



PROCEDURE INTERNE / INTERNAL PROCEDURE

Politique de Sécurité des Systèmes d'Information

Gestion documentaire

Projet : S5
Objet : IT documentation
Classification : Restricted
Version : C
Date : Avril 2025

Auteurs : S. LAVERDURE - DSI

Document version :

Version	Date	Auteur	Commentaire
A	01/02/2023	A.ENNAJI	Version initiale
B	01/07/2024	S. LAVERDURE	Version modifiée
C	01/04/2025	G. LABROUSSE	Mises à jour

Table des matières

Gestion documentaire	1
Table des matières.....	2
1. Périmètre.....	4
2. Définition.....	4
3. Sécurité de l'information dans la gestion des projets (§1.2.3 VDA ISA)	4
4. Gestion des actifs (§1.3 VDA ISA)	5
4.1. Responsabilité des actifs	5
4.1.1. Inventaire d'actifs	5
4.1.2. Propriété des actifs.....	5
4.1.3. Bon usage des actifs	5
4.1.4. Retour d'actifs.....	6
4.2. Classification de l'information (§1.3.2 VDA ISA)	6
4.2.1. Classification de l'information.....	6
4.2.2. Marquage de l'information	6
4.2.3. Manipulation de l'information	6
4.3. Manipulation des supports	6
4.3.1. Manipulation des supports amovibles	7
4.3.2. Mise au rebut des supports	7
5. Gestion des incidents de sécurité (§1.6 VDA ISA).....	7
6. Sécurité des ressources humaines (§2 VDA ISA)	8
6.1. Avant embauche.....	8
6.1.1. Collaborateurs	8
6.1.2. Collaborateurs sensibles	8
6.2. Durant le contrat.....	8
6.3. Violation de contrat.....	9
6.4. Travail à distance / nomade	9
6.5. Sensibilisation des collaborateurs	9
6.5.1. Sensibilisation à l'arrivée des collaborateurs	10
6.5.2. Renouvellement des sensibilisations.....	10
7. Politique de sécurité physique et continuité d'activité (§3 VDA ISA)	10
7.1. Sécurité Physique	10
7.1.1. Zones de sécurité physique.....	10
7.1.2. Accueil des visiteurs	10
7.1.3. Attribution / Révocation des accès.	11
7.2. Plan de Reprise d'Activité (PRA)	11
7.3. Gestion des équipements confiés	11
7.4. Politique d'utilisation des mobiles et outils de télétravail	12
8. Contrôles d'accès (§4 VDA ISA)	12
8.1. Accès utilisateurs au réseaux et services informatiques.....	12
8.2. Gestion des accès utilisateurs et utilisateurs à privilèges	12
8.3. Bon usage des secrets de connexion.....	13
8.4. Politique des mots de passe	13
8.5. Restriction d'accès au réseau.....	13
8.6. Contrôles et revues des comptes et droits d'accès	14
9. Politique d'utilisation des mesures de chiffrements (§5.1 VDA ISA)	14
10. Sécurité des opérations (§5.2 VDA ISA)	14
10.1. Gestion du changement	14
10.2. Protection antivirus	15
10.3. Journaux et journalisation	15
10.4. Gestion des vulnérabilités	15
10.5. Gestion des audits techniques.....	15
10.6. Gestion du réseau	16
11. Acquisition, maintenance et développement (§5.3 VDA ISA)	16
11.1. Exigences de sécurité pour les nouveaux développements	16
11.2. Exigences de sécurité pour les services réseaux	16
11.3. Réversibilité et sécurité de destruction de l'information dans le Cloud	16

11.4. Ségrégation des données de l'organisation dans le cloud	16
12. Sécurité dans les relations fournisseurs (§6 TISAX)	17
12.1. Exigences de sécurité de l'information pour les fournisseurs	17
12.2. Services IT sur cloud externe.....	17
12.2.1. 1.2.4 Partage des responsabilités avec les services IT externes (based on ISO27017)	17
12.2.2. Gestion des services IT externes	17
12.2.3. Retour et suppression sécurisé des actifs informationnels des services IT externes	18
12.2.4. Protection de l'information dans les services IT externes partagés.....	18
13. Conformité (§7 VDA ISA)	18
13.1. Veille légale et réglementaire	18
13.2. Protection des données à caractère personnel.	18
14. Gestion des exceptions	19

1. Périmètre

Le présent document définit les règles de la politique de sécurité du système d'information de la société GMD Eurocast. Il se base sur la politique générale de sécurité de l'information en vigueur au sein de GMD Eurocast.

2. Définition

Acronyme	Définition
SI	Système d'Informations
SMSI	Système de Management de la Sécurité de l'Information
RSMSI	Responsable du Système de Management de la Sécurité de l'Information.
DSI	Directeur des Systèmes d'Information
RSSI	Responsable de la Sécurité du Système d'Information
DPO	Délégué à la Protection des Données
RDD	Revue de Direction
RSI	Responsable Système Informatique
Business platform	Tous les composants du SI qui contribue aux affaires.
PSSI	Politique de Sécurité du Système d'Information
PGSSI	Politique Global de la Sécurité du Système d'Information
COSSI	Comité Opérationnel de Sécurité du Système d'Information
CPSSI	Comité de Pilotage de la Sécurité du Système d'Information
CAB	Change Advisory Board : Comité de gestion des changements
ITSM	Information technologie service management

3. Sécurité de l'information dans la gestion des projets (§1.2.3 VDA ISA)

La sécurité de l'information dans la gestion des projets concerne tous les projets de l'entreprise, notamment les projets :

- Produits ;
- De R&D ;
- Les projets informatiques ;
- Les projets d'entreprises ;

Tous les projets doivent être classifiés en prenant en compte leurs besoins de sécurité, en fonction des risques encourus dans le cadre du projet. Les procédures d'évaluations, et les critères de classification des projets dépendent du type de projet :

- *Pour les projets **Produits** :* Intégré à la classification globale du projet, dans le fichier *E_C1_F1_Pré-analyse_des_risques_projets*, prend en compte les risques de sécurité de l'information et la confidentialité des données du projet. Le RSSI est intégré dans les projets complexes et à risque.
- *Pour les projets **R&D** :* Classification dédiée, sur 4 niveaux, dans le fichier *E_C2_F3_Liste_des_projets_R&D*. Les documents produits dans le cadre de ces projets sont classifiés à hauteur de la confidentialité du projet.
- *Pour les projets **Informatiques** :* La classification est réalisée conformément à la procédure *E_S5_P4_SP1_I1_Procédure_Evaluation_des_besoins_de_sécurité_dans_les_projets_IT..* Le RSSI est intégré dans le process d'analyse de risques des projets très sensibles.

