Politique générale de sécurité des systèmes d'information

Fiche de contrôle

Versions	Date	État
V1	Décembre 2020	Révision du document
V2	Janvier 2021	Révision du document

Auteurs	Fonction	Contact
JM. VARNET	Directeur informatique du groupe, CIO	jean-marc.varnet@algeco.com

Destinataires	Fonction	Contact
Équipe dirigeante		
Comité exécutif		
Directeurs informatiques		

Sommaire

1 ENGAGEMENT GÉNÉRAL DU COMITÉ EXÉCUTIF DU GROUPE EN MATIÈRE DE POLITIQUE DE SÉCURITÉ

Cette politique fait partie de l'ensemble des politiques de Modulaire Group, elle précise leur application pour la France, mais en cas de conflit les politiques de Modulaire Group (sur https://www.modulairegroup.com/corporate-policies), prévaudront.

Aujourd'hui, le système d'information d'Algeco est un support indispensable et joue un rôle de plus en plus important dans les activités quotidiennes de l'entreprise afin de relever les défis et respecter les orientations stratégiques de l'entreprise.

Une défaillance ou un piratage des systèmes d'information pourraient entraîner l'incapacité de livrer des modules, de conclure un contrat avec un client ou d'établir des factures. En conséquence, la disponibilité des systèmes d'information ainsi que l'intégrité du traitement de l'information doivent être entièrement contrôlées.

Algeco évolue dans un contexte concurrentiel dans lequel les actifs humains et informationnels sont activement recherchés et où toute défaillance peut être exploitée contre l'entreprise. En conséquence, Algeco doit mettre en œuvre les actions appropriées pour se protéger en garantissant la continuité de son activité, de ses informations ainsi que de celles de ses clients.

Par conséquent, ce document s'inscrit dans le cadre d'un effort visant à formaliser les principes de base en matière de sécurité. Il est conçu pour répondre aux exigences d'Algeco, compte tenu de l'importance croissante des systèmes d'information, d'améliorer et de maintenir les processus d'affaires, la confidentialité et l'intégrité des données, ainsi que la gestion et la gouvernance de l'entreprise. Cette politique répond également à la nécessité de protéger les données personnelles des clients et des collaborateursde l'entreprise.

L'entreprise vise à démontrer au travers de cette politique que la sécurité informatique ne constitue pas une contrainte, mais plutôt une manière de procéder aux changements nécessaires ainsi que de faire face aux menaces et risques posés par l'environnement ou par un contexte particulier.

La réussite de cette opération repose sur l'**implication de l'équipe** :

- Dans les questions organisationnelles ou comportementales et les problèmes techniques ;
- Dans le suivi permanent des actions et des incidents ;
- Dans l'établissement d'une méthodologie structurée et coordonnée au niveau de Algeco ainsi que de règles et procédures devant être mises en œuvre au niveau local/national.

Chaque personne a un rôle important à jouer à son niveau personnel et au travers de ses propres actions afin d'assurer la meilleure protection possible des ressources informatiques de Algeco.

Notre politique vise un objectif précis, basé sur notre stratégie et dans le respect de nos valeurs. Je compte sur nos employés, en plus de se conformer à la politique utilisateur, pour faire preuve de vigilance, de prudence et de réactivité dans leurs tâches quotidiennes.

J'encourage le Comité exécutif et ses équipes de direction à renforcer l'engagement de nos collaborateurs dans ce processus.

Mark HIGSON, CEO Modulaire Group *(Signature)*

2 INTRODUCTION

2.1 Objet de la présente politique

L'**ITSGP (Information Technology Security General Policy** ou Politique générale de sécurité informatique) a pour objectif de fournir un référentiel cohérent pour la Sécurité du système d'information (SI) d'Algeco.

Il s'agit d'un document fondateur qui fait partie d'un plus grand ensemble de documents décrivant les mesures de sécurité visant à assurer la sécurité des données.

Elle précise les enjeux et objectifs de sécurité et exprime les principes de gouvernance en matière de sécurité des systèmes d'information. La présente politique permet de garantir :

- La **disponibilité** des informations et les moyens de les traiter ;
- L'**exactitude** et **l'exhaustivité** des informations et les moyens de les traiter ;
- La **confidentialité** des informations gérées ;
- La **traçabilité** et la **vérifiabilité** des informations traitées.

2.2 Champ d'application

L'ITSGP (Information Technology Security General Policy) couvre l'ensemble des données et leur traitement (création, stockage, échange, etc.), que le format soit matériel ou immatériel (électronique, imprimé, oral, image, etc.) dans toute notre organisation.

Cela signifie qu'elle s'applique :

- **À l'ensemble du personnel permanent ou temporaire de l'entreprise**, travaillant au sein de l'entreprise ou à distance ;
- **À l'ensemble des partenaires de l'entreprise, qu'il s'agisse de personnes physiques ou morales** (sous-traitants, prestataires de services, fournisseurs), ayant accès au système d'information d'Algeco ;
- **À tous les équipements et logiciels physiques** permettant le traitement des données d'Algeco.

2.3 Cadre juridique et réglementaire

La sécurité du système d'information a pour objectif principal de préserver la propriété d'information du groupe dans un cadre réglementaire complexe et en constante évolution, au sein duquel Algeco opère.

De ce fait, l'ensemble du document de référence en matière de sécurité d'Algeco repose sur le cadre réglementaire européen et international.

