FORCALQUIER•LURE
COMMUNAUTÉ DE COMMUNES

EXTRAIT DU REGISTRE DES DELIBERATIONS DU CONSEIL COMMUNAUTAIRE DU 14 AVRIL 2026

Délibération n°2026-14

Accusé de réception en préfecture
004-240400440-20260414-14-2026-DE
Date de réception préfecture : 16/04/2026

Thème : AFFAIRES GENERALES 10
Objet : Approbation des avis de la conférence d'entente du Système Commun d'Archives Numériques (SCAN)

L'an deux mille vingt-six le quatorze du mois d'avril, le Conseil communautaire dûment convoqué par Monsieur le Président le 08 avril 2026 s'est réuni à l'Hôtel de Ville de Forcalquier sous la présidence de Monsieur David GEHANT.

Membres en exercice : 28 Membres présents : 25 Pouvoirs : 2 Suffrages exprimés : 27

Étaient présents :

Guy JAUFFRED ; David GEHANT ; Gérard VASSEUR ; Brigitte PLAIDY ; Noëlla LEDUC ; Thierry LABUSSIERE ; Emmanuel LUTHRINGER ; Karima COEURET ; Elodie OLIVER ; Marjorie HUBEAU ; Thomas CHERBAKOW ; Jean-Michel GRES ; Lorraine PRUNET ; Robert USSEGLIO ; Céline MOSTEIRO ; Dominique JAUBERT ; Camille FELLER ; Christophe LOPEZ ; Maryse BLANC ; Mathieu RICHARD ; Nadine CURNIER ; Christian CHIAPELLA ; Patricia PAUL ; François BERGNA ; Christine SANTUCCI.

Étaient représentés :
M. Didier MOREL donne procuration à M. David GEHANT
M. Stéphane DERRIVES donne procuration à Mme Maryse BLANC

Absents excusés :
Didier MOREL, Stéphane DERRIVES, Adrien NIMSGERN

Conformément aux dispositions de l'article L. 2121-15 du code général des collectivités territoriales, il a été procédé à la nomination d'un secrétaire choisi au sein de la présente Assemblée ; Madame Elodie OLIVER a été désignée à la majorité des suffrages pour remplir ces fonctions qu'elle a acceptées.

13 communes sont donc représentées.

VU les articles L.5221-1 et L.5221-2 du code général des collectivités territoriales relatifs à l'établissement d'une entente entre plusieurs établissements de coopération intercommunale,

VU les articles R.212-18-1 et R.212-18-2 du code du patrimoine relatifs aux conditions de mutualisation entre services publics d'archives pour la conservation d'archives numériques,

VU la délibération du conseil communautaire de la communauté de communes du « Pays de Forcalquier - Montagne de Lure » n° 36-2025 du 4 avril 2025,

VU la délibération du conseil communautaire de la communauté d'agglomération « Durance Luberon Verdon Agglomération » n° CC-36-04-25 du 8 avril 2025,

VU la convention d'entente relative à la création d'un système commun d'archives numériques (SCAN) du 30 avril 2025,

CONSIDÉRANT l'avis n°2025-14 émis par la conférence d'entente du 05 décembre 2025 relatif à la validation du niveau de service appliqué au flux d'instruction du droit des sols,

CONSIDÉRANT l'avis n°2025-16 émis par la conférence d'entente du 05 décembre 2025 relatif à la validation de la politique de sécurité des systèmes d'information au sein du système commun des archives numériques (SCAN),

Ceci exposé,
LE CONSEIL COMMUNAUTAIRE, DECIDE :

- D'approuver l'avis n°2025-14 relatif à la validation du niveau de service appliqué au flux instruction du droit des sols,

- D'approuver l'avis n°2025-16 relatif à la validation de la politique de sécurité des systèmes d'information au sein du système commun des archives numériques (SCAN),

- D'autoriser Monsieur le Président ou en cas d'empêchement, un vice-président à effectuer toute démarche consécutive à cette décision et à signer, au nom et pour le compte de la communauté de communes, toute pièce de nature administrative, technique ou financière nécessaire à l'exécution de la présente délibération.

POUR : 27
CONTRE : 0
ABSTENTIONS : 0

AINSI FAIT ET DÉLIBÉRÉ, les jours, mois et an susdits,
POUR EXTRAIT CONFORME

Le Président,
David GEHANT

SCAN
Système commun des
archives numériques

AVIS DE LA CONFÉRENCE D'ENTENTE

N° AV-2025-14

Accusé de réception en préfecture
004-240400440-20260414-14-2026-DE
Date de réception préfecture : 16/04/2026

Le 5 décembre 2025 à 14h00, la conférence d'entente du système commun des archives (SCAN), dûment convoquée par lettres individuelles, en date du 28 novembre 2025, s'est réunie en session Ordinaire sous la présidence de Monsieur Laurent GARCIA, dans la salle de réunion du Complexe Fachleitner à MANOSQUE.

Présents :
Monsieur Laurent GARCIA, Madame Sylvie SAMBAIN.

Absents représentés :
Monsieur Jean-Claude CASTEL donne pouvoir à Monsieur Laurent GARCIA, Madame Sandra FAURE donne pouvoir à Monsieur Laurent GARCIA.

Absents excusés :

Absents :
Monsieur Christian CHIAPELLA, Monsieur Michel DALMASSO.

Secrétaire de séance : Jérôme ROCCHI

Le quorum est atteint.

AV-2025-14 - VALIDATION DU NIVEAU DE SERVICE APPLIQUÉ AU FLUX INSTRUCTION DU DROIT DES SOLS

Vu le code général des collectivités territoriales et le code du patrimoine ;

Vu la norme NF Z42-013 concernant les spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes ;

Vu la norme NF461 relative aux exigences de certification de systèmes d'archivage électroniques ;

Vu le standard d'échange de données pour l'archivage (SEDA) ;

Il est apparu nécessaire pour la conférence d'entente de formaliser le niveau de service appliqué au flux d'instruction du droit des sols dont le système commun des archives numériques a la charge (SCAN).

Il est également apparu indispensable que ce niveau de service soit imposé à toutes les parties prenantes suite à la validation de cet avis par les conseils communautaires concernés qui seront chargés de sa bonne application. Ainsi, le présent niveau de service doit être vu comme un document réglementaire approuvé par les assemblées délibérantes des EPCI, s'imposant à chaque partie, plutôt que comme un document contractuel négocié entre elles.

Le présent avis précise les modalités de mise en place du niveau de service.

1- ÉDITION DU NIVEAU DE SERVICE

Nom : Niveau de service du flux urbanisme

Identifiant unique : Flux_urba

Description : Pas de commentaire

Engagement (ajouté à la liste des engagements du service d'archives dans les attestations si renseigné) : Cf. avis n°2025-14

Espace de stockage sécurisé : ECS-01 ☒
ECS-02 ☒ (pour certificats d'urbanisme d'information CUa uniquement)

2- POLITIQUE D'HORODATAGE

Service d'horodatage pour les messages SEDA : Openssl local

Service d'horodatage pour les pièces jointes : Openssl local

Service d'horodatage pour les conversions de fichier : Openssl local

3- POLITIQUE DE CONVERSION

Activer la conversion des formats de conservation :

- ☐ Document
- ☒ Document PDF
- ☐ Feuille de calcul
- ☐ Présentation
- ☐ Image
- ☐ Audio
- ☐ Vidéo

Activer la conversion des formats de diffusion :

- ☐ Document
- ☒ Document PDF
- ☐ Feuille de calcul
- ☐ Présentation
- ☐ Image
- ☐ Audio
- ☐ Vidéo

Il est demandé à la conférence d'entente de bien vouloir :

- ÉMETTRE un avis suite à cet exposé

CET AVIS EST ADOPTÉ A L'UNANIMITÉ DES MEMBRES PRÉSENTS ET REPRÉSENTÉS.