Selon les besoins de sécurité identifiés à la suite du recueil des exigences et à l'analyse de risque projet, des mesures de sécurités sont établies tels que :

- Formation / sensibilisation des équipes
- Isolement physique d'une machine, protection visuelle du produit,
- Droits d'accès restreints au répertoire de projet
- Journalisation des accès dans le cadre du projet
- Anonymisation totale ou partielle des documents
- Signature d'une clause de sécurité spécifique au projet (NDA, ...)

Des fichiers de suivi de l'ensemble des projets permettent leur suivi :

- **Projets R&D** : E_C2_F3_Liste projet R&D 2024
- **Projets Produits / Process** : E_C3_SP1_F7_Tableau_de_bord_projets
- **Projets Informatiques** : E_S5_P4_SP1_F3_Liste_des_projets_IT

→ **Chaque site** doit assurer l'évaluation des risques des projets selon les procédures des différents processus impactés et tenir à jour la liste des projets comprenant la classification des projets.
 → **Chaque site** doit piloter et surveiller le déploiement des mesures de sécurité dans les différents projets.

4. Gestion des actifs (§1.3 VDA ISA)

4.1. Responsabilité des actifs

4.1.1. Inventaire d'actifs

Les actifs informationnels (familles d'informations gérées par GMD Eurocast) sont identifiés dans le fichier d'analyse de risques. Ils sont identifiés afin de définir les besoins de sécurité des données, propre à chaque site. De plus, l'inventaire des actifs informationnels permet de collecter les informations sur le traitement de la donnée (stockage, transfert, accès).

→ **Chaque site** doit tenir à jour l'inventaire de ses actifs informationnels au sein du fichier d'analyse de risques.

Les familles d'actifs supports (site, équipements, logiciels, groupe de personnes) sont identifiés au pôle. Les sites industriels peuvent avoir des actifs supports qui leurs sont propres (exemple : application industrielle, plateforme-client, ...), auquel cas, ces actifs supports doivent également être identifiés. La correspondance entre les actifs supports et actifs informationnels est documenté au sein de l'analyse de risque, centralement au sein de la matrice de correspondance entre actifs informationnels et support, localement au sein de l'inventaire des actifs informationnels.

→ **Chaque site** doit tenir à jour l'inventaire de ses actifs supports au sein du fichier d'analyse de risques.

→ **Chaque site** doit identifier les supports liés au stockage et au transfert des informations dans la colonne « Description » de l'inventaire des actifs informationnels.

L'inventaire détaillé des actifs supports est suivi centralement par le Pôle Reyrieux.

❖ Sont inventoriés dans LanSweeper :

- Le matériel informatique et téléphonie : serveurs, réseaux, postes de travail fixes et portables, PDA, tablettes, supports de stockage, ...
- Applications : logiciels, os, ...
- Infrastructure de support informatique : imprimantes, onduleurs, ...

❖ Les applications externes sont inventoriées dans GLPI.

❖ Les smartphones sont inventoriés sur le site d'Orange Business Services avec le numéro d'IMEI.

4.1.2. Propriété des actifs

Chaque actif inventorié doit être attribué à un propriétaire unique, dont les responsabilités sont décrites dans le document PGSSI.

4.1.3. Bon usage des actifs

Les exigences de sécurité des actifs sont identifiées pour :

- L'identification (voir 4.1.1 du présent document)
- La préparation (voir les procédures de hardening)
- La gestion (voir 4.2.3 du présent document)
- Le transport (voir 4.2.3 du présent document)
- Le stockage (voir 4.2.3 du présent document)
- Le retour et la destruction (voir 4.1.4 du présent document)

4.1.4. Attribution et retour d'actifs

Les règlements relatifs au retour des actifs lors du départ de l'organisation ou de la résiliation du contrat doivent être mis en place. La procédure de *E_S5_I10_arrivée départ* intègre les exigences liées à la remise et à la restitution des actifs.

Remise d'actifs

- À l'embauche d'un collaborateur, un enregistrement est créé dans GLPI. Le formulaire *E_S5_F2_Remise_de_matériel* contenant le détail des équipements qui sont attribués au collaborateur (PC, badge, etc..) est rempli. Le collaborateur atteste la récupération du matériel, et la preuve est conservée dans l'enregistrement GLPI.
- En cas de nouvelle attribution de matériel, un nouvel enregistrement est créé, et le même procédé est respecté.

Restitution d'actifs

- Au départ du collaborateur, un contrôle est assuré entre les équipements restitués et le contenu des enregistrements GLPI liés au collaborateur. Une fiche *E_S5_F16_Restitution_de_matériel* est complétée et enregistrée dans GLPI.
- → **Sur les sites industriels, le CL-SI** doit s'assurer que cette procédure est respectée au départ du collaborateur pour assurer la récupération de tous les actifs confiés.
- En cas de réutilisation de matériel, le PC est remis à l'IT, qui le formate et effectue un effacement bas niveau avant réaffectation du matériel.
- → **Les sites industriels** doivent s'assurer que le matériel soit remis à l'IT avant toute réaffectation et que le matériel en attente de destruction soit stocké en zone « Sensible ».

4.2. Classification de l'information (§1.3.2 VDA ISA)

4.2.1. Classification de l'information

Le schéma de classification des documents et de l'information est formalisé au sein du document *E_M1_I9_Classification_de_l_information_EUROCAST_FR*. Les critères définissent des échelles de confidentialité.

Les règles de gestion associées à chacun des niveaux de confidentialité concernent les activités suivantes :

- Transferts physiques
- Transferts électroniques
- Stockage
- Impression
- Copie
- Destruction

4.2.2. Marquage de l'information

L'ensemble des documents politiques, procédures, modes opératoires et enregistrements (tickets, comptes rendus, emails, etc..) doit disposer d'un marquage clair précisant le niveau de classification des informations traitées.