Les domaines à traiter sont les suivants :

- Protection des données à caractère personnel (RGPD) ;
- Propriété Intellectuelle ;
- Archivage légal ;
- Prévention de la fraude ;
- Cybercriminalité ;
- Utilisation de méthodes cryptographiques ;

- Confidentialité de la correspondance et de la vie privée.

En tant que leader du marché, Algeco doit se conformer aux réglementations spécifiques des pays dans lesquels l'entreprise est implantée. Le système d'information doit intégrer cette exigence, tout particulièrement en matière de protection des informations personnelles et financières.

Cette politique est néanmoins applicable quel que soit le cadre réglementaire en vigueur, puisque des documents spécifiques détaillés permettant sa mise en œuvre seront adaptés au contexte juridique et réglementaire local, si celui-ci est différent de celui applicable pour le groupe.

3 RESPONSABILITÉS ET GOUVERNANCE

3.1 Rôles et responsabilités

3.1.1 IT (Information Technology Department ou Service de technologie de l'information)

IT :

- Est responsable de la définition, de la mise à jour et de la distribution des cadres et normes techniques applicables à la sécurité des systèmes d'information ;
- Est responsable de la gestion de la sécurité tout au long du cycle de vie des systèmes d'information ;
- Est en charge de la maintenance permettant d'assurer sur le long terme le niveau de sécurité souhaité ;
- Assure la définition, la mise en œuvre et la maintenance des projets permettant la continuité des activités d'Algeco ;
- Vérifie que les objectifs de sécurité et les niveaux de sécurité ciblés sont atteints et que les cadres et normes techniques sont respectés ;
- Est chargé de sensibiliser les utilisateurs à la sécurité des systèmes d'information en mettant en œuvre des campagnes d'information, en fixant des objectifs pédagogiques et en définissant des termes communs au sein d'Algeco.

3.1.2 CIO (Chief Information Officer ou Directeur des systèmes d'information)

Le Directeur des systèmes d'information est responsable du développement et de la maintenance des systèmes d'information du groupe, et notamment de la sécurité. Le CIO délègue la gestion de la sécurité au CISO.

3.1.3 CISO (Chief Information Security Officer ou responsable de la sécurité des systèmes d'information RSSI)

Le CISO dirige et coordonne la sécurité des systèmes d'information et, à cet égard, a les responsabilités suivantes :

- Analyser les risques posés à Algeco et évaluer leurs conséquences/impacts potentiels ;
- Assurer la protection des systèmes d'information d'Algeco ;
- Fournir à cette fin un ensemble de politiques, procédures et lignes directrices et les réviser chaque année ;
- S'assurer que la sécurité informatique, les contrôles, les politiques et les procédures fonctionnent efficacement dans l'ensemble du groupe ;
- Travailler en collaboration avec l'équipe de direction du groupe afin d'identifier et de mettre en œuvre tous les changements nécessaires pour assurer la conformité à la réglementation de toutes les unités opérationnelles stratégiques (Strategic Business Unit ou SBU) ;
- Représenter la fonction informatique lorsqu'il s'agit d'assister des activités d'audit internes et externes et s'assurer que toutes les mesures correctrices sont prises comme convenu dans le cadre des examens après audit ;

- Pilotage et organisation de la sécurité au sein d'Algeco à l'aide du Comité de sécurité informatique ;
- Sensibiliser les utilisateurs à la sécurité en matière de systèmes d'information ;
- Audit et contrôle du respect de l'ITSGP et d'autres documents de référence en matière d'informatique.

Si le rôle de CISO n'est pas rempli par une ressource dédiée, il peut être partagé entre différents postes au sein de l'équipe de gestion informatique (c.-à-d. les directeurs informatiques), via un support externe ou une expertise tierce.

3.1.4 Directeurs informatiques

Les directeurs informatiques, y compris les directeurs informatiques de l'unité organisationnelle stratégique (SBU) et le directeur de l'infrastructure informatique, ont les responsabilités suivantes en matière de cybersécurité :

- Relayer et accompagner les objectifs de sécurité informatique du groupe au sein de leur périmètre géographique et fonctionnel ;
- Donner des retours d'expérience sur les progrès réalisés ; p.ex. déploiement d'outils, campagne de sensibilisation à la sécurité, etc. ;
- Procéder au déploiement des politiques de sécurité informatique et assurer leur adoption et leur respect au sein de leur SBU ;
- Prendre part au comité de sécurité informatique (réunion bimensuelle) ;
- Alerter le Comité de sécurité informatique en cas d'incident et participer à la gestion des crises d'incidents.

3.2 Gouvernance

3.2.1 Comité de sécurité informatique (ITSC)

Le Comité de sécurité informatique, dirigé par le Directeur Informatique du groupe, se réunit une fois tous les deux mois et a les responsabilités suivantes :

- Partager des informations sur la sécurité informatique avec les relais locaux (Directeurs informatiques des SBU), et recueillir des informations auprès de ceux-ci (nouveaux projets, incidents, changements, audits et contrôles), afin de prendre les bonnes décisions au bon moment.
- Couvrir les sujets liés à la sécurité informatique à un niveau stratégique et couvrir des sujets ayant des implications au sein du groupe et des différentes SBU.
- Assurer le suivi et le pilotage de l'ensemble des activités visant à mieux respecter la politique de sécurité informatique au sein des différentes SBU.