Fait et délibéré en séance les jours, mois et an susdits.

Le Président de la conférence d'entente,
Laurent GARCIA

Accusé de réception en préfecture
004-240400440-20260414-14-2026-DE
Date de réception préfecture : 16/04/2026

SCAN
Système commun des archives numériques

AVIS DE LA CONFÉRENCE D'ENTENTE

N° AV-2025-16

Accusé de réception en préfecture
004-240400440-20260414-14-2026-DE
Date de réception préfecture : 16/04/2026

Le 5 décembre 2025 à 14h00, la conférence d'entente du système commun des archives (SCAN), dûment convoquée par lettres individuelles, en date du 28 novembre 2025, s'est réunie en session Ordinaire sous la présidence de Monsieur Laurent GARCIA, dans la salle de réunion du Complexe Fachleitner à MANOSQUE.

Présents :
Monsieur Laurent GARCIA, Madame Sylvie SAMBAIN.

Absents représentés :
Monsieur Jean-Claude CASTEL donne pouvoir à Monsieur Laurent GARCIA, Madame Sandra FAURE donne pouvoir à Monsieur Laurent GARCIA.

Absents excusés :

Absents :
Monsieur Christian CHIAPELLA, Monsieur Michel DALMASSO.

Secrétaire de séance : Jérôme ROCCHI

Le quorum est atteint.

AV-2025-16 - VALIDATION DE LA POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION AU SEIN DU SYSTÈME COMMUN DES ARCHIVES NUMÉRIQUES

Vu le code général des collectivités territoriales et le code du patrimoine ;

Vu la norme NF Z42-013 concernant les spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes ;

Vu la norme NF461 relative aux exigences de certification de systèmes d'archivage électroniques ;

Vu le standard d'échange de données pour l'archivage (SEDA) ;

Il convient pour la conférence d'entente de rendre un avis concernant la politique de sécurité des systèmes d'information présenté en annexe.

Dans ce cadre, il convient de renseigner dans ce document la politique de sécurité déployée au sein du système commun des archives numériques.

Le rapport présente les processus de sécurité des systèmes d'information, leurs modalités techniques et leur mise en œuvre.

Il est demandé à la conférence d'entente de bien vouloir :

- ÉMETTRE un avis suite à cet exposé

CET AVIS EST ADOPTÉ A L'UNANIMITÉ DES MEMBRES PRÉSENTS ET REPRÉSENTÉS.

Fait et délibéré en séance les jours, mois et an susdits.

Le Président de la conférence d'entente,
Laurent GARCIA

2025

PSSI & Chartes Informatiques

Politique de Sécurité du Système d'Information

Table des matières

1. Déclaration de la Direction

Les Systèmes d'Information (S.I) remplissent des fonctions indispensables au fonctionnement optimal de l'entreprise. Leur disponibilité doit être assurée à tout moment et en toutes circonstances.

Certaines informations qu'ils traitent sont particulièrement sensibles, notamment des données concernant les failles de sécurité présentes chez nos clients. Les Systèmes d'Information doivent garantir que ces informations restent authentiques et confidentielles. Leur ouverture vers l'extérieur doit se faire dans un cadre sécurisé et maîtrisé.

Ces mêmes données sont exposées à des menaces et des risques réels, notamment de vol et de négligence, pouvant engager la responsabilité de tous.

Au regard de ces risques, le Groupement DLVAgglo a la responsabilité, vis-à-vis de ses clients, de garantir un niveau de sécurité suffisant pour protéger les données qui lui sont confiées.

Pour relever ce défi, une démarche est menée pour identifier les lacunes, élaborer et mettre en œuvre un plan d'action visant à permettre de maîtriser ces risques.

La Politique de Sécurité des Systèmes d'Information constitue le cadre unique de référence du Groupement pour toutes les questions de Sécurité des Systèmes d'Information.

Chacun doit veiller personnellement à sa bonne mise en application, et faire preuve de vigilance dans son usage des moyens de traitement des informations. Chacun doit donc s'assurer que les règles de Sécurité des Systèmes d'Information applicables à son périmètre sont respectées.

A cette fin, je délègue au Responsable de la Sécurité des Systèmes d'Information (RSSI) la responsabilité de mettre à jour les orientations de la Politique de Sécurité des Systèmes d'Information.

A Manosque, le jj/mm/2024.

Prénom NOM.

Statut.

Signature avec tampon

Signé par le DGS

2. Introduction

2.1. Préambule

Le développement rapide de l'usage des Technologies de l'Information et de la Communication (TIC) dans l'ensemble des secteurs d'activité constitue un enjeu stratégique pour bon nombre d'entreprises. Il s'accompagne toutefois d'un accroissement significatif des risques d'atteinte aux informations conservées sous forme électronique, et plus généralement aux processus s'appuyant sur les Systèmes d'Information (SI).

Conscient de cet état de fait, le Groupement conduit une démarche de Sécurité des Systèmes d'Information (SSI), ceci afin de sécuriser ses SI.

Cette démarche est matérialisée par la mise en œuvre d'une Politique de Sécurité des Systèmes d'Information (PSSI) qui permettra notamment de renforcer la confiance et l'adhésion des salariés, des institutions et plus largement des clients.

des institutions et plus largement des clients.

2.2. Définition

Est dénommé « Groupement » dans la présente charte le groupement des collectivités DLVAgglo , Ville de Manosque, CCAS, Régie de l'eau (EPIC) et Syndicat Mixte Scènes De Haute-Provence (SMSDHP)

2.3. Référentiel

La SSI du Groupement s'appuie sur un référentiel constitué de 3 segments :

- La Politique Générale de Sécurité des Systèmes d'Information (PGSSI) qui :
  - Définit les principes fondamentaux de la SSI ;
  - Définit les principes de gouvernance de la SSI ;
  - Définit les objectifs de SSI.
- Les Méthodes, Stratégies, Processus, Procédures, Chartes, etc. qui :
  - Mettent en œuvre de façon concrète les principes de sécurité.
- Les mesures de sécurité qui :

- Sont la résultante organisationnelle et technique des Méthodes, Stratégies, Processus, Procédures, Chartes, etc.

2.4. Objet

La présente PGSSI du Groupement est un document de référence, validé et approuvé par la direction, qui doit être pris en compte par l'ensemble des acteurs et utilisateurs des SI.

Elle explicite les principaux enjeux, les principes fondamentaux, les principes de gouvernance et les objectifs de SSI pour le Groupement.

Les différentes mesures prévues sont destinées à être mises en œuvre de manière graduelle, afin de permettre une progression de la SSI soutenable par la structure et d'atteindre à terme la cible de sécurisation fixée.

2.5. Champ d'application

La présente PGSSI du Groupement concerne le périmètre global de ses activités. Elle concerne ainsi l'ensemble des sites, personnels et SI concernés par ces activités.

2.6. Cycle de vie

La présente PGSSI du Groupement doit être révisée à minima annuellement consécutivement à la mise à jour des analyses de risques de la société. La PGSSI est mise à jour par le Responsable de la Sécurité des Systèmes d'Information (RSSI) du Groupement et doit être ensuite approuvée lors d'un Comité de Pilotage (COPIL) en charge de la SSI du Groupement.

2.7. Diffusion

La présente PGSSI du Groupement est diffusée à l'ensemble des collaborateurs en version numérique sur Teams. Elle est consultable depuis le dossier l'intranet du Groupement.

Elle est également jointe aux contrats liant le Groupement à ses tiers lorsque nécessaire.

