**SRV-FICHIER** (172.24.4.210)	Lundi @ 00:30 Mardi @ 00:30 Mercredi @ 00:30 Jeudi @ 00:30 Vendredi @ 00:30	Samedi @ 00:30	14	NAS-SYNO-01
BKP-SRV-FICHIER-LEVIIA	VMware Backup	**SRV-FICHIER** (172.24.4.210)		A la fin du Job : BKP-CL02-LEVIIA	15	Leviia S3
BKP-VEEAM	VMware Backup	**SRV-PROXYBKP01** (172.24.4.200) **SRV-PROXYBKP02** (172.24.4.200) **SRV-PROXYBKP03** (172.24.4.200) **SRV-VEEAM-01** (172.24.4.200)	Dimanche @ 15:00	Samedi @ 15:00	7	NAS-SYNO-01