Le Comité de sécurité informatique est composé, pour chaque domaine :

- Participants :
  - Directeur informatique France
  - Directeur informatique Royaume-Uni
  - Directeur informatique DACHS
  - Directeur informatique ENSE
  - Directeur informatique NORDICS
  - Directeur informatique Infrastructure

- Invités :
    - Responsable sécurité des infrastructures informatiques
    - Directeur juridique adjoint

3.2.2 Reporting

Des **rapports réguliers** doivent être présentés au Comité de sécurité informatique, sur l'état de la sécurité de l'information au sein d'Algeco. Ces rapports s'appuient sur un tableau de bord de sécurité présentant un panel d'indicateurs clés de performance (ICP ou KPI) pertinents. Ces indicateurs doivent aider à évaluer le niveau actuel d'exposition et de protection du système d'information, ainsi que les efforts de sécurité réalisés. En outre, tout comité compétent identifié peut, sur demande, se voir remettre un rapport annuel décrivant l'état général du programme de sécurité de l'information d'Algeco et sa conformité.

4 PRINCIPES DE SÉCURITÉ

Les principes de sécurité d'Algeco sont issus de la norme internationale ISO/CEI 27002:2013 (Technologie de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information).

4.1 P1 – Identification et maîtrise des risques de sécurité

Afin de protéger son système d'information, Algeco doit connaître, analyser et évaluer les risques auxquels il est exposé, et agir en conséquence. Des **analyses régulières des risques** sont nécessaires pour élaborer un plan d'atténuation approprié, afin de réduire à un niveau acceptable les risques avérés auxquels est confrontée l'entreprise.

4.2 P2 – Protection des systèmes informatiques, des infrastructures et des postes de travail

Il convient de veiller à la protection des informations et de la communication sur les réseaux et systèmes permettant leur collecte, leur traitement, leur diffusion et leur stockage. La première étape consiste à sécuriser le matériel et les logiciels utilisés.

À cet effet, les principes suivants doivent être transposés au niveau opérationnel et mis en œuvre :

- Les réseaux et les infrastructures doivent être protégés en installant le matériel nécessaire, en configurant le matériel et les logiciels de manière à garantir le niveau de sécurité nécessaire, en **séparant et segmentant/partitionnant les systèmes et réseaux**, en **filtrant** les flux de données et en ayant recours à des **solutions logicielles de sécurité**.
- Les serveurs, autres systèmes partagés et postes de travail individuels doivent être protégés en choisissant un matériel adéquat, en sécurisant la configuration utilisée (« **renforcement** ») et en utilisant des logiciels de sécurité. Les procédures de **gestion de la configuration** devraient être efficaces et régulièrement testées.
- La **disponibilité, l'intégrité, la confidentialité et la traçabilité** des informations doivent être garanties dans le respect des objectifs en matière de sécurité, notamment lors de leur transit sur les réseaux et leur traitement sur les systèmes :
    - Des mécanismes doivent être mis en place contre tout **accès externe non autorisé** ;
    - Les **informations sensibles** doivent être isolées afin d'éviter tout accès non autorisé ;
    - Des mécanismes visant à empêcher la lisibilité des informations des personnes non autorisées (p.ex. **solutions d'anonymisation ou de chiffrement**) doivent être mis en place ;
    - Des **contrôles des événements de sécurité et des mécanismes de surveillance** doivent être mis en place.
- Tous les logiciels (des micrologiciels aux applications et systèmes d'exploitation) doivent bénéficier des **mises à jour de sécurité** publiées par leur éditeur, et ces mises à jour de sécurité doivent être effectuées selon une politique claire et formelle.

- La politique de mise à jour de toute composante du système d'information doit inclure une **procédure de mise à jour d'urgence**, conçue pour faire face à une importante vulnérabilité. Les procédures de **gestion des correctifs et le traitement des alertes** doivent être efficaces et régulièrement testées ;
- La divulgation, la modification, le vol ou la destruction non autorisée de biens physiques (documents, postes de travail, supports amovibles, etc.) doivent être évités.
- Outre la protection physique des actifs, sites et bâtiments de l'entreprise, des **dispositifs de protection physiques et logiques** des supports disponibles sur le réseau doivent être implémentés, afin d'éviter toute intrusion ou tout accès non autorisé.

Il convient, dans les politiques de sécurité, de formaliser les directives techniques et fonctionnelles de sécurité suivantes pour les infrastructures et systèmes :

- Directives et mécanismes techniques de **sélection et de positionnement des logiciels spécialisés contre les logiciels malveillants, les intrusions logiques et pour la protection des codes malveillants** (avec mise en œuvre de différents outils à différents points stratégiques) ;
- Directives et mécanismes **de mise à jour des correctifs et configurations**, avec maintien en condition opérationnelle des solutions sélectionnées ;
- Directives et mécanismes relatifs à la protection des données sensibles **(chiffrement, pseudonymisation, anonymisation**, etc.) ;
- Directive relative à la **protection des postes de travail et des supports amovibles des utilisateurs** (p. ex. clés USB).

Ces directives sont définies pour les postes de travail de bureau ainsi que pour les postes de travail mobiles (ordinateurs portables, smartphones, tablettes, etc.).

4.3 P3 – Sécurité des utilisateurs

4.3.1 Avant l'embauche

1. **Les vérifications des antécédents** de certains candidats à l'emploi doivent être effectuées conformément aux lois, réglementations et à la déontologie applicables et proportionnellement aux exigences commerciales, à la classification des informations à consulter et aux risques perçus.
2. Les collaborateurs doivent accepter, dans le cadre de leurs obligations contractuelles, les termes de leur **contrat de travail** et le signer. Ce contrat doit déterminer leurs responsabilités ainsi que celles de l'organisation en matière de sécurité informatique, telles que décrites dans la politique utilisateur en matière d'informatique.