3. Principes fondamentaux de Sécurité des Systèmes d'Information

3.1. Valeurs

La PSSI du Groupement adopte les 4 valeurs suivantes :

- Le respect des contraintes de confidentialité des usagers/collaborateurs ;
- Le respect des contraintes opérationnelles ;
- Le respect des contraintes économiques ;
- Le respect des contraintes réglementaires applicables.

3.2. Proportionnalité

La PSSI du Groupement adopte le principe de proportionnalité qui consiste à :

- Mettre en œuvre les actions strictement nécessaires en regard des objectifs poursuivis ;
- Prioriser les actions présentant le meilleur ratio bénéfices obtenus / ressources investies.

3.3. Subsidiarité

La PSSI du Groupement adopte le principe de subsidiarité qui consiste à :

- Confier la responsabilité d'une action à l'entité compétente la plus proche de la population directement concernée par cette action ;
- Escalader cette responsabilité à l'entité hiérarchiquement supérieure lorsque la compétence de l'entité initialement responsable est ou devient insuffisante, et ainsi de suite.

3.4. Amélioration continue

La PSSI du Groupement adopte le principe d'amélioration continue qui consiste à :

- Assurer un effort constant afin de s'approcher au plus près d'une cible intrinsèquement évolutive et de s'y maintenir ;
- Choisir le franchissement progressif de multiples paliers raisonnables au franchissement brusque d'un unique palier inatteignable.

Pour ce faire, le cycle Plan Do Check Act (PDCA) est utilisé :

3.4.1. Plan (P)

L'étape Plan (Planifier en français) consiste à définir, planifier et attribuer les actions permettant d'atteindre la cible fixée.

3.4.2. Do (D)

L'étape Do (Développer en français) consiste à mettre en œuvre les actions définies, planifiées et attribuées précédemment.

3.4.3. Check (C)

L'étape Check (Contrôler en français) consiste à vérifier l'effectivité et l'efficacité des actions mises en œuvre précédemment.

3.4.4. Act (A)

L'étape Act (Ajuster en français) consiste à améliorer la cible en la corrigeant ou en l'affinant en fonction des conclusions des contrôles précédents.

3.5. Critères

La PSSI du Groupement adopte les 4 critères suivants :

3.5.1. Disponibilité (D)

La disponibilité est, pour une application, le fait d'être accessible par ses utilisateurs lorsque ceux-ci en ont la nécessité. Une perte de disponibilité peut être causée par une panne matérielle, une panne réseau, etc. Le besoin en disponibilité est alors représenté par le délai pendant lequel les utilisateurs peuvent s'en passer. Les responsables ont alors pour tâche de rendre à nouveau accessible l'application avant l'écoulement de ce délai.

3.5.2. Intégrité (I)

L'intégrité est, pour les données d'une application, le fait d'être complètes et exactes. Une perte d'intégrité signifie que les données consultées seront erronées. Ceci peut être causé par de mauvaises manipulations, de la malveillance ou des bugs applicatifs, etc. Le besoin en intégrité est alors représenté par la tolérance des utilisateurs face à ces erreurs. Les responsables ont alors pour tâche de corriger les données dans les plus brefs délais après identification du problème.

3.5.3. Confidentialité (C)

La confidentialité est, pour les données d'une application, le fait d'être accessibles par plus ou moins d'utilisateurs. Une perte de confidentialité signifie que les données ont été consultées par des personnes non habilitées. Ceci peut être causé par des droits trop étendus, des actions illicites, etc. Le besoin en confidentialité est alors représenté par l'étendue des utilisateurs habilités à y accéder. Les responsables ont alors pour tâche de corriger la faille qui a permis aux personnes non habilitées d'accéder aux données.

3.5.4. Traçabilité (T)

La traçabilité est, pour une application, le fait d'être capable de savoir qui a réalisé quelle action et quand. Une perte de traçabilité signifie que des actions critiques réalisées n'ont pas

d'auteur connu. Ceci peut être causé par l'absence de mécanismes de traçabilité, par un effacement illégitime des traces, etc. Le besoin en traçabilité est alors représenté par le détail que l'on souhaite obtenir en matière de traces. Les responsables ont alors pour tâche de mettre en œuvre les mécanismes de traçabilité adéquats.

3.6. Approches

La PSSI du Groupement adopte les 3 approches suivantes :

- L'approche par les risques :
  - L'objectif est ici de maîtriser les risques de SSI existants en les traitant des plus critiques aux moins critiques ;
  - Ceci nécessite donc de formaliser et tenir à jour une analyse de risques de SSI permettant de piloter les actions de traitement associées.
- L'approche par les projets :
  - L'objectif est ici de ne pas détériorer le niveau de SSI existant avec de nouveaux projets porteurs de risques non maîtrisés ;
  - Ceci nécessite donc de mettre en œuvre une gestion de projets permettant d'assurer la SSI.
- L'approche par la réglementation :
  - L'objectif est ici de se mettre en conformité avec l'ensemble des réglementations de SSI applicables ;
  - Ceci nécessite donc d'intégrer les exigences réglementaires comme une priorité dans le plan d'actions SSI.

3.6.1. Approche par les projets

La PSSI du Groupement intègre la sécurité dans les projets de la façon suivante :

3.6.1.1. Méthode de gestion de projets

L'intégration de la SSI dans les projets nécessite qu'une méthode de gestion de projets soit adoptée officiellement, de façon globale et transverse à l'ensemble du Groupement. La méthode choisie est celle du cycle en V.

3.6.1.2. Cycle de vie des projets

L'intégration de la SSI dans les projets doit se faire au plus tôt et tout au long du cycle de vie des projets :

- En amont des projets, afin de pouvoir exprimer les besoins en Sécurité des Systèmes d'Information ;
- Lors de la conception des solutions projets, afin de pouvoir définir les mesures de Sécurité des Systèmes d'Information adressant au mieux les besoins en Sécurité des Systèmes d'Information ;

- Lors de la mise en œuvre des solutions projets, afin de pouvoir attester de la bonne intégration des mesures de Sécurité des Systèmes d'Information définies ;
- Lors des tests des solutions projets, afin de pouvoir valider le fonctionnement et les performances des mesures de Sécurité des Systèmes d'Information ;
- Lors de la mise en production, afin de pouvoir clore le projet sur ses aspects Sécurité des Systèmes d'Information ;
- Lors de la décommissions de systèmes, afin de préserver les informations et s'assurer de la réversibilité.

Ces différentes étapes de Sécurité des Systèmes d'Information devront être adaptées afin de s'inscrire naturellement dans la méthode de gestion de projets adoptée par le Groupement.

3.6.1.3. Documentation

La documentation de Sécurité des Systèmes d'Information devant être produite pour chaque projet est :

- L'expression des besoins en Sécurité des Systèmes d'Information ;
- La liste des mesures de Sécurité des Systèmes d'Information à mettre en œuvre ;
- La liste des mesures de Sécurité des Systèmes d'Information mises en œuvre ;
- Le cahier de tests Sécurité des Systèmes d'Information ;
- Le Procès-Verbal (PV) Sécurité des Systèmes d'Information.

D'autres documents spécifiques Sécurité des Systèmes d'Information pourront être exigés selon les contextes, comme une annexe des clauses Sécurité des Systèmes d'Information à intégrer à un éventuel contrat tiers.

3.6.1.4. Cotation de sécurité

L'intégration de la Sécurité des Systèmes d'Information dans les projets s'articule autour d'une cotation Sécurité des Systèmes d'Information des critères de Disponibilité, d'Intégrité, de Confidentialité et de Traçabilité selon les échelles suivantes.

La cotation Sécurité des Systèmes d'Information des biens essentiels pourra être revue au fil du temps selon les évolutions du contexte.