4.2.3. Manipulation de l'information

La manipulation de l'information est formalisée dans le document *E_M1_I9_Classification_de_l_information_EUROCAST_FR*. De plus, les règles de bon usage des actifs sont également reprises dans la Charte Informatique.

4.3. Manipulation des supports

Les règles de gestion des supports amovibles doivent être rédigées : transport, suppression, destruction, transfert, mesures de protections. Ces règles sont conditionnées au niveau de classification de l'information placée sur ces supports.

4.3.1. Manipulation des supports amovibles

Les règles de gestion des supports amovibles sont établies :

- Interdiction stricte de clés USB personnelles.
- La DSI fournit aux collaborateurs, sur demande validée par le Chef de Site, un support amovible strictement réservée à un usage professionnel.
- Les supports amovibles sont scannés par la solution anti-malware lorsque branchés sur les équipements protégés.

4.3.2. Mise au rebut des supports

Les supports en attente de destruction doivent être identifiés, recensés et conservés dans un local sécurisé. Le matériel est inventorié dans LanSweeper, le matériel en attente de destruction est identifié comme « à détruire » dans LanSweeper.

Le matériel en attente de destruction doit être stocké en zone « Sensible » pour prévenir le vol de matériel contenant de la donnée. La destruction est réalisée par l'IT, par l'endommagement / la destruction du disque dur.

5. Gestion des incidents de sécurité (§1.6 VDA ISA)

La gestion des incidents de sécurité s'appuie sur l'outil GLPI permettant l'enregistrement, le suivi, la clôture, la conservation intègre et la trace des incidents. Les incidents de sécurité peuvent porter sur l'organisation, les processus, les infrastructures et équipements ou le système d'information. Les exemples d'événements et incidents de sécurité sont identifiés dans la procédure de gestion des incidents.

→ La gestion des incidents est réalisée centralement, néanmoins, les collaborateurs des sites industriels doivent remonter au RSSI les incidents de sécurité propre aux sites industriels via GLPI. Les CL-SI doivent inciter les collaborateurs à créer un ticket en cas d'incident ou de suspicion d'incident.

Les exigences liées à la remontée et la gestion des événements de sécurité sont intégrées à la sensibilisation des collaborateurs.

- Le signalement d'un événement, d'une faille ou d'un incident de sécurité est exprimé au travers d'un ticket d'incident type dans l'outil GLPI, par tout collaborateur de l'organisation. Si ce signalement est réalisé par un prestataire ou fournisseur auprès de son interlocuteur dans l'organisation, ce dernier doit alors l'enregistrer dans l'outil GLPI et en préciser la source. Des outils peuvent également remonter des alertes d'événements ou d'incidents de sécurité, qui génèrent également des tickets d'incidents dans GLPI.
- A la création du ticket, l'équipe IT reçoit automatiquement une notification par email. En fonction de l'urgence et/ou de la gravité du constat, le RSSI est tenu d'intervenir en consultation ou intervention.
- Dans le ticket d'incident de sécurité de l'information, l'outil de gestion doit enregistrer :
 - L'évaluation de l'impact et de la sévérité qui sont fixés par le collaborateur créant le ticket,
 - Ces évaluations seront au besoin actualisées par le support IT ou le RSSI,
 - Après analyse et investigation, le ticket d'incident sera attribué par le RSSI à un collaborateur pour traitement.
- L'émetteur du ticket, ou son représentant dans l'organisation, est informé automatiquement de l'avancée du traitement du ticket.

→ **Chaque site** doit s'assurer de la participation des collaborateurs aux programmes de sensibilisations et s'assurer de la remontée des événements de sécurité par les collaborateurs dans GLPI.

Les événements, qualifiés en incident ayant une composante IT sont communiqués auprès du SOC lorsque le RSSI estime nécessaire l'intervention d'Orange Cyberdéfense.

Les preuves associées à l'incident de sécurité (logs, copie d'écran, snapshot d'un équipement, ...) sont conservées par le RSSI dans un espace sécurisé. La référence à ces éléments de preuve peut être mentionnée dans le ticket d'incident.

Une information sur les incidents de sécurité en cours de traitement est réalisée par le RSSI auprès des responsables de service lors des comités de pilotage ou de communications spécifiques. La procédure de gestion des événements et incidents de sécurité est spécifiée dans le document *E_S5_P2_Gestion_des_événements_et_incidents_de_sécurité*. Le bilan et le retour d'expérience associés aux incidents de sécurité sont réalisés après chaque traitement d'incident avec impact.

→ **Les CL-SI** doivent communiquer localement sur événements et incidents de sécurité traités par le site central et sur les leçons apprises suite à l'analyse de ces incidents, selon les communications réalisées par le RSSI.

6. Sécurité des ressources humaines (§2 VDA ISA)

6.1. Avant embauche

6.1.1. Collaborateurs

Le consentement RGPD est systématiquement recueilli lors de la récupération d'information de la part d'un candidat.

Pour toute embauche :

- Une enquête d'e-réputation est effectuée.
- Deux entretiens sont effectués
 - Un entretien en visio-conférence
 - Un entretien physique sur le site de rattachement
- Un contrôle des références est effectué.
- La récolte des documents pré-requis est réalisée, soit en interne, soit par un cabinet de recrutement.
- L'identité est vérifiée : CNI ; Attestation de sécurité sociale ; Justificatif de domicile

Une clause de confidentialité et une obligation de respecter les politiques de sécurité sont intégrées dans les contrats. La clause de confidentialité s'étant au-delà des contrats.

Les responsabilités et les devoirs associés à l'utilisation de données sensibles sont également rappelés dans la Charte Informatique.

Les vérifications effectuées et documents recueillis sont stockés dans un outil dédié, garantissant notamment que les données ne seront pas conservées au-delà des délais légaux.

6.1.2. Collaborateurs sensibles

La liste des rôles « sensibles » et « confidentiels » vis-à-vis de la sécurité de l'information figure dans le fichier *E_M3_F3_Demande_de_Recrutement_Recruitment_Request* . Ce sont des utilisateurs à privilèges élevés (administrateurs, profil « sécurité », ...) ou ayant accès à des informations sensibles (DAF, RAF, RH, chefs de service, ...), comme des données à caractère personnel.