4.3.2 Pendant la durée du contrat d'embauche

1. La direction doit exiger de tous les collaborateurs et utilisateurs tiers qu'ils appliquent les consignes de sécurité conformément aux politiques et procédures établies en la matière par l'entreprise.
2. Toutes les activités menées par les collaborateurs d'Algeco doivent être réalisées au moyen **des appareils de l'entreprise**, et les connexions au réseau local via des ordinateurs personnels doivent être évitées. Cependant, le BYOD (Bring Your own Device ou AVEC Apportez Votre Équipement personnel de Communication) est toléré car l'accès aux outils collaboratifs et aux e-mails est autorisé à partir d'appareils personnels

(ordinateurs de bureau, ordinateurs portables, tablettes, smartphones). L'utilisation et l'accès à d'autres outils de travail depuis un appareil personnel sont interdits, sauf en cas de dérogation accordée par les directeurs informatiques.

3. Un **processus disciplinaire** officiel et communiqué doit être mis en place pour agir contre les collaborateurs ayant commis une **violation de la sécurité de l'information**.

4.3.3 Cessation ou changement d'emploi

Les tâches et responsabilités **toujours valides après la cessation ou le changement** d'emploi doivent figurer sur le contrat de l'employé, du sous-traitant ou de l'utilisateur tiers.

L'employé ou les utilisateurs tiers doivent être tenus au courant de ces tâches et responsabilités.

4.4 P4 – Gestion des identités et des accès

Un contrôle de l'accès physique et logique au matériel et aux logiciels permet de garantir un niveau élevé de sécurité de ces derniers.

À cet effet, les principes suivants doivent être transposés au niveau opérationnel et mis en œuvre :

- Toute personne accédant à une composante du système d'information doit être **identifiée, authentifiée** et limitée dans ce qu'elle peut faire au strict minimum nécessaire, y compris les administrateurs (« **principe de moindre privilège** »).
- Toute action ayant un impact potentiel sur la sécurité du système d'information doit être **enregistrée et reliée à son auteur**. Il en va de même pour toute action ayant un impact significatif sur l'activité.
- Tout compte donnant accès à une composante doit être **personnel et nominatif**. L'utilisation de comptes génériques/de service, souvent utilisés pour les accès techniques dans le cadre de la gestion des dispositifs, devrait être autorisée par une dispense validée et la mise en œuvre des mesures d'atténuation requises.
- Les responsabilités confiées à une personne ne doivent pas permettre à une personne malveillante, ayant compromis le compte de la première, de perpétrer des actes frauduleux. Des procédures clairement définies formalisent les actions assignées aux différents acteurs et mentionnent les **séparations des tâches**, avec des processus indépendants de **gestion des comptes** (ouverture, modification, gestion des comptes perdus…), **profils et droits** (par composant ou groupe de composants) et **attribution de profils et de droits à des comptes** (octroi de droits…). Les processus doivent également clairement distinguer les rôles du **bénéficiaire** (à qui un droit est attribué), **le demandeur** (qui demande le droit pour le compte du bénéficiaire), le **validateur** (qui confirme le droit à donner) et le **gestionnaire fonctionnel** (qui donne et vérifie régulièrement les droits d'utilisateur).
- Tout droit attribué sur le système d'information doit être **temporaire** (c.-à-d. avoir un début et une fin). Pour les collaborateurs en contrat à durée indéterminée, les droits attribués prennent fin avec la cessation du contrat.
- Toute donnée utilisée pour l'identification (p. ex. identifiant) ou l'authentification (p. ex. mot de passe) doit être **transmise en toute sécurité**, afin de garantir son intégrité et sa confidentialité.

Les directives et mécanismes relatifs à la **gestion des droits d'accès** sur les postes de travail (les droits administratifs ne sont pas accessibles aux utilisateurs) et la procédure d'authentification des utilisateurs doivent être formalisés.

4.5 P5 – Sécurité de l'information

4.5.1 Définition des responsabilités liées aux actifs

1. Un **actif** doit être considéré comme un atout précieux permettant à Algeco d'exercer ses activités. Il peut s'agir d'une base de données, d'un fichier ou d'une chose physique (appareils informatiques, etc.) ou d'une personne physique et de ses aptitudes (comme ses compétences, son expérience). Les actifs liés à des données (ainsi que les moyens de traitement associés) doivent être **identifiés et conservés dans un inventaire à jour**, mentionnant **leur propriétaire**.
2. Les règles d'utilisation correcte des informations et des moyens de traitement associés doivent être formalisées et mises en œuvre en conséquence, comme décrit dans les politiques de sécurité spécifiques.
3. Tous les collaborateurs et les tiers doivent **restituer tous les moyens de traitement** dont ils disposent à la fin de leur contrat.

4.5.2 Classification des informations

1. Les renseignements devraient être **classifiés** en fonction de leur valeur, de leurs exigences légales, de leur sensibilité ou de leur criticité pour l'entreprise, tel que défini dans la politique de sécurité spécifique relative à la classification des informations.
2. Cette classification élabore et met en œuvre un ensemble de guides et de procédures appropriés pour le traitement et la protection des informations et des dispositifs connexes sur lesquels elles sont stockées.
3. Une **politique d'archivage des documents** devrait également être définie conformément aux obligations légales en vigueur, appliquées aux documents numériques et aux documents physiques.

