Principes généraux de la sécurité informatique

1. Introduction

1.1. Préambule et objectifs

Le groupe ABC arbitrage (ci-après, le "groupe") construit des systèmes de trading innovants et des stratégies de gestion quantitatives sur une gamme d'actifs, avec un focus sur les opportunités de trading de niche et à court-moyen terme. Il opère sur près de 100 marchés à travers le monde (24h/24 et 5 jours/5), fournissant de la liquidité grâce à des signaux mécaniques ou systématiques. Ses techniques de trading reposent sur une approche scientifique et axée sur les données pour générer de l'alpha, traitant des milliards de données chaque jour. Dans ce contexte, le groupe est dépendant de la qualité de ses informations et de son infrastructure technique, dont la qualité des données et les performances, sont absolument cruciales pour son activité. Cela l'oblige donc à s'assurer d'un fort niveau de sécurité.

Par ailleurs, le groupe est soumis à un cadre réglementaire dense et en constante évolution, qui tend vers une responsabilisation accrue des entreprises en matière de protection des données et de sécurité des systèmes d'information. Dans le même temps, les attentes des parties prenantes du groupe se renforcent, du fait de la montée en puissance des exigences de transparence, de fiabilité et de résilience dans la chaîne de valeur. Ces exigences couvrent les enjeux liés à la propriété intellectuelle, aux licences et, plus largement, à la conformité des usages numériques. Le groupe considère la sécurité de l'information, la

résilience opérationnelle et la continuité d'activité comme des piliers essentiels de sa gestion des risques et de sa responsabilité vis-à-vis de ses parties prenantes.

Le groupe a ainsi mis en place un corpus de documents de référence, qui définissent les objectifs de sécurité, les mesures mises en place, les règles générales et recommandations, les conditions de mise en œuvre et les mécanismes de contrôles afin de réduire les risques à un niveau acceptable. Le présent document a pour objet de formaliser, à un niveau volontairement général et non opérationnel, les engagements du groupe à ces égards, sans en dévoiler les modalités opérationnelles, techniques ou organisationnelles détaillées, afin de ne pas compromettre leur efficacité. Les modalités opérationnelles, techniques et organisationnelles détaillées de mise en œuvre des dispositifs de sécurité, de continuité et de reprise font l'objet de documents internes distincts, non publics, régulièrement mis à jour et testés. Ils permettent de :

- garantir la sécurité de l'information ;
- prévenir toute fuite d'informations et assurer la confidentialité des données ;
- assurer la continuité des activités ;
- encadrer les modalités de reprise des systèmes d'information en cas d'incident majeur ;
- renforcer la confiance des contreparties : prestataires et clients.

1.2. Champ d'application / Périmètre

Les différents principes et règles qui en découlent s'appliquent à :

- L'ensemble des entités du groupe ;
- L'ensemble du système d'information du groupe ;
- L'ensemble de ses activités et métiers, quels que soient leurs lieux d'implantation ;
- L'ensemble des Dirigeants et collaborateurs des sociétés du groupe ;
- L'ensemble des tiers, qui pourraient utiliser le SI du groupe et/ou hébergent des données appartenant au groupe ;
- L'ensemble du patrimoine informationnel et intellectuel du groupe quel qu'en soit la nature (électroniques, imprimées, manuscrites, vocales, images, données personnelles- conformément aux dispositions du RGPD, données ou flux, etc.).
- L'ensemble des moyens humains, techniques et organisationnels permettant de créer, de conserver, d'échanger, de partager et de supprimer des informations entre les acteurs internes et/ou tiers du groupe, quel qu'en soit le support (composants matériels, logiciels, bases de données ou espace de stockage et d'archivage, équipements liés aux postes de travail et aux dispositifs clients, les équipements d'infrastructure et de sécurité, procédures et réseaux d'échange d'information, bâtiments et locaux, etc.)
- L'ensemble des informations relatives ou appartenant à ses clients, ses partenaires ou tout autre tiers avec lesquels il est en relation, en particulier celles dont l'altération ou la divulgation pourrait porter atteinte à son image ou son activité et celles de ses contreparties ;
- L'ensemble des informations nécessaires à la gestion de son personnel, telles que les informations d'identité, salariales ou d'appréciation, dont la divulgation constituerait une violation de la vie privée.