3.6.1.5. Jalons d'arbitrage

L'intégration de la Sécurité des Systèmes d'Information dans les projets nécessite que des jalons d'arbitrage soient définis au sein de chaque projet :

- Un jalon d'arbitrage doit ainsi être défini à chacune des étapes de Sécurité des Systèmes d'Information définies ci-dessus ;
- Chaque jalon d'arbitrage doit autant que possible être planifié afin de pouvoir concorder avec la planification d'une instance d'arbitrage.

Ces jalons d'arbitrage seront sous la responsabilité des chefs de projets.

3.6.1.6. Instance d'arbitrage

L'intégration de la Sécurité des Systèmes d'Information dans les projets nécessitera une instance d'arbitrage capable de prononcer :

- La conformité d'un projet dans sa prise en compte de la Sécurité des Systèmes d'Information : Le projet peut alors suivre son cours ;
- La conformité partielle d'un projet dans sa prise en compte de la Sécurité des Systèmes d'Information, ceci ne le mettant pas en danger : Le projet peut alors suivre son cours mais se trouve également dans l'obligation de corriger ses manques ;
- La non-conformité d'un projet dans sa prise en compte de la Sécurité des Systèmes d'Information, ceci le mettant en danger : Le projet ne peut alors plus suivre son cours et doit se remettre complètement en conformité avant de pouvoir éventuellement se poursuivre.

Cette instance d'arbitrage se réunira à minima semestriellement afin de pouvoir piloter l'avancement des projets dans le temps.

3.6.2. Approche par la réglementation

La PSSI du Groupement est en lien avec les textes réglementaires applicables suivants :

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données) (GDPR) ;
- Code pénal ;
- Code civil ;
- Code des postes et des communications électroniques ;
- Code de la propriété intellectuelle ;
- Code du patrimoine ;
- Code du travail ;
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux liberté (CNIL) ;
- Loi n° 2004-575 du 21 juin 2004 pour la Confiance dans l'Économie Numérique (LCEN) ;
- Loi n° 2006-961 du 1 août 2006 relative au Droit d'Auteur et aux Droits Voisins dans la Société de l'Information (DADVSI) ;
- Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (HADOPI) ;
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles ;
- Instruction Interministérielle (II) 901/SGDSN/ANSSI : relative à la protection des systèmes d'informations sensibles ;
- Référentiel Général de Sécurité (RGS) ;

- NIS2 ;

De nombreuses réglementations sectorielles viennent s’ajouter à cette liste, au cas par cas, selon les missions adressées pour les clients.

3.6.3. Approche Ecoresponsable

Dans le cadre de notre engagement en faveur du développement durable et conformément à la loi du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique (loi REEN), nous adoptons les mesures suivantes pour minimiser l'impact écologique de nos activités numériques.

Remarques : Ces engagements de sobriété participent également à la sécurisation en limitant les sources de données et donc les fuites et pertes possibles.

- Limitation des impressions papier

Nous encourageons l'utilisation de documents électroniques et limitons les impressions papier au strict nécessaire. Lorsqu'une impression est indispensable, il est recommandé d'utiliser le mode recto-verso et de privilégier le noir et blanc afin de réduire la consommation de papier et d'encre.

- Extinction des systèmes informatiques

Les utilisateurs sont tenus d'éteindre les équipements informatiques (ordinateurs, imprimantes, etc.) en fin de journée et lors des périodes d'inutilisation prolongées. Cette pratique vise à diminuer la consommation énergétique inutile et à prolonger la durée de vie des appareils.

- Gestion des équipements obsolètes

Nous nous engageons à lutter contre l'obsolescence des équipements en favorisant leur maintenance, leur mise à jour régulière et, lorsque cela est possible, leur réutilisation. Avant de procéder au remplacement d'un appareil, une évaluation de sa nécessité est effectuée afin de limiter le gaspillage de ressources.

- Recyclage des Déchets d'Équipements Électriques et Électroniques (DEEE)

Conformément à la réglementation en vigueur, notamment la loi REEN, nous assurons le recyclage des DEEE en collaborant avec des filières agréées. Les équipements en fin de vie sont collectés, triés et traités afin de récupérer les matériaux valorisables et de disposer des substances dangereuses de manière sécurisée.

- Décommissionnement des applications et serveurs obsolètes

Nous procédons régulièrement à l'arrêt des applications obsolètes et à la désactivation des serveurs inutiles ou d'archives, afin de réduire la consommation énergétique et d'optimiser les ressources informatiques.

- Nettoyage des données obsolètes

Conformément à la réglementation en vigueur, nous mettons en place une politique de suppression des données obsolètes afin de limiter la saturation des systèmes de sauvegarde et d'optimiser leur performance.

Le temps de conservation des données doit être conforme aux obligations légales mais pas les dépasser.

- Optimisation de la structuration des données

Afin d'éviter les doublons et de rationaliser le stockage, nous optimisons la structuration des données en adoptant des pratiques de gestion efficaces et en favorisant une classification rigoureuse des informations.

- Optimisation de la taille des données

L'utilisation d'image de haute définition produit des volumes de données très importants.

Il est de la responsabilité de chacun d'utiliser des formats de fichiers raisonnables adaptés au besoin de qualité. Il est conseillé de diminuer par défaut le niveau de définition des images (photos et vidéos).

- Utilisation responsable des moteurs de recherche

Nous sensibilisons les utilisateurs à l'utilisation rationnelle des moteurs de recherche, tant sur internet que sur les réseaux locaux, afin de limiter l'empreinte carbone des requêtes en ligne. Chaque recherche sur internet engendrant une consommation d'énergie, nous encourageons une utilisation raisonnée et l'emploi de moteurs de recherche écoresponsables (Qwant.com, Ecosia.org…)

- Blocage des publicités en ligne

L'utilisation de bloqueurs de publicités est encouragée afin de limiter le chargement d'éléments inutiles sur les pages web, ce qui contribue à réduire la consommation de bande passante et l'empreinte énergétique de la navigation internet.

Ces actions s'inscrivent dans notre démarche de responsabilité sociétale des entreprises (RSE) et visent à réduire l'empreinte environnementale de nos activités numériques.

4. Principes de gouvernance de Sécurité des Systèmes d'Information

4.1. Responsable de la Sécurité des Systèmes d'Information (RSSI)

La Politique de Sécurité des Systèmes d'Information du Groupement nécessite un Responsable de la Sécurité des Systèmes d'Information afin d'être pilotée dans sa globalité.

4.1.1. Rattachement

Le Responsable de la Sécurité des Systèmes d'Information du Groupement est rattaché au Directeur Général (DG) du Groupement et lui rend compte.

Le Responsable de la Sécurité des Systèmes d'Information du Groupement est positionné comme Maîtrise d'Ouvrage (MOA) Sécurité des Systèmes d'Information.

Le Responsable de la Sécurité des Systèmes d'Information du Groupement s'appuie sur le Responsable des Systèmes d'Information (RSI) du Groupement pour la Maîtrise d'Œuvre (MOE) Sécurité des Systèmes d'Information.

4.1.2. Contexte d'intervention

La fonction de Responsable de la Sécurité des Systèmes d'Information du Groupement est assurée à hauteur de 2 jours par mois.

Le présentiel du Responsable de la Sécurité des Systèmes d'Information du Groupement est assuré au siège du Groupement.