4.6 P6 – Sécurité lors du travail mobile

L'évolution des technologies a permis aux utilisateurs d'accéder au système d'information tout en étant mobiles. Des mesures spécifiques doivent aider à sécuriser ce nouveau type d'utilisation et d'accès.

À cet effet, les principes suivants doivent être transposés au niveau opérationnel et mis en œuvre :

- Les appareils mobiles (ordinateurs portables, tablettes, smartphones…) doivent être protégés en choisissant un matériel adéquat (p. ex. doté d'un support fournisseur adéquat), en **sécurisant leur configuration** (verrouillage d'écran, chiffrement…), en installant des **mises à jour de sécurité** et en utilisant, le cas échéant, des logiciels de sécurité.
- L'**état de la flotte mobile** doit être surveillé et analysé afin de prendre toute les mesures pertinentes nécessaires.

- Les **points d'accès** au système d'information utilisés par les appareils mobiles doivent être **identifiés et sécurisés** (authentification forte, chiffrement, délai d'expiration, VPN...).
- Les utilisateurs mobiles doivent être informés des questions de sécurité, telles que décrites dans la politique utilisateur renfermant à la fois des règles et un code de pratique.
- L'utilisation de téléphones mobiles personnels est tolérée pour accéder aux e-mails, et l'utilisation personnelle des appareils mobiles professionnels est également tolérée dans la mesure où cette utilisation est raisonnable. En tout état de cause, l'usage professionnel et l'usage personnel doivent être clairement séparés.
- Les risques liés à la **perte ou au vol d'appareils mobiles** doivent être analysés et couverts.

4.7 P7 – Gestion du journal de sécurité

1. La charge des principaux systèmes (processeurs, mémoire, espace disque, etc.) et des ressources réseau doit être **surveillée**, afin d'en dégager les tendances globales (moyennes, niveaux de pics et fréquences, etc.) par application.
2. Les événements ayant un impact sur la sécurité ou présentant un risque de sécurité doivent être consignés au niveau du réseau, du système ou de l'application.
3. **Les journaux des événements** doivent être traités et tenus à jour en regard des risques opérationnels et réglementaires identifiés.
4. Les journaux des événements doivent être tenus **à jour et examinés** périodiquement.
5. Les moyens de journalisation et les données enregistrées doivent être protégés contre les falsifications et les risques non autorisés.
6. Toutes les procédures opérationnelles doivent être **tenues à jour** afin de permettre une réaction rapide en cas d'incidents de sécurité.

4.8 P8 – Incidents de sécurité et gestion de crise

1. Des processus doivent être mis en place pour permettre une réponse rapide et efficace en cas d'incidents de sécurité informatique, et pour permettre **un processus d'alerte** via les canaux appropriés.
2. Chaque utilisateur doit consigner et signaler toutes les vulnérabilités de sécurité informatique observées ou suspectées. En ce qui concerne les violations de sécurité impliquant des données à caractère personnel, celles-ci doivent être signalées à l'autorité de contrôle compétente si elles sont susceptibles d'entraîner un risque pour les droits et libertés des personnes, comme prévu dans la Procédure de gestion des violations de la sécurité des données à caractère personnel.
3. Il convient d'**évaluer** les événements liés à la sécurité informatique afin de déterminer s'ils doivent être qualifiés d'incidents de sécurité informatique.
4. Les connaissances recueillies à la suite de l'analyse et de la correction des incidents doivent être utilisées pour **réduire la probabilité** ou l'impact d'incidents subséquents.
5. Les processus d'identification, de collecte, d'acquisition et de protection d'informations **constituant des éléments de preuve** doivent être définis et appliqués.
6. Il convient également de coordonner les interventions en cas d'infection des postes de travail ou des serveurs (à titre d'exemple) et d'activer des **processus de gestion des incidents et de gestion de crise**.
7. En matière de gestion de crise, les conditions d'entrée, les processus et les conditions de sortie propres à la crise doivent être définis et formalisés dans le cadre d'une **procédure de gestion de crise**.
8. Les personnes ayant des responsabilités pendant les crises doivent être **formées** à la gestion de crise.

4.9 P9 – Aspects de la gestion de la continuité des activités liés à la sécurité de l'information

1. Les **interruptions** d'activité de l'entreprise doivent être neutralisées.
2. Les processus opérationnels critiques doivent être protégés contre les principales **défaillances des systèmes d'information ou les effets de catastrophes**.
3. La **récupération** de ces processus doit être garantie dès que possible.
4. L'**intégrité et la disponibilité** des informations et des moyens de traitement des informations doivent être maintenues.
5. Les moyens et processus de **sauvegarde d'urgence et de récupération des ressources informatiques** doivent être définis dans les délais et conformément aux **objectifs de disponibilité** fixés par le secteur concerné, notamment en termes durée maximale d'interruption admissible (Recovery Time Objectives ou RTO) et de perte de données maximale admissible (Recovery Point Objectives ou RPO).

Algeco met en œuvre une stratégie de services fournis aux utilisateurs conformément à ses objectifs et priorités, à savoir un **Business Continuity Plan** (BCP) ou plan de continuité d'activité. Ce BCP vise à garantir les informations dans les délais nécessaires à l'exécution des missions de l'entreprise, et à définir l'ensemble des plans et moyens nécessaires pour satisfaire aux **exigences de l'entreprise en matière de continuité des activités**. Le BCP doit être testé et maintenu en conditions opérationnelles.