Lors des phases de recrutement, ces collaborateurs sensibles sont soumis aux mêmes vérifications que tous les collaborateurs, complété de :

- La vérification des diplômes

Ces contrôles peuvent être externalisées auprès d'un cabinet de recrutement, auquel cas les documents/preuves des contrôles sont récoltés auprès du cabinet.

6.2. Durant le contrat

Tous les collaborateurs du Pôle Eurocast sont sensibilisés et formés à la sécurité de l'information.

Les supports de formation et de sensibilisation doivent être documentés, validés par le RSSI et doivent à minima intégrer les thèmes suivants :

- Politiques et objectifs de sécurité de l'information
- Réaction en cas de malwares
- Gestion des mots de passe
- Enjeux de conformité de la sécurité de l'information
- Transferts d'information, NDA
- Utilisation des services IT

Une planification des formations et sensibilisations à la sécurité de l'information et des indicateurs appropriés de suivi doivent être définis.

Les mesures de sensibilisation et de formation sont mises en place à intervalles réguliers selon le document *E_S5_F5_Control_Review_and_Audit_Planning_FR* mais également dans le cadre de réponses à des événements de sécurité survenue en interne ou en externe.

6.3. Violation de contrat

Une procédure de traitement des violations des spécifications contractuelles relatives à la sécurité de l'information doit être décrite.

Ce processus disciplinaire peut être intégré dans le Règlement intérieur de la société.

6.4. Travail à distance / nomade

Le concept de travail à distance / travail nomade recouvre le travail en home-office mais également en déplacement hors des bureaux.

Les collaborateurs effectuant leur mission en dehors des zones de sécurité définies par le SMSI doivent respecter les règles de la charte informatique.

Pour se connecter à distance à leur espace de travail, les collaborateurs doivent suivre la procédure de connexion sécurisée (VPN, authentification forte, ...). Les mesures de sécurité applicables dans le cadre du home-office sont établies dans ce même document, et rappelées dans la Charte Informatique.

6.5. Sensibilisation des collaborateurs

Le concept de sensibilisation de GMD Eurocast est géré et animé centralement, et comprend :

- La première sensibilisation des collaborateurs à la suite de leur arrivée dans l'entreprise.
- Le renouvellement périodique des sensibilisations.
- Les sensibilisations ciblées.

La sensibilisation à la sécurité de l'information permet d'assurer que l'ensemble des collaborateurs sont informées :

- Des politiques de sécurité de l'information de l'entreprise et de la charte IT.
- De la nécessité de remonter les événements de sécurité de l'information, y compris les incidents non-informatiques.
- Des réflexes à avoir en cas de malwares.
- Des règles de gestion et usage de compte et mots de passe
- Des enjeux de la conformité TISAX, vis à vis de la productivité et des exigences clients.
- Des règles de confidentialité de l'information.
- Des règles d'utilisation des services IT externes.
- Des méthodes d'attaques fréquemment utilisés contre les entreprises du secteur industriel et automobile.
- Des règles de sécurité en télétravail/travail nomade.

6.5.1. Sensibilisation à l'arrivée des collaborateurs

Un parcours d'intégration des collaborateurs est en œuvre au sein de GMD Eurocast *E_M3_P1_F6_Programme_Accueil_Reception_Program*. Sur les aspects de sécurité de l'information, il comprend :

- Le parcours du règlement intérieur et de la charte IT avec le RRH du site.
- Une information sur l'existence du SMSI et une sensibilisation aux enjeux de la sécurité de l'information pour l'entreprise avec le Responsable Qualité du site.
- Une formation / sensibilisation aux risques Informatique, au RGPD, et à la Politique Compliance au travers de l'outil Upility.
- Une sensibilisation aux règles de sécurité propres au site avec le CL-SI.

6.5.2. Renouvellement des sensibilisations

Des actions ponctuelles pourront être menées

- Suite aux campagnes de phishing biannuelle.
- En cas de comportement inapproprié détecté par Sentinel-One.
- De détection d'incidents par le CL-SI ou le RSSI.

7. Politique de sécurité physique et continuité d'activité (§3 VDA ISA)

7.1. Sécurité Physique

7.1.1. Zones de sécurité physique

La sécurité physique est gérée au sein de GMD Eurocast par un concept de zones de sécurité physique. Chaque zone physique doit être affecté à un niveau de sensibilité :

- Verte : Publique
- Jaune : Restreinte
- Violette : Sensible
- Rouge : Confidentielle

Les critères de qualification des zones, ainsi que les exigences de sécurités associées sont recensés dans le document *E_S5_I2_Politique_de_Sécurité_Physique.pdf*.

→ **Chaque site** doit établir un plan de site indiquant la sensibilité des zones.

→ **GMD Eurocast, holding de tête**, valide les niveaux de sensibilité des zones identifiés sur le plan des sites industriels.

→ **Chaque site** doit identifier les non-conformités aux exigences de la politique de sécurité physique et définir le plan d'action pour traiter ces non-conformités.

7.1.2. Accueil des visiteurs

La procédure d'accueil des visiteurs est décrite dans le document *E_S5_I5_Politique de Gestion des visiteurs*.

→ **Chaque site** peut adapter localement sa procédure d'accueil des visiteurs.

→ **Chaque site** doit tenir à jour un registre des visiteurs, consignait arrivées et départ.

Les règles d'accès et de comportement des visiteurs sont établies dans le document *E_S5_I2_Politique_de_Sécurité_Physique* et sont :

- Communiquées aux visiteurs via le livret d'accueil des visiteurs communiqué en amont de la visite
- Rappelées par la personne accueillant le visiteur.
- Visibles via des pictogrammes affichés (ou zones de couleur identifiées) à l'entrée des zones sensibles et confidentielles.

→ **Chaque site** doit personnaliser le livret *E_M4_P1_F3_Livret_Accueil_Visiteur* avec les informations propres au site.

→ **Chaque site** doit veiller à ce que le livret d'accueil des visiteurs soit systématiquement communiqué en amont de la visite et/ou remis à l'arrivée du visiteur.