4.1.3. Description des missions et des activités

Les missions du Responsable de la Sécurité des Systèmes d'Information du Groupement sont :

- Définition et mise en œuvre de la Politique de Sécurité des Systèmes d'Information :
  - Définit les objectifs et les besoins liés à la Sécurité des Systèmes d'Information du Groupement, en collaboration avec les acteurs concernés (direction générale, direction des systèmes d'information, direction des ressources humaines, direction qualité, etc.) ;
  - Rédige la Politique de Sécurité des Systèmes d'Information et les procédures de sécurité associées en collaboration avec les acteurs concernés (cf. ci-dessus) ;
  - Met en œuvre la Politique de Sécurité des Systèmes d'Information au sein du Groupement, en assure les évolutions et les mises à jour ;
  - Met en place une organisation permettant d'assurer, dans la durée, la gouvernance du Systèmes d'Information du Groupement.
- Diagnostic et analyse des risques de la Sécurité des Systèmes d'Information :
  - Évalue les risques sur la sécurité des systèmes d'information.
- Choix des mesures de sécurité et plan de mise en œuvre :

- Étudie les moyens permettant d'assurer la Sécurité des Systèmes d'Information et leurs bonnes utilisations par les acteurs du Groupement ;
- Propose à la direction du Groupement, pour arbitrage, une liste de mesures de sécurité à mettre en œuvre, assure dans la durée, le suivi et l'évolution de ce plan d'action ;
- Assure la maîtrise d'ouvrage de la mise en œuvre des mesures de sécurité (cette mission, selon le type de mesure technique ou organisationnelle, peut être éventuellement partagée avec un responsable métier ou le responsable du système d'information).

- Sensibilisation, formation et conseil sur les enjeux de la Sécurité des Systèmes d'Information :
  - Informe régulièrement et sensibilise les directions du Groupement sur les enjeux et les risques de la SSI ;
  - Conduit des actions de sensibilisation et de formation auprès des utilisateurs sur les enjeux de la SSI ;
  - Participe à la réalisation de la charte de Sécurité des Systèmes d'Information du Groupement et en assure la promotion auprès de l'ensemble des utilisateurs.
- Audit et contrôle de l'application des règles de la Politique de Sécurité des Systèmes d'Information :
  - Conduit régulièrement des audits de Sécurité des Systèmes d'Information afin de vérifier la bonne application de la Politique de Sécurité des Systèmes d'Information par les acteurs du Groupement ;
  - Surveille et gère les incidents de sécurité survenus au sein du Groupement ;
  - Vérifie l'intégration de la Sécurité des Systèmes d'Information dans l'ensemble des projets du Groupement.
- Veille technologique et prospective :
  - Suit les évolutions réglementaires et techniques afin de garantir l'adéquation de la Politique de Sécurité des Systèmes d'Information avec ces évolutions.

4.1.4. Profil et compétences requises

Le Responsable de la Sécurité des Systèmes d'Information du Groupement doit avoir pour compétences :

- Niveau de formation et d'expérience :
  - Formation de niveau licence (ou master 2) avec une spécialisation complémentaire en Sécurité des Systèmes d'Information ;
  - Cadre technique ayant une expérience avérée dans la conduite de projets.
- Compétences techniques :
  - Connaissance des concepts techniques des applications informatiques du secteur, des réseaux informatiques et des mécanismes de sécurité ;

- Connaissance des standards de sécurité ISO 2700x ;
- Expérience dans le pilotage de projets organisationnels ;
- Connaissance juridique sur la Sécurité des Systèmes d'Information.

- Compétences personnelles :
  - Capacité à piloter et gérer des projets ;
  - Capacité à organiser et conduire le changement ;
  - Capacité à gérer des situations de crise ;
  - Capacité à animer des groupes de travail, sessions de sensibilisation et formation ;
  - Bon relationnel et esprit de synthèse.

4.1.5. Moyens mis à disposition

Le Responsable de la Sécurité des Systèmes d'Information du Groupement dispose des moyens suivants :

- Un bureau, personnel ou partagé ;
- Un poste de travail avec un bureau, une chaise, un ordinateur portable, un téléphone mobile, un courriel ;
- Un accès physique aux infrastructures du Groupement ;
- Un accès logique aux Systèmes d'Information du Groupement.

Le Responsable de la Sécurité des Systèmes d'Information est joignable à l'adresse suivante :

- rssi@dlva.fr

Il n'existe ni Ressources Humaines (RH), ni ressources financières allouées spécifiquement à la Sécurité des Systèmes d'Information du Groupement. Ces ressources devront être affectées par la Direction Générale du Groupement selon les possibilités.

4.2. Délégué à la Protection des Données (DPD)

Le Règlement Général sur la Protection des Données nécessite un Délégué à la Protection des Données afin de piloter la mise en conformité du Groupement.

4.2.1. Rattachement

Le Délégué à la Protection des Données du Groupement est rattaché au Directeur Général (DG) du Groupement et lui rend compte.

Le Délégué à la Protection des Données du Groupement est positionné comme Maîtrise d'Ouvrage (MOA) Protection des Données à Caractère Personnel.

Le Délégué à la Protection des Données du Groupement s'appuie sur le Directeur des Systèmes d'Information (RSI) du Groupement pour la Maîtrise d'Œuvre (MOE) Protection des Données à Caractère Personnel.

4.2.2. Contexte d'intervention

La fonction de Délégué à la Protection des Données du Groupement est assurée à hauteur de 0,5 jour par mois.

Le présentiel du Délégué à la Protection des Données du Groupement est assuré au siège du Groupement.

4.2.3. Description des missions et des activités

Les missions du Délégué à la Protection des Données du Groupement sont :

- Information, conseils et diffusion d'une culture de la protection des données au sein du Groupement :
  - Mener ou piloter des actions visant à sensibiliser la direction, les salariés (dont le personnel participant aux opérations de traitement) aux règles à respecter en matière de protection des données à caractère personnel ;
  - Faire en sorte de présenter les efforts de mise en conformité réalisés par les salariés de manière positive, pour valoriser le travail accompli et encourager à le poursuivre ;
  - S'assurer que les personnes concernées sont informées des traitements opérés impliquant leurs données personnelles, ainsi que de leurs droits ;
  - Informer sans délai le responsable de traitement de tout risque encouru en cas de non-respect de ses recommandations et de l'impact que ferait courir un risque à la direction du Groupement ;
  - Formaliser une procédure pour informer directement le responsable de traitement d'une non-conformité majeure ;
  - Rendre compte chaque année de son action en présentant un rapport annuel au responsable de traitement qui est le respect fidèle de son action au cours de l'année écoulée et qui fait état des éventuelles difficultés rencontrées.
- Audit et contrôle du respect du règlement et du droit national en matière de protection des données :
  - Mener, faire mener ou piloter, de façon maîtrisée et indépendante, toute action permettant de juger du degré de conformité du Groupement ;
  - Mettre en évidence les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.) ;
  - Vérifier le respect du cadre légal ou la bonne application de procédures, méthodes ou consignes relatives à la protection des données personnelles ;
  - Porter conseil auprès des métiers concernés et, si besoin, auprès du responsable de traitement, ainsi qu'auprès des prestataires et sous-traitants prenant part aux traitements décidés par le responsable de traitement ;
  - Recevoir et traiter des réclamations de personnes concernées par les traitements pour lesquels il a été désigné et veille au strict respect du droit des personnes ;

- Traiter les réclamations et les plaintes avec impartialité, ou mettre en œuvre les procédures propres à assurer leurs bons traitements.

- Coopération avec l'autorité de contrôle :
  - Constituer le point de contact privilégié de l'autorité de contrôle (la CNIL) ;
  - Etablir et maintenir une documentation relative aux traitements de données à caractère personnel notamment au moyen d'un registre des traitements ;
  - Faciliter l'accès par l'autorité aux documents et informations dans le cadre de l'exercice des missions et des pouvoirs de cette autorité ;
  - Solliciter le conseil de l'autorité de contrôle si nécessaire.