Le service informatique est responsable de la définition et de la maintenance du **Disaster Recovery Plan** (DRP) ou plan de reprise après sinistre, qui définit la mise en œuvre de **sauvegardes fiables de récupération**, et, au minimum, d'un **site de sauvegarde**. Les sauvegardes des données et applications utilisées au sein de l'entreprise sont essentielles pour surmonter des **incidents opérationnels ou des catastrophes majeures**. Des tests réguliers (au moins une fois par an) pour vérifier les sauvegardes de récupération (essais de restauration) doivent être effectués et un rapport sur les résultats des essais être établi.

Ces plans doivent...

- être conformes aux exigences légales en matière de sécurité de l'information et, en particulier, les plans de reprise ne doivent pas introduire de risques importants ;
- être conformes aux objectifs de sécurité de l'entreprise ainsi qu'aux politiques de sécurité actuelles ;
- inclure les exigences en matière de sécurité au sein de tous les processus opérationnels.

Une **politique de sauvegarde régulière pour les informations et les logiciels essentiels** est définie pour les activités de l'entreprise, conformément aux obligations légales en vigueur, appliquées aux documents numériques et physiques.

4.10 P10 – Sensibilisation à la sécurité et formation

La plupart du temps, ce sont les personnes qui constituent le maillon le plus faible de la chaîne de sécurité. Sans équipes informatiques bien formées et sans utilisateurs bien avertis, la moindre stratégie de sécurité informatique est vouée à l'échec. Les efforts de **sensibilisation à la sécurité** et l'organisation de **cours de formation** constituent des éléments essentiels de l'instauration d'une politique de sécurité.

Ainsi, les collaborateurs et les utilisateurs tiers doivent suivre les séances de sensibilisation et de formation appropriées en matière de sécurité, et obtenir périodiquement les mises à jour pertinentes des politiques et procédures de sécurité liées à leurs fonctions.

Ce principe de sécurité vise à s'assurer que toutes les fonctions disposent de ressources suffisantes et adéquatement qualifiées pour gérer l'établissement, la mise en œuvre et le maintien d'une politique de sécurité de l'information.

4.11 P11 – Contrôle des niveaux de sécurité et de conformité

Des contrôles appropriés doivent être mis en œuvre pour protéger les informations confidentielles et sensibles, conformément aux principes et aux règles définis dans les politiques et les normes approuvées (ainsi que les règlements spécifiques). Tout écart par rapport aux normes doit être **corrigé, ou des contrôles compensatoires** doivent être **mis en œuvre** au besoin. Le Comité de sécurité informatique doit être informé et consulté en cas de déviations ou de demandes de dérogations.

Des audits indépendants doivent être réalisés et toutes les conclusions et recommandations relatives à la sécurité de l'information doivent être communiquées au Comité de sécurité informatique. Des mesures correctives appropriées doivent être prises si nécessaire.

Il convient d'évaluer régulièrement dans quelle mesure Algeco satisfait, en matière de sécurité de l'information, aux **exigences réglementaires ou de conformité**. Les contrôles effectués au cours des audits doivent couvrir au minimum le respect des règles définies dans l'IT Security General Policy (ITSGP) et ses transpositions opérationnelles, le respect de la

réglementation (p. ex. RGPD), le respect de la propriété intellectuelle, la bonne utilisation des licences logicielles, l'intégrité et la confidentialité des données sensibles. Les efforts et initiatives visant à **assurer le respect de la sécurité de l'information** au sein des SBU doivent être surveillés.

4.12 P12 – Sécurité liée au cycle de vie des systèmes d'information

1. Les exigences relatives aux mesures de sécurité de l'information doivent être documentées dans les exigences techniques et contractuelles pour les **nouveaux systèmes d'information** ou lorsque de **nouveaux changements** surviennent sur les systèmes existants.
2. Des règles dédiées au **développement de logiciels et de systèmes** doivent être définies et appliquées.
3. **L'implémentation des changements** doit être surveillée au moyen de processus formalisés. Lorsque des changements sont effectués sur les systèmes de production, les applications essentielles pour l'activité de l'entreprise doivent être **testées** afin de vérifier qu'il n'y aura pas d'effet indésirable sur l'activité ou la sécurité de l'entreprise.
4. Un **environnement de développement** doit être donné pour la réalisation de tâches de développement ou d'intégration spécifiques, ainsi que pour le cycle de vie global du développement.
5. L'activité de développement de **systèmes externalisés** doit être surveillée et contrôlée.
6. Les tests de conformité et les critères connexes devraient être définis pour les **nouveaux systèmes d'information, les mises à jour et les mises à niveau.** Les données test doivent être soigneusement sélectionnées, protégées et contrôlées.