7.1.3. Attribution / Révocation des accès.

Les règles de gestion des accès physiques aux sites et aux zones sensibles/confidentielles sont documentées dans la procédure d'allocation, gestion, et révocation des droits d'accès. Elles comprennent :

- La procédure d'attribution des accès.
- Les règles d'inventaires et de revues des accès.
- La procédure de révocation des accès.
- La conservation des logs d'accès aux zones confidentielles.
- La gestion de la perte des moyens d'accès.
- Les règles relatives aux périodes et durées de validité des accès.

Les accès par badges sont inventoriés dans l'outil ad hoc propre au site.

→ **Chaque site** doit tenir à jour un registre des clés d'accès aux zones sensibles, revu régulièrement.

7.2. Plan de Reprise d'Activité (PRA)

Sur la base des éléments de l'analyse de risque, les situations de crise et de désastre majeurs sont identifiées dans le plan de reprise et de continuité de l'activité, ainsi que les procédures de gestion de crise et de gestion des situations d'urgence.

Les impacts des situations de crise sur les principaux équipements sont recensés.

Des mesures de redondance des équipements sont déployées afin de limiter l'impact des crises, ainsi que des mesures de prévention des désastres naturels :

- Mesures de protection et de détection anti-incendie
- Mesures contre les inondations et les phénomènes naturels (foudre, séismes, ...)

Les stratégies et procédures de sauvegarde et de restauration sont définies et mises en œuvre sur la base des besoins de continuité exprimés par les métiers (RPO / RTO : Recovery Point Objectives / Recovery Time Objectives).

Dans la mesure du possible, des dispositifs redondants de continuité d'activité pour la gestion de l'énergie et des communications sont également identifiés et déployés :

- Onduleurs
- Groupes électrogènes
- Double alimentation électrique
- Double opérateur de communication

Les processus et procédures de PRA et PCA sont régulièrement testés en fonction de la fréquence définie dans le plan de contrôle, d'audits et de revues *E_S5_F5_Control_Review_and_Audit_Planning_FR*.

7.3. Gestion des équipements confiés

- L'outil automatique de gestion des services informatiques répertorie tous les équipements pouvant être prêtés aux collaborateurs de l'organisation. Dans le cadre de l'organisation, l'outil de gestion sélectionné est **LANSWEEPER**
- L'inventaire de ces équipements est revu une fois par an.
- Les prêts d'équipement par l'organisation, pour un collaborateur, font l'objet d'une fiche d'identification du matériel affecté au collaborateur. La fiche d'identification du matériel, au format papier ou électronique, comprend :
 - Le nom du matériel et son identification unique, reconnue par l'outil de gestion des services informatiques
 - Le nom du collaborateur à qui l'équipement est prêté

- La date d'obtention du matériel et la date de rendu (si le prêt est terminé)
- La signature du collaborateur à qui l'équipement est prêté
- La signature du collaborateur qui a préparé les équipements.
- Lors de l'affectation, les informations de prêt sont vérifiées et reportées sous forme de ticket dans l'outil de gestion des services informatiques
- Une charte informatique donnée par le document *E_S5_I2_Charte_Informatique_FR* mentionne toutes les règles d'usage, les restrictions et les procédures en cas de perte ou vol du matériel mobile emprunté par les collaborateurs.
- Les collaborateurs souhaitant faire usage d'équipement mobile doivent signer et approuver la charte informatique. Le gestionnaire des équipements doit s'assurer de ces éléments avant tout prêt.
- L'usage de matériel personnel est interdit.

7.4. Politique d'utilisation des mobiles et outils de télétravail

- L'inventaire des équipements mobiles est effectué lors de l'inventaire des équipements et suivi sur LANSWEEPER
- Les règles de sécurité concernant les smartphones sont listées dans le document *E_S5_P4_SP4-Durcissement des téléphones mobiles*. A minima, les smartphones doivent être chiffrés et protégés par un code PIN.
- Les règles d'usage des équipements mobiles sont définies dans la *E_S5_I2_Charte_Informatique*.

8. Contrôles d'accès (§4 VDA ISA)

8.1. Accès utilisateurs au réseaux et services informatiques

Des règles ayant pour objectif d'empêcher les accès non autorisés aux services disponibles sur le réseau sont définies :

- À l'exception des réseaux et services communs, les utilisateurs ont uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.
- Des méthodes et solutions d'authentification appropriées sont utilisées pour contrôler les accès des utilisateurs distants. En particulier, dans le cas d'accès à distance à des informations ou applications sensibles, des solutions d'authentification fortes sont utilisées.
- Une matrice des droits d'accès est fournie par le document *E_S5_P3_F1_Revue de compte et droit* La demande de droits se fait au travers d'un formulaire électronique dans l'outil GLPI ([Lien GLPI](#))

→ **Chaque site** doit passer par GLPI pour toute demande de modification des droits d'accès.

8.2. Gestion des accès utilisateurs et utilisateurs à privilèges

La création, la modification et l'effacement des accès utilisateurs doivent systématiquement être l'objet d'une demande formelle, par le biais d'un ticket GLPI, et doit pouvoir être tracé.

→ **Chaque site** doit passer par GLPI pour toute demande de création ou suppression de compte.

Tout compte doit être nominatif, associé à une seule et unique personne, les opérations effectuées par le biais de ce compte devant pouvoir être tracés et associé à cette personne. L'utilisation de compte collectifs est limitée aux cas où aucun besoin de traçabilité n'est identifié, ou aux cas de roulement d'équipe où il est toujours possible d'identifier l'auteur d'une action. Les règles détaillées de gestion des comptes sont définies dans le document *E_S5_P7_Gestion_des_accès*.

Les comptes utilisateurs sont désactivés dès le départ du propriétaire de compte. Les comptes sont désactivés dans un premier temps, et conservés à des fins de traçabilités et supprimés lorsque la conservation n'est plus nécessaire.

→ **Les sites industriels** doivent informer l'équipe IT par le biais d'un ticket GLPI en amont du départ des collaborateurs afin de garantir la capacité de l'équipe IT à désactiver les comptes le jour du départ du collaborateur.