Le Délégué à la Protection des Données pourra exécuter d'autres missions et tâches. Dans ce cas, le responsable du traitement veille à ce que ces missions et tâches n'entraînent pas de conflit d'intérêt avec notamment des tâches et/ou missions portées par le Responsable de la Sécurité des Systèmes d'Information.

4.2.4. Profil et compétences requises

Le Délégué à la Protection des Données du Groupement doit avoir pour compétences :

- Niveau de formation et d'expérience :
  - Formation de niveau licence (ou master 2) avec une spécialisation complémentaire en protection des données ;
  - Expérience souhaitée sur les enjeux liés à la protection des données personnelles dans les domaines suivants :
    - Management et protection des données personnelles ;
    - Juriste digital ;
    - Programme Data Protection Management ;
    - Diplôme Universitaire en protection des données ;
    - Certificat de spécialisation Délégué à la protection des données ;
    - Droit en numérique ;
    - Ingénieur en cyberdéfense.
- Compétences techniques :
  - Connaissance des concepts techniques des applications informatiques du secteur, des réseaux informatiques et des mécanismes de sécurité ;
  - Connaissance du droit et des législations des données informatiques ;
  - Pratique en matière de protection des données ;
  - Connaissance en gestion du risque et en conformité d'un traitement à caractère personnel ;
  - Connaissances générales sur l'audibilité du système d'information et sur les métiers et les processus du secteur.
- Compétences personnelles :

- Capacité à piloter et gérer des projets ;
- Sens de l'analyse, esprit de synthèse, rigueur et méthode ;
- Sens de la communication :
  - Établir aisément avec ses interlocuteurs une relation propice aux échanges et à la communication ;
  - Faire preuve de diplomatie, savoir être pondéré et nuancé tout en faisant appliquer la réglementation.
- Faire preuve d'objectivité, d'impartialité, d'indépendance, de capacité de prise de décision et de réactivité ;
- Sens de la discrétion et de la confidentialité : le Délégué à la Protection des Données est tenu au secret professionnel.

4.2.5. Moyens mis à disposition

Le Délégué à la Protection des Données du Groupement dispose des moyens suivants :

- Un bureau, personnel ou partagé ;
- Un poste de travail avec un bureau, une chaise, un ordinateur portable, un téléphone mobile, un courriel ;
- Un accès physique à le Groupement ;
- Un accès logique aux Systèmes d'Information du Groupement.

Le Délégué à la Protection des Données est joignable à l'adresse suivante :

- dpo-rgpd@dlva.fr pour DLVAgglo
- mdelvallee@ville-manosque.fr pour Ville de Manosque
- dpo-regieeau@dlva.fr pour la Régie des Eaux

5. Objectifs de Sécurité des Systèmes d'Information

Les objectifs de SSI du Groupement sont référencés ci-dessous en se basant sur la classification du guide d'hygiène de l'ANSSI.

5.1. Politiques de sécurité de l'information

5.1.1. Orientations de la direction en matière de sécurité de l'information

La Direction du Groupement attend de chaque collaborateur une participation active dans le processus de sécurisation continue des actifs du groupement.

Des efforts permanents de sensibilisation et de formation sont déployés pour garantir une culture de la sécurité au sein de l'entreprise.

La société base ses principes de sécurité sur les préconisations de l'ANSSI, de la CNIL et du référentiel NIS2.

5.2. Organisation de la sécurité de l'information

5.2.1. Organisation interne et alerte

La sécurité des SI est l'affaire de tous.

Les collaborateurs doivent rapporter immédiatement tout manquement, comportement ou incident pouvant porter atteinte à la sécurité des données de l'entreprise.

Le RSSI est la personne à privilégier pour ces déclarations, à défaut le RSI ou la direction.

En fonction du cas, un incident de sécurité pourra être formalisé et permettra d'engager les moyens nécessaires à sa résolution, incluant notamment les actions du DPO et la relation aux autorités.

5.2.2. Pilotage de la Sécurité des Systèmes d'Information (COPIL SSI)

Les activités de sécurité de l'information sont sous l'autorité du **DGA du Pôle Ressources** en coordination avec le RSI, le RSSI et le DPO.

Les sujets de sécurité sont abordés couramment selon les dispositions suivantes ;

5.2.2.1. Réunions opérationnelles hebdomadaires

Les réunions opérationnelles permettent de coordonner les équipes techniques et de déclencher, le cas échéant, tout processus de gestion d'incident ou dispositif de sécurité.

- Point équipe interne hebdomadaire équipe opérationnelle SI
  Le point équipe traite des besoins opérationnels courants, de l'avancée des projets et des problématiques de sécurité de la période.
- Point de coordination gouvernance entre le RSI et le DGA
  Le point de coordination avec la gouvernance permet d'échanger régulièrement sur toute difficulté ou sujets portant sur la sécurité des informations.

5.2.2.2. Comités Exceptionnels

En complément du traitement courant, des outils d'observation du niveau de sécurité sont établis pour reporter régulièrement à la gouvernance du groupement par l'intermédiaire du DGA et partagé lors des comités du groupement.

La DSI maintient notamment un Cyber Score partagé avec le DGS et les recommandations et améliorations associées à prévoir.

5.2.2.3. Cellule de Crise

En cas d'incident de sécurité, ou d'escalade, une cellule de crise peut être convoquée pour organiser et coordonner les actions préventives et curatives.

5.3. La sécurité des ressources humaines

5.3.1. Avant l'embauche

Avant une embauche, les références des futurs collaborateurs sont vérifiées :

- Par des entretiens RH et techniques préalables,
- Par un contrôle des qualifications (CV, Certifications, diplômes…),
- Par le contrôle du casier judiciaire,
- Par la prise de références extérieures.

5.3.2. Prise de poste

A l'entrée du collaborateur dans ses fonctions, il est accompagné ;

- Par les RH qui crée son identité numérique (matricule) dans le SI RH,
- Par son Responsable de service qui demande ses accès et habilitations via un formulaire d'habilitation dédié et lui présente les outils spécifiques au métier,
- Par l'équipe SSI qui lui délivre son matériel, le sensibilise à l'usage du SI et l'oriente vers une base d'information de référence (Wiki Interne).

5.3.3. Pendant la durée du contrat

Pendant la durée de leurs contrats, les collaborateurs sont suivis, notamment vis-à-vis :

- Du maintien et de l'augmentation de leurs compétences,
- De leur assiduité,
- De leurs qualités relationnelles,
- Du respect des politiques internes, notamment SSI,
- De l'évolution de ses habilitations (cf formulaire dédié),
- Du respect de l'usage des outils.

5.3.4. Rupture, terme ou modification du contrat de travail

En cas de modification des conditions d'exécution des fonctions d'un collaborateur, ses habilitations sont systématiquement revues en conséquence.

Les moyens informatiques mis à disposition sont étendus ou retirés. Le collaborateur doit rendre tout équipement ou moyen dont il n'a plus l'usage.

La récupération des moyens informatiques pour restitution au service SSI est de la responsabilité du Responsable de service.

5.4. Gestion des actifs

5.4.1. Responsabilités relatives aux actifs

L'équipe SSI du groupement est responsable des :

- Moyens de raccordement réseau/opérateur,
- Moyens bureautiques et outils office,
- Moyens Wifi propres aux bâtiments administratifs et zones publiques permanentes,
- Systèmes centraux (serveurs applicatifs et métiers),
- Des sauvegardes,
- Systèmes Cloud à disposition des collaborateurs et des usagers,

Elle n'est pas responsable :

- Des équipements tiers dépendant de ses moyens de raccordement (ex : Panneaux d'affichage public, plots de sécurité, Portail de sécurité groupe scolaire, GTB/GTC…),
- Des équipements déployés ponctuellement dans l'espace public,
- De tout équipement non approvisionné par l'équipe SSI.