4.13 P13 – Sécurité liée aux activités informatiques externalisées

1. Les exigences en matière de sécurité des systèmes d'information (pour limiter les risques liés à l'**accès par un tiers** aux informations ou aux moyens de traitement) doivent être documentées dans la procédure appropriée.
2. Les exigences applicables liées à la sécurité des systèmes d'information doivent être établies et discutées avec chaque **tiers** qui accédera, traitera et stockera, communiquera ou fournira des composantes de l'infrastructure.
3. **Les engagements contractuels avec des tiers** devraient inclure des exigences relatives à la gestion des risques liés aux systèmes d'information.
4. Les services fournis par des tiers doivent faire l'objet d'un **suivi et d'un audit périodiques**.
5. **Les changements** effectués dans le cadre d'un service **fourni par un tiers** doivent être gérés, en s'assurant qu'ils sont conformes aux politiques et procédures de sécurité de Algeco, et en s'assurant qu'ils tiennent compte de l'importance des informations après évaluation du risque associé.
6. Les tiers doivent s'engager à **sensibiliser et à former leurs collaborateurs aux bonnes pratiques en matière de sécurité informatique**. Ils doivent également s'assurer que les collaborateurs ont connaissance des règles de sécurité applicables d'Algeco (p. ex. par le partage de la politique utilisateur en matière d'informatique d'Algeco).

4.14 P14 – Fusions et acquisitions

La réalisation de fusions et d'acquisitions conduit Algeco à intégrer de nouvelles personnes, de nouveaux sites, de nouvelles applications et de nouveaux processus dans son système d'information. Cette intégration doit être gérée de manière réfléchie et organisée, en tenant compte des enjeux de sécurité du groupe et de sa nouvelle entité.

À cette fin, il convient de décliner sur le plan opérationnel et d'appliquer les principes suivants :

- L'intégration doit être précédée d'un premier **audit de maturité** et d'un **inventaire complet des systèmes et processus** de la nouvelle entité, avec l'établissement d'une **cartographie complète** et la mise en œuvre d'une **analyse des risques**, sur les activités et systèmes de l'entité ainsi que sur le processus d'intégration à venir.
- Le **plan d'intégration**, détaillant les opérations de **remplacement et de récupération** des systèmes et infrastructures de l'entité, doit être intégré en tenant compte des besoins opérationnels (« en l'état ») et des questions liées à la maintenance et à la sécurité informatique.
- Une fois le processus d'intégration achevé, les systèmes et infrastructures repris ou remplacés doivent être reconsidérés **en fonction de leur niveau de risque identifié**, et notamment du niveau de sensibilité des informations qu'ils sont susceptibles de contenir ou de traiter.

4.15 P15 – Dérogations

Toutes les dérogations relatives aux différentes politiques ou directives de cette ITSGP doivent être **analysées** au regard des risques induits.

Toutes les dérogations à une mesure doivent être **documentées** et faire l'objet d'une **acceptation formelle,** avec **validation écrite et traçable des risques associés** par le Comité de sécurité informatique et, si nécessaire, par d'autres avis consultatifs.

Toutes les dérogations, ainsi que les mesures d'atténuation liées, doivent être temporaires et examinées régulièrement (au moins une fois par an).

5 MESURES

5.1 Modifications/Révisions

La présente ITSGP est révisée une fois par an et peut évoluer dans les cas suivants :

• Une modification majeure du contexte interne d'Algeco (changement organisationnel, changement de mission, nouvelles pratiques ou technologies, etc.) ;

• Une modification du contexte juridique ou réglementaire (nouvelles lois, etc.) ;

• Une évolution des risques (risques de réévaluation, etc.).

Le CISO est responsable de la révision et de la modification éventuelle de la politique, qui doit être validée par l'ITSC (IT Security Committee) d'Algeco.

5.2 Implémentation et suivi

Le CIO (Chief Information Officer ou directeur des systèmes d'information) a désigné le CISO comme responsable de la définition et du suivi de la présente ITSGP.

5.3 Entrée en vigueur de la politique

La présente ITSGP entre en vigueur à la date de sa validation par le Comité exécutif d'Algeco.

6 Annexe – références

6.1 Archivage des documents relatifs à la sécurité

	Algeco Documents relatifs à la politique de sécurité	Responsable de maintenance
RP	Risk Policy (soumis le 24 janvier 2019)	Service juridique
RAIC	Algeco Risk Analysis IT and Cyber (du 28 novembre 2018)	Services juridiques et informatiques
ITSGP	IT Security General Policy	Service informatique
ITSPIC	IT Security Policy for Information Classification	Service informatique
BCP CMP	General Policy of the Business Continuity Plan Crisis Management Plan	Service juridique
ITSPIC	IT Security Policy for Incident Response	Service informatique
SSPR	Specific Security Policy for Retention	Service juridique
ITUP	IT User Policy	Service informatique & services RH
CE	Code of Ethics	Service juridique
NDA	Non Disclosure Agreement	Service juridique
PP	Privacy Policy relating to the protection of Personal Data in accordance with GDPR	Service juridique
PDSB	GDPR Personal Data Security Breach Management Procedure	Service juridique

6.2 Principales normes applicables

• ISO/CEI 27001:2013 : Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

• ISO/CEI 27002:2013 : Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

• ISO/CEI 27005:2018 : Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

6.3 Références

Cadres NIST (2018), ISO (2013/2018), Royaume-Uni (Version 1.1 mai 2018), AUS (2018/2019)

6.4 Glossaire

BCP – Business Continuity Plan ou Plan de continuité d'activité : Ensemble des mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des services essentiels de l'entreprise, puis de la reprise de toutes les activités.

BIA – Business Impact Analysis : les objectifs d'une BIA sont d'identifier les activités essentielles ou critiques de l'entreprise. Elle permet également de se prononcer sur les objectifs de temps de reprise pour ces activités.