Les comptes d'utilisateurs à privilèges doivent systématiquement être individuels. Les utilisateurs à privilèges ne doivent pas utiliser de compte « admin » générique. En aucun cas, les admins ne sont autorisés à modifier les permissions qui leurs sont accordés.

8.3. Bon usage des secrets de connexion

Les collaborateurs de l'organisation doivent respecter des règles de manipulation et de confidentialité des informations secrètes d'authentification :

- Pas de divulgation des informations d'authentification à des tiers - pas même à des personnes autorisées - en tenant compte des paramètres juridiques.
- Pas d'écriture ou de stockage non chiffré des informations d'authentification
- Changement d'information d'authentification lorsqu'un compromis potentiel est suspecté
- Interdire l'utilisation d'information d'authentification identiques pour des but professionnels et non professionnels
- Changement des informations d'authentification initiales obligatoire lors de la première connexion
- Qualité des informations d'authentification obligatoire (longueur mot de passe, etc.) et adaptée au rôle du collaborateur (utilisateur / administrateur)

La création, la modification et le stockage des mots de passe doivent suivre les règles édictées dans le document *E_S5__Charte_Informatique_FR*. Un outil de gestion des mots de passe validé par l'ANSSI est mis à disposition des collaborateurs (Keepass).

La transmission des informations secrètes d'authentification se fait par remise en main propre par le N+1 et modification du mot de passe à la première connexion.

8.4. Politique des mots de passe

La politique de mot de passe est la suivante :

- Règles de complexité des mots de passe définie :
 - Longueur : minimum 12 caractères, maximum 20 caractères,
 - Doit contenir des majuscules, des minuscules, des chiffres et/ou des symboles.
 - Ne doit pas commencer par un chiffre,
 - Peut contenir des caractères spéciaux (& »#[!\\@])\$%),
 - Peut contenir des caractères accentués,
 - Ne doit pas contenir un mot figurant dans le dictionnaire, un nom, prénom ou surnom.
- Renouvellement des mots de passe tous les 3 mois.
- Interdiction du partage des mots de passes.
- Utilisation de mots de passe différents pour chaque compte.
- Authentification forte quand l'outil le permet et que le collaborateur dispose d'un téléphone portable d'entreprise.
- Sensibilisation de l'ensemble des collaborateurs à la présente politique.
- Contrôle et l'audit des bonnes pratiques.
- Utilisation d'un gestionnaire de mots de passe (Keepass).

8.5. Restriction d'accès au réseau

L'accès au réseau est contrôlé et segmenté. Les règles de segmentation sont tenues à jour dans un registre.

8.6. Contrôles et revues des comptes et droits d'accès

Les comptes et les droits d'accès physiques, réseau, système et applicatifs sont audités régulièrement, à minima une fois par an, en fonction des fréquences définies dans le plan de contrôle, d'audits et de revues *E_S5_F5_Control_Review_and_Audit_Planning_FR_EN.xlsx*. Un compte-rendu de revue des droits d'accès doit être formalisé et des plans d'actions correctives mis en œuvre le cas échéant. Toute modification effectuée à la suite d'une revue de compte doit être tracée dans un ticket. Les résultats des revues des droits d'accès sont analysés lors des comités de pilotage sécurité.

9. Politique d'utilisation des mesures de chiffrements (§5.1 VDA ISA)

Toute utilisation de mesure de cryptographie doit respecter les paramètres juridiques et légaux (Loi pour la Confiance en Economie Numérique) en vigueur, en France. Les règles cryptographiques sont définies dans le document *E_S5_I4_Politique_de_cryptographie_FR..* Dans le cas de force majeure, l'utilisation de mesure de chiffrement dépréciées doit faire l'objet d'une dérogation formelle validée par le RSSI.

Des procédures de gestion du cycle de vie des clés sont établies au sein du même document, abordant :

- La génération des clés ;
- La distribution des clés ;
- Le stockage sécurisé ;
- La durée de vie des clés et certificats ;
- La régénération des certificats ;
- La révocation des certificats ;
- Le renouvellement et suppression des clés.

La conformité à la politique de cryptographie est supervisée centralement, site par site, par le biais d'un registre dédié.

10. Sécurité des opérations (§5.2 VDA ISA)

10.1. Gestion du changement

La gestion des changements s'applique aux changements :

- Des systèmes IT ;
- Des processus de l'entreprise ;
- De l'organisation.

L'objectif de la gestion des changements est d'empêcher les changements de provoquer une réduction du niveau de sécurité de l'information dans l'entreprise. Ainsi, tout changement doit faire l'objet :

- D'une approbation formelle ;
- D'une analyse d'impact sur la sécurité de l'information ;
- D'une planification et de tests ;
- De l'identification de procédure de retour arrière en cas de défaut.

La document *E_S5_P9_Gestion du changement* détaille la procédure de gestion des changements permettant le respect des exigences ci-dessus. L'outil GLPI est mis en œuvre pour assurer la traçabilité des changements et le respect de la procédure.

Un bilan et retour d'expérience associé aux changements doit être réalisé au cours des CPSSI mensuels.

→ **Chaque site** doit se conformer à la procédure de gestion des changements *E_S5_P8_Gestion du changement*. Les managers sont habilités à réaliser des demandes de changement par le biais de l'outil GLPI. Le CL-SI est consulté par le RSSI pour le traitement de la demande de changement.

→ **Chaque site** doit assurer la traçabilité de tout changement par la création d'un ticket de changement, y compris pour les changements d'organisation ou apportés aux processus de réalisation.

10.2. Protection antivirus

Pour assurer la protection contre les virus, les mesures suivantes sont mises en œuvre :

- Un antivirus est déployé pour l'ensemble du parc informatique (serveurs, ordinateurs) **SentinelOne**.
- Les signatures des anti-virus sont déployées automatiquement par une console centralisée, qui ne peut pas être désactivée par les utilisateurs.
- Des sensibilisations des collaborateurs ont lieu régulièrement.
- Les pièces jointes associées aux emails sont scannées systématiquement par l'agent **SentinelOne**. Une évaluation de la légitimité des emails est effectuée par l'outil **VadeSecure**.
- En matière de durcissement, les logins et mots de passe par défaut des équipements sont modifiés lorsque cela est possible.
- Les utilisateurs ne sont pas administrateurs de leurs postes. Seules quelques personnes ont conservé ce droit, pour des raisons motivées. Ces exceptions sont gérées au travers du formulaire électronique 'Gestion des exceptions' dans GLPI.