Cependant, les règles de sécurité de l'équipe SSI Le Groupement s'appliquent à l'ensemble de l'écosystème.

Elle a autorité pour interdire tout usage réputé dangereux pour ses systèmes.

Elle est garante de l'application des obligations de sécurité réglementaire et du maintien des critères de sécurité.

Les connexions aux réseaux et systèmes sont surveillées. En cas de suspicion, le Groupement se réserve le droit de bloquer les connexions de tout équipement suspect ou inconnu.

Les équipements sont protégés par différents dispositifs, notamment des mécanismes d'authentification, de contrôle des réseaux, des mises à jour automatisées, un antispam et une application de protection et de sécurisation.

5.4.2. Classification de l'information

Chaque collaborateur du Groupement détermine la valeur et la sensibilité des informations dont il est responsable et identifie les risques associés, notamment les risques de conformité (dont les conformités légales ou GDPR). Il peut consulter le RSSI et le DPO pour l'aider dans sa réflexion.

5.5. Appareils mobiles et télétravail

Le Groupement fournit à ses collaborateurs les ressources sécurisées nécessaires au télétravail. Les collaborateurs doivent utiliser le PC portable, leur compte professionnel et le protocole de connexion adapté fourni par l'entreprise pour télétravailler.

Toutes les données de l'entreprise doivent être stockées sur les espaces sous contrôle du Groupement. Le stockage en dehors des zones synchronisées avec les services cloud en contrat avec le Groupement et les lecteurs réseaux partagés sont à proscrire.

Les collaborateurs du Groupement ont l'autorisation d'utiliser leur smartphone personnel pour utiliser leur boîte mail professionnelle selon la procédure d'approbation contrôlée par l'équipe informatique.

Toute externalisation de données (sauvegarde personnelle, envoi vers système externe, données sur PC personnel…) est interdite, à l'exception des systèmes prévus à cet effet hébergés en propre par les clients et uniquement dans le cadre de missions en cours.

5.5.1. Manipulation des supports amovibles

Chaque collaborateur du Groupement à la responsabilité des supports de données qu'il manipule.

Il doit s'assurer de leur mise en sûreté et de leur nettoyage permanent.

Tout besoin de destruction physique doit être adressé au DSI.

Les supports amovibles non fournis par l'équipe IT ne sont pas sous sa responsabilité, aucune maintenance ou support n'y est associé.

5.6. Contrôle d'accès aux systèmes

La Direction Informatique du Groupement veille à appliquer la règle du moindre privilège, qui consiste à attribuer à une personne uniquement les habilitations nécessaires à son activité.

Les habilitations et moyens informatiques des collaborateurs sont demandés et revus régulièrement par leur responsable de service et adaptés en conséquence, ils sont nominatifs.

Toute modification des droits accordés à un utilisateur est soumise à validation signée de son responsable.

La politique d'authentification impose des mots de passe de minimum 12 caractères.

La DSI met en place de l'authentification forte au cas par cas pour protéger les accès les plus critiques et selon les profils utilisateurs.

Pour la gestion de leurs comptes applicatifs, internes ou en lien avec leurs missions, les collaborateurs sont incités à utiliser un outil de coffre-fort numérique stocké sur un espace sauvegardé.

5.7. Cryptographie

5.7.1. Mesures cryptographiques

Les supports de données des Serveurs du Groupement sont chiffrés.

Toute transmission de données en dehors des mails (intra application et/ou intersites) est chiffrée, notamment entre client et serveur.

Les connexions à des outils web et plateforme cloud sont systématiquement chiffrées (ssl/tls/https).

5.8. Sécurité physique et environnementale

5.8.1. Zones d'accès restreints

Le Groupement met en œuvre des moyens de protection pour empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation.

Les locaux techniques informatiques du Groupement sont sous alarme et sous clef.

Les codes d'accès sont revus à minima annuellement et en fonction des incidents de sécurité ou des mouvements de personnel.

Les locaux techniques sont sécurisés et leur accès est strictement restreint et contrôlé.

Seuls les personnels autorisés ont le droit d'accéder aux locaux et espaces administratifs et techniques du Groupement.

Tout visiteur d'une zone à accès restreint doit avoir une raison légitime de se présenter et être accompagné par un hôte responsable.

5.8.2. Matériels

Les PC portables des collaborateurs le Groupement sont fournis avec des filtres de confidentialité sur demande.

Le matériel fourni par le Groupement ne doit jamais être laissé sans surveillance. Toute disparition, vol ou destruction doit être immédiatement signalé au DSI.

En cas de perte ou de vol de PC, le Groupement a les moyens de bloquer les accès aux ressources de l'entreprise.

En cas de perte ou de vol de Smartphone, le Groupement a les moyens de bloquer les accès aux ressources de l'entreprise, de localiser l'équipement ou de communiquer avec le détenteur.

5.9. Sécurité liée à l'exploitation

5.9.1. Procédures et responsabilités liées à l'exploitation

L'exploitation des Systèmes du Groupement est sous contrôle de la DSI. Celle-ci s'assure de la qualité de l'exploitation en s'imposant des procédures de traitement documentées.

Les services en plateforme Cloud (Saas) sont sous la responsabilité d'exploitation du détenteur du service, Le Groupement s'assure du respect des termes contractuels.

Tout changement majeur est co-validé par le DSI, le RSSI et le DPO pour s'assurer du respect des réglementations et de l'état de l'art.

La résilience des systèmes est cadrée par des procédures d'exploitation spécifiques assurant la qualité.

Un COPIL SI/SSI est tenu régulièrement pour tracer les modifications et échanger avec la direction.

5.9.2. Protection contre les logiciels malveillants

Les PC et serveurs de l'entreprise sont protégés par un Antivirus.

Le système de messagerie est protégé par un Antispam.

5.9.3. Sauvegarde

La société le Groupement est dotée d'un système de sauvegarde garantissant la récupération de ses données.

Le système de sauvegarde couvre les actifs centraux et les serveurs, mais ne s'étend pas au contenu local des PCs.

Le stockage sur les PC, en dehors des zones partagées sur le réseau est à proscrire.

Il est interdit d'avoir ses propres sauvegardes en dehors d'un support ou d'un système sous contrôle direct de l'entreprise.

5.9.4. Journalisation et surveillance

La DSI du Groupement possède des moyens de supervision et de journalisation des systèmes.

Ils permettent de s'assurer de la bonne santé des systèmes, de leur mise à jour régulière, de leur intégrité et de suivre les mouvements de données.

Les équipes chargées de l'administration procèdent à une routine de vérification quotidienne.

5.9.5. Maîtrise des logiciels en exploitation

Seuls les logiciels autorisés par la DSI sont autorisés.

Les PC sont configurés pour empêcher l'installation d'application sans validation de la DSI.

Toute demande spécifique doit lui être soumise et fera l'objet d'une étude d'impact SSI.

La DSI est garante du respect des systèmes de licences et des obligations contractuelles des outils sous son contrôle.

5.10. Sécurité des communications

5.10.1. Transfert de l'information

La transmission des informations entre les collaborateurs du Groupement est réalisée à travers les répertoires réseaux sur le serveur de fichiers ou à travers applications Saas ou espace de stockage cloud soumis à gestion de droits contrôlées par la DSI

Les collaborateurs peuvent utiliser leur messagerie du groupement si elle est appropriée, notamment pour les échanges extérieurs.

Le moyen de transfert privilégié avec l'extérieur est l'ouverture ponctuelle d'un espace collaboratif Google Workspace, dont les accès doivent être vérifiés par le collaborateur.

5.10.2. Accès Distants

Le Groupement utilise une messagerie et espace cloud comme système principal accessible depuis une connexion internet.