CIO : Chief Information Officer (Directeur des systèmes d'information)

CISO : Chief Information Security Officer (Responsable de la sécurité des systèmes d'information, RSSI)

DRP - Disaster Recovery Plan (Plan de reprise d'activité PRA) : ensemble des procédures et dispositions prévues pour garantir la reprise des systèmes informatiques suite à un sinistre survenu dans l'entreprise. Sous-ensemble du BCP qui couvre les moyens informatiques et de télécommunication. Il garantit la reprise des systèmes désignés comme critiques, dans les délais fixés.

Externalisation : Transfert de tout ou partie d'une fonction d'une organisation (entreprise ou administration) à un partenaire externe.

IT : Information Technology (technologie de l'information, informatique)

LAN – Local Area Network : réseau interne local, auquel sont connectés tous les ordinateurs d'Algeco par le biais d'une prise réseau disponible.

Intrusion logique : une intrusion logique regroupe les actions, effectuées par une personne ou un objet, pour pénétrer dans un espace logique défini où sa présence n'est pas souhaitée.

Code malveillant : tout programme visant à endommager un système d'information ou un réseau ou de causer des dommages à travers ces derniers.

Remarque : les virus ou les vers sont deux types bien connus de codes malveillants.

6.5 Documents de référence relatifs à la sécurité informatique

Les documents de référence relatifs à la sécurité informatique d'Algeco sont organisés sous forme de pyramide à trois niveaux :

- Le premier niveau est composé de :

- L'engagement pris par le Comité exécutif d'Algeco (ExComm) en matière de sécurité informatique, présenté dans le premier chapitre du présent document ;
- La présente ITSGP présentant les principes de sécurité en vigueur au sein d'Algeco ;

- Le deuxième niveau est composé de politiques de sécurité spécifiques, afin de détailler les rôles et les responsabilités pour des sujets clés tels que :
  - La politique utilisateur en matière d'informatique présentant les consignes de sécurité SI destinées aux utilisateurs d'Algeco ;
  - Le plan de continuité d'activité ;
  - La classification des informations.

- Le troisième et dernier niveau est composé des éléments suivants :
  - Guides de sécurité fournissant, le cas échéant, les procédures permettant le bon respect des politiques de sécurité spécifiques ;
  - Procédures de sécurité fournissant, le cas échéant, une description détaillée par étapes permettant la mise en conformité avec les mesures de la Politique de sécurité spécifique.

La structure des documents de référence relatifs à la sécurité d'Algeco est illustrée sous forme de pyramide dans le schéma ci-dessous :

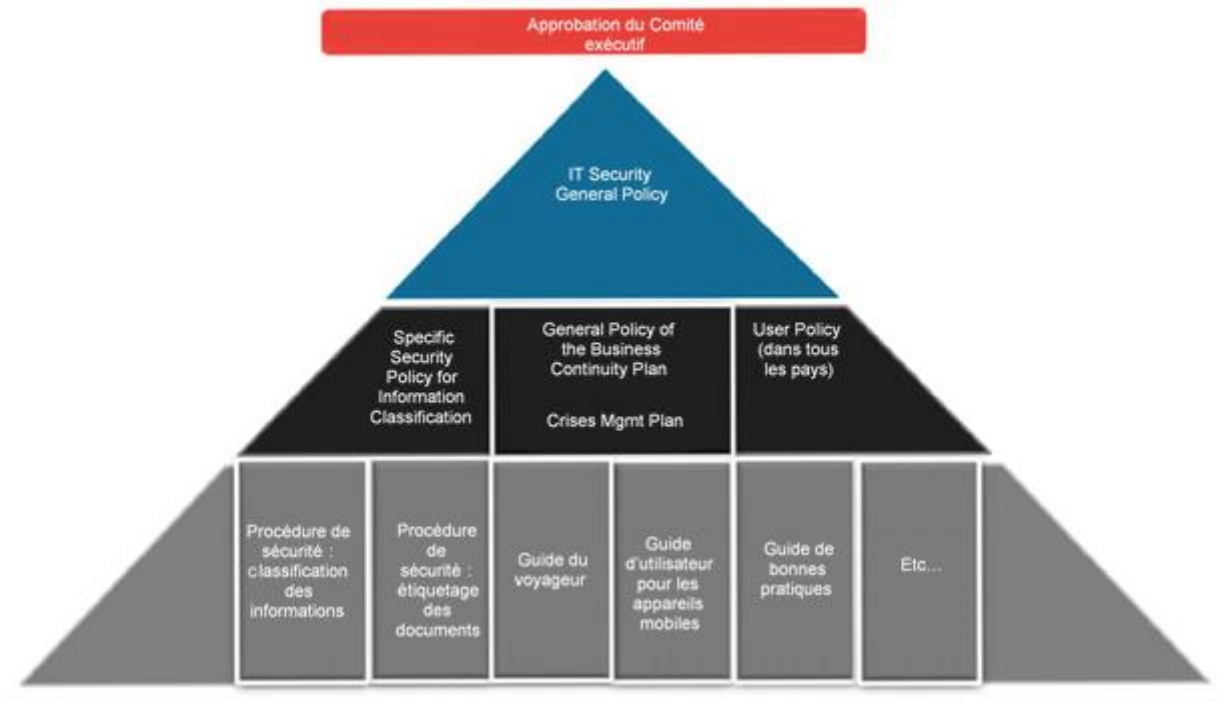

Fig 2 : Structure des documents de référence relatifs à la sécurité d'Algeco

Cette politique a été émise en février 2023.