10.3. Journaux et journalisation

La traçabilité des opérations et la levée d'alerte sur les outils informatiques sont assurés par la gestion des logs :

- Les besoins en matière de journalisation sont identifiés (logs réseaux, systèmes, applicatifs) lors du déploiement de nouveaux systèmes informatiques, notamment lors des projets informatiques et lors de la gestion des changements.
- L'ensemble des logs, hors AD, est centralisé dans un serveur puits de log **Wazuh**.
- Les accès au puits de log sont limités aux seuls administrateurs et donnent lieu à une alerte.
- Les accès administrateurs au sein de l'AD sont journalisés dans l'application **Wazuh**.
- Cette application permet de faire remonter des alertes associées à la détection de comportements anormaux.
- Ces alertes doivent donner lieu à des événements de sécurité, en cas de comportement suspect ou malveillant.

10.4. Gestion des vulnérabilités

Les vulnérabilités sont gérées au travers de différents logiciels :

- **SentinelOne** pour l'analyse des vulnérabilités de type obsolescence des versions logicielles.
- **Greenbone** réalise des scans de vulnérabilité réguliers de type OWASP.

De plus, **SentinelOne** identifie également des failles de vulnérabilité sur les systèmes.

Le site de l'ANSSI CERT.FR est régulièrement consulté pour le suivi des nouvelles vulnérabilités (CVSS) accessible depuis GLPI. Une veille des vulnérabilités est également assurée auprès des éditeurs.

La gestion des mises à jour est gérée :

- Mensuellement pour les OS des serveurs et postes de travail, et monitoré via l'outil **LanSweeper**. La mise à jour des OS est effectuée via **WSUS**.
- Les versions vulnérables d'OS et de logiciels sur les serveurs et postes de travail sont supervisées continuellement via **SentinelOne**.

Le document *E_S5_P3_F3 Procédure de gestion des vulnérabilités* recense les différents mécanismes et outils de veille aux vulnérabilités, et la procédure de traitement de ces vulnérabilités.

10.5. Gestion des audits techniques

Des audits techniques externes, en complément des scans de vulnérabilités réalisés via l'outil Greenbone, doivent être planifiés par le RSSI et intégrés au plan de plan de contrôles, audits et revues. Ces audits sont planifiés en fonction des besoins, l'objectif étant de réaliser à minima un audit technique externe par an. Ces audits peuvent être :

- Un test d'intrusion du SI pôle.
- Un test d'intrusion sur un sous-ensemble des sites industriels.
- Un audit du réseau.

Les conclusions de cet audit technique devront donner lieu à un plan d'action et/ ou une actualisation de l'analyse de risques.

10.6. Gestion du réseau

Une séparation des réseaux est déployée et les schémas d'architecture sont formalisés. Les matrices d'échanges inter-réseaux sont définies dans le document VLAN.xlsx, accessible au service IT uniquement. Des revues de ces règles de filtrage sont planifiées et réalisées régulièrement.

Des règles de prévention et de détection sont déployées au niveau du pare-feu. Des mécanismes de contrôles de la sécurité des réseaux sont en place au niveau du pare-feu. Seuls les équipements identifiés par leur adresse Mac peuvent se connecter aux réseaux wifi et filaires.

Les accès distants sont réalisés par VPN sécurisé, avec des mécanismes d'authentification forte.

La supervision du réseau est réalisée par l'outil **Zabbix**, les bureaux IT sont équipés d'écran de supervision.

11. Acquisition, maintenance et développement (§5.3 VDA ISA)

11.1. Exigences de sécurité pour les nouveaux développements

Les exigences de sécurité pour les nouveaux développements ou les évolutions de systèmes existants sont identifiées en amont et testées tout au long du cycle de développement.

Les données de test sont gérées et protégées (phases de création, de stockage et de destruction) ; les données de production ne sont jamais utilisées lors des phases de test.

11.2. Exigences de sécurité pour les services réseaux

Les protocoles et les niveaux de sécurité des services de réseaux acceptés sont identifiés et reportés dans les procédures de sécurisation des réseaux.

Les contrats des opérateurs doivent intégrer des SLA relatifs aux protocoles et niveaux de sécurité des services de réseaux.

11.3. Réversibilité et sécurité de destruction de l'information dans le Cloud

Dans le cas d'utilisation de services Cloud, les règles de réversibilité et de destruction des données en fin de contrat sont établies dans les accords contractuels conclus avec les prestataires de services.

11.4. Ségrégation des données de l'organisation dans le cloud

Dans le cas d'utilisation de services Cloud, les règles de ségrégation des « tenants » sont établies dans les accords contractuels conclus avec les prestataires de services et vérifiées par l'organisation.

12. Sécurité dans les relations fournisseurs (§6 TISAX)

12.1. Exigences de sécurité de l'information pour les fournisseurs

Les fournisseurs et les partenaires font l'objet d'une évaluation des risques basée afin de les classer sur l'échelle suivante :

- Niveau 1 : Fournisseur sans impact ou avec un faible impact.
- Niveau 2 : Fournisseur sensible.
- Niveau 3 : Fournisseur très sensible.

Les critères de classification, et exigences applicables pour chaque niveau sont définies dans le document **E_S1_P1_F8_Evaluation_des_fournisseurs_sensibles.xlsx**.