Pour se connecter au réseau interne, les collaborateurs doivent passer par une liaison VPN.

Les prestataires agissant sur les systèmes doivent passer par un portail applicatif dédié dont l'accès et l'usage est validé par la DSI.

5.11. Acquisition, développement et maintenance des systèmes d'information

Les systèmes du Groupement sont sous contrôle total de la DSI.

Tout équipement utilisé pour accéder à ses réseaux est soumis à validation et contrôle interne.

Tout développement, acquisition ou suppression d'un système est soumis à étude budgétaire et de sécurité.

Tout projet interne engageant des ressources informatiques ou traitant d'information de l'entreprise est soumis à un processus d'accompagnement à la sécurité (Security by design).

5.12. Relations avec les prestataires et fournisseurs

Le Groupement s'assure de la gestion de la sécurité des Systèmes d'Information avec ses fournisseurs et partenaires, incluant les services d'hébergement dans le Cloud. Pour ce faire, la société le Groupement :

- Vérifie les conditions de sécurité et les certifications ;
- Applique les besoins de sécurité appropriés, en les formalisant dans les documents contractuels ;
- Ajoute si nécessaire des clauses de confidentialité et de protection des données personnelles dans les contrats des prestataires ;
- S'assure du niveau de sécurité de ses prestataires, notamment en réclamant ses certifications en vigueur, en vérifiant ses références et les CV des intervenants ;
- S'assure de l'effectivité des paramètres techniques de sécurité ;
- Vérifie les clauses spécifiques obligatoires liées au RGPD avec l'aide de ses confrères DPO (Ville et Agglo) ;
- La DSI vérifie ponctuellement le fonctionnement des outils déployés dans d'autres contextes (partenaires ou structures équivalentes).

5.13. Gestion des incidents liés à la sécurité de l'information

Les incidents de sécurité sont à rapporter immédiatement au RSSI et au DSI, directement ou à défaut via le support informatique.

Les incidents portant sur des atteintes à des données personnelles sont à soumettre directement au DPO via son mail de contact (dpo-rgpd@dlva.fr).

Ces incidents sont soumis à analyse par le RSSI ainsi que le DPO et donneront lieu le cas échéant à des mesures organisationnelles et techniques pour améliorer les usages et la sécurité des systèmes.

Le Groupement est doté de moyens permettant d'analyser techniquement les incidents de sécurité au sein de ses systèmes (supervision, EDR, logs…). Ces données techniques pourront être collectées et sauvegardées en vue d'investigations futures.

La DSI peut faire appel à ses prestataires spécialisés (Antivirus, Antispam, Opérateur) pour l'aider à gérer ces incidents de sécurité.

5.14. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

La DSI met en œuvre des moyens de redondances de connexion opérateur pour gérer les cas de dégradation d'accès à la donnée.

Les systèmes centraux (serveurs, distribution réseau) possèdent des mécanismes de résilience et sont segmentés.

En mesure exceptionnelle, La Direction est seule responsable du renvoi des collaborateurs à leur domicile en cas de problème majeur pour envisager un travail en mode dégradé (accès à Google Workspace).

5.15. Conformité

5.15.1. Conformité aux obligations légales et réglementaires

Le Groupement est conforme aux attentes de la CNIL et de l'ANSSI quant à la gestion de ses données.

5.15.2. Revue de la sécurité de l'information

La DSI suit les sujets de sécurité de façon hebdomadaire à l'occasion de réunion d'équipe sur la base de tableaux de bord dédiés.

Les projets numériques nécessitant un accompagnement de sécurité sont traités comme des activités courantes.

La sécurité est l'affaire de tous et sous la responsabilité du RSSI qui en assure le suivi.

5.16. Intelligence Artificielle

On ne dit pas « j'utilise l'Intelligence Artificielle », mais plutôt de Système d'Intelligence Artificielle (SIA). L'utilisation d'outils reposant sur un SIA est tolérée.

Dans le cadre du respect de la présente Politique, les Utilisateurs sont tenus de respecter les règles énoncées dans la Charte Informatique.

Lorsqu'ils utilisent de tels outils, les utilisateurs s'engagent à s'assurer de la pertinence des résultats obtenus, à respecter la confidentialité des données ainsi que les grands principes de la protection des données à caractère personnel.

En ce sens, les utilisateurs ne doivent en aucun cas utiliser des données métier confidentielles et des données à caractère personnel pour générer du contenu.

Les utilisateurs ne doivent en aucun cas installer des extensions sur leurs terminaux lorsque l'utilisation d'un tel outil le requiert.

Les utilisateurs ayant des besoins non couverts par les logiciels ou applications mis à leur disposition sont invités à contacter le service informatique et le DPD ou le référent IA afin de formuler ce besoin, qui sera ensuite qualifié pour décision et action.

6. Annexes

6.1. Annexe 1 : Classification

Pour toute information manipulée par le Groupement, quels qu'en soient le support ou la forme, la présente classification en 4 niveaux s'applique :

6.1.1. Publique

Les informations de classification « Publique » sont des informations non sensibles et publiques.

Ces informations sont libres d'accès en interne ou en externe le Groupement.

6.1.2. Interne

Les informations de classification « Interne » sont des informations non sensibles mais non publiques.

Ces informations sont libres d'accès en interne, et peuvent être diffusées en externe le Groupement, à toute personne en ayant le besoin dans le cadre de ses relations avec le Groupement, dans les conditions minimales de sécurité.

6.1.3. Limitée

Les informations de classification « Limitée » sont des informations sensibles dont la divulgation est de nature à compromettre de façon significative le déroulement normal d'un projet, causer un préjudice significatif pour le Groupement ou pour l'un de ses clients.

Ces informations ne sont communicables qu'aux personnes ayant le besoin d'en connaître dans le cadre de leurs activités, dans les conditions suffisantes de sécurité.

6.1.4. Confidentielle

Les informations de classification « Confidentielle » sont des informations extrêmement sensibles dont la divulgation est de nature à compromettre de façon critique le déroulement normal d'un projet, causer un préjudice massif pour le Groupement ou pour l'un de ses clients.

Ces informations ne sont communicables qu'aux personnes formellement autorisées, dans les conditions optimales de sécurité.

6.2. Annexe 2 : glossaire

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CNIL	Commission Nationale de l'Informatique et des Libertés
COPIL	Comité de Pilotage
COPIL SSI	Comité de Pilotage de la Sécurité des Systèmes d'Information
DG	Direction Générale / Directeur Général
DICT	Disponibilité Intégrité Confidentialité Traçabilité
DPD	Délégué à la Protection des Données
DSI	Direction des Systèmes d'Information / Directeur des Systèmes d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EBIOS RM	EBIOS Risk Manager – Version actualisée en vigueur de la méthode EBIOS
EDR	Endpoint Detection Response
GTB/GTC	Gestion Technique des Bâtiments / Gestion Technique Centralisée
HADOPI	Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet
II	Instruction Interministérielle
ISO	International Organization for Standardization
LCEN	Loi pour la Confiance dans l'Economie Numérique
MOA	Maîtrise d'Ouvrage
MOE	Maîtrise d'Œuvre
NIS2	Network and Information Security. Directive (UE) 2022/2555
PASSI	Prestataires d'Audit de la Sécurité des Systèmes d'Information
PDCA	Plan Do Check Act
PGSSI	Politique Générale de Sécurité des Systèmes d'Information
PSSI	Politique de Sécurité des Systèmes d'Information
PV	Procès-Verbal
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
RH	Ressources Humaines
RSSI	Responsable de la Sécurité des Systèmes d'Information
RT	Responsable de Traitement
SSI	Sécurité des Systèmes d'Information
ST	Sous-Traitant
TIC	Technologies de l'Information et de la Communication