Pour les Fournisseurs obtenant une criticité supérieure ou égale à 2, Eurocast doit s'assurer de :

- Avoir signé une NDA (doit comprendre clause de confidentialité et de réversibilité)
- Remplir le questionnaire d'auto-évaluation. Pour les fournisseurs ayant un SMSI certifié (ISO 27001, TISAX, ...), le questionnaire est facultatif et n'est envoyé que si l'évaluateur juge nécessaire de recueillir plus d'informations sur la sécurité de l'information du fournisseur. Le certificat du Fournisseur doit être récupéré.
- Examiner le questionnaire du fournisseur le cas échéant, et décider des actions correctives pertinentes à mettre en place et conserver les enregistrements des résultats de l'examen. Les décisions prises au cours de la revue doivent être documentées et enregistrées.
- Les fournisseurs atteignant une criticité supérieure ou égale à 3 doivent :
 - En amont de l'échange d'informations sensibles, les méthodes d'échanges autorisées doivent être définies avec le fournisseur.
 - Pour les fournisseurs cloud et IT uniquement :
 - Avoir fait l'objet d'une étude de sécurité par le RSSI ou RSI.
 - Des SLAs doivent être définis.
- Le cas échéant, les exigences de sécurité du client sont relayées dans les contrats avec les fournisseurs.
- Le respect des engagements contractuels de sécurité est contrôlé tout au long de l'année et documenté annuellement dans la fiche **E_S1_P1_F8_Listing_fournisseur_sensible**.
- Les fournisseurs sont tenus de communiquer leurs exigences de sécurité à leurs propres fournisseurs. Dans tous les cas, les fournisseurs sont tenus d'informer l'organisation de toute sous-traitance.

12.2. Services IT sur cloud externe

12.2.1. 1.2.4 Partage des responsabilités avec les services IT externes (based on ISO27017)

- Les services informatiques cloud sont identifiés dans le document **E_S1_F22_A_Listing_fournisseur_sensible**.
- Les employés responsables de la gestion des services informatiques sont désignés.
- Modèle de contrat de fournisseur avec une identification claire des responsabilités ; un TOM (Mesures techniques et organisationnelles, basées sur les exigences VDA) pourrait être annexé au contrat.
- Identification des services informatiques externalisés / partagés dans le champ d'application du SMSI.
- Évaluation régulière de la sécurité de l'information des fournisseurs de services informatiques

12.2.2. Gestion des services IT externes

- Les services informatiques externes sont sélectionnés et évalués en fonction de critères de sécurité avant d'être utilisés.
- Une évaluation des risques est effectuée pour les services informatiques externes

- Les exigences en matière de sécurité des actifs informationnels sont communiquées aux services informatiques externes.

12.2.3. Retour et suppression sécurisé des actifs informationnels des services IT externes

- Il est garanti qu'une clause du contrat du fournisseur régit le retour et le retrait sécurisé des actifs informationnels des services informatiques externes.
- Une procédure de réversibilité des services informatiques externes sera décidée si nécessaire.

12.2.4. Protection de l'information dans les services IT externes partagés

- Une ségrégation efficace des tenants est assurée dans les services informatiques externes partagés, comme les services cloud.
- Les règles et l'accord de ségrégation du fournisseur de cloud doivent être vérifiés avant l'utilisation.

13. Conformité (§7 VDA ISA)

13.1. Veille légale et réglementaire

Les exigences réglementaires applicables, par pays, sont recensées dans le système de veille réglementaire RedOnline. La prise en compte des exigences légales doit être validée au sein de cet outil. Des objectifs de conformité et un indicateur de suivi de la conformité y est évalué.

En complément, les exigences réglementaires applicables liées à la sécurité de l'information doivent être recensés pour chaque pays dans le fichier géré par la DSI de GMD_Eurocast : *E_M3_F14_Registre_de_veille_règlementaire_SSI*.

Pour chaque exigence légale identifiée relative à la sécurité de l'information, doit être suivi :

- L'applicabilité de l'exigence à GMD Eurocast,
- L'état de la conformité,
- Les éventuelles actions à mener.

→ **Chaque pays inclut dans le périmètre du SMSI** doit faire l'objet d'un Registre de veille réglementaire au format du document *E_M3_F14_Registre_de_veille_règlementaire_SSI*.

La veille est réalisée grâce à différents canaux :

- Juriste de la société GMD
- Remontées d'informations par les partenaires du groupe GMD
- Feedback partenaire IT / consultants
- Sites spécialisés (ANSSI, CNIL, ...) et flux RSS
- Réseaux sécurité (CLUSIF, CLUSIR, club RSSI, ...)

Des sessions de sensibilisation au respect des exigences légales et réglementaires sont réalisées régulièrement. La communication relative au respect des exigences légales et réglementaires est réalisée au cours des COSSI et COPIL sur SMSI, sauf dans le cas d'une évolution majeure qui donnera lieu à une communication spécifique.

Les enregistrements du SMSI (logs, rapports de revues de droits, d'audit, tickets d'incidents, de changements, ...) sont conservés dans le respect des durées de conservation légales.

13.2. Protection des données à caractère personnel.

GMD Eurocast se conforme aux exigences du RGPD par le biais des mesures suivantes :

- Les exigences légales en matière de sécurité concernant les données personnelles sont intégrées dans les procédures et processus correspondants.


- L'identification des données à caractère personnel est intégrée dans les critères de risques au moment de la classification d'un projet.
- Des registres de traitement sont établis, en qualité de Responsable de traitement et de Sous-Traitant du Responsable de traitement.
- Une politique de gestion des données à caractère personnel est établie et communiquée aux parties intéressées.
- Un DPO est nommé et ces fonctions et autorités sont définies.
- Une adresse générique **dpo@gmd-eurocast.com** destinée à collecter les demandes d'exercices de droit ou à signaler une violation est communiquée aux parties intéressées.
- Enfin, les procédures destinées à répondre aux demandes d'exercices des droits sont formalisées.
- L'importance du respect des exigences en matière de données personnelles est communiquée à l'ensemble de l'organisation.
- Les exigences en matière de données personnelles sont intégrées dans les contrats de travail, de vente et de sous-traitance / prestation.

14. Gestion des exceptions

L'ensemble des règles fixées dans la PSSI constituent des exigences de sécurité qui doivent être respectées.

Cependant, à titre exceptionnel des dérogations peuvent être établies dans un cadre déterminé :

- Demande exprimée par un collaborateur et approbation formelles du RSSI ou sponsor du SMSI sous la forme d'une dérogation dans l'outil GLPI.
- Tenue d'un registre des dérogations par le RSSI.
- Chaque dérogation est limitée dans le temps et sa pertinence doit faire l'objet d'un suivi régulier. Ce suivi est intégré dans le plan de contrôles, d'audits et revues.

Rédacteur	Vérificateur
Directeur Système d'Information Stéphane LAVERDURE le 17/04/2025 	Le Sponsor Alain GIL