1.3. Principes & références

La démarche s'appuie sur une analyse approfondie des risques associés au système d'information, tels qu'identifiés dans la cartographie des risques globale du groupe. Elle repose également sur les standards reconnus, références réglementaires et bonnes pratiques de place, telles que le guide de la Politique de Sécurité des Systèmes d'Information (PSSI) publié par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou encore la norme internationale ISO/IEC 27001, ISO/IEC 27002 ainsi que les référentiels du NIST.

Ce référentiel s'inscrit dans une démarche transversale et cohérente avec les autres dispositifs internes du groupe. Il est notamment complété par la Charte d'achats responsables, qui intègre des exigences spécifiques en matière de sécurité et de protection de l'information vis-à-vis des fournisseurs et prestataires, ainsi que par le Règlement intérieur, qui précise les obligations des collaborateurs en matière d'usage des outils numériques et de sécurité des systèmes d'information et les sanctions applicables en cas de manquement. Il est également complété par la Politique de protection des données personnelles et de conformité au Règlement général sur la protection des données (RGPD), afin d'assurer une prise en compte systématique des enjeux relatifs aux données à caractère personnel.

Conformément au principe du maillon le plus faible, selon lequel l'efficacité globale de la sécurité dépend du composant, du processus ou de la personne la plus vulnérable de la chaîne, des mesures de protection homogènes sont mises en place.

2. Principes et règles de sécurité

2.1. Corpus documentaire de référence

La sécurité et l'intégrité des systèmes ont toujours été une préoccupation sérieuse pour ABC arbitrage. La cybersécurité est traitée avec la même importance que les autres niveaux de sécurité. Ainsi que mentionné en introduction, le groupe s'est doté :

- d'une Politique de Sécurité des Systèmes d'Information (PSSI), visant à garantir la sécurité de l'information (confidentialité, intégrité, disponibilité, mais aussi fiabilité et traçabilité), la protection des données, y compris à caractère personnel, la maîtrise des risques cyber et technologiques ;
- d'un *Business Continuity Plan* (BCP), destiné à assurer la continuité des activités critiques en cas d'événement majeur susceptible d'en perturber leur fonctionnement normal (ex : panne électrique, défaillance des communications, corruption ou perte de données, etc.) et atténuer les pertes ;
- d'un *Disaster Recovery Plan* (DRP), encadrant les modalités de reprise des systèmes d'information en cas d'incident majeur affectant les infrastructures techniques ;
- d'un processus de gestion de crise formalisé, précisant notamment la gouvernance de la cellule de crise, les modalités d'activation et de communication, les rôles et

responsabilités, ainsi que les principes de gestion des informations sensibles et de suivi post-incident ;

- d'une Charte informatique, communiquée à l'ensemble des collaborateurs et annexée au Règlement intérieur, définissant notamment les principes, règles et les devoirs quant à l'usage et la sécurité des systèmes d'information, à la protection des données - y compris les données personnelles - et au respect de la propriété intellectuelle ; sa violation est susceptible d'entraîner des sanctions.

2.2. Principales mesures mises en place

2.2.1. Mesures générales et gouvernance

Le groupe a défini clairement les responsabilités et les rôles des différents acteurs de la sécurité, afin de garantir une bonne anticipation des problématiques de sécurité, une gestion cohérente des règles, leur mise en œuvre effective et coordonnée et le suivi de leur application dans la durée. La gouvernance en termes de sécurité du système d'information du groupe est organisée de la manière suivante :

- **Le Conseil d'administration** est régulièrement informé des enjeux majeurs liés à la sécurité des systèmes d'information et à la résilience opérationnelle. Il reçoit des reportings dédiés portant notamment sur les résultats des audits et l'état d'avancement des projets liés à la cybersécurité. Le CTO est à disposition du Conseil d'administration pour échanger et répondre à toute question.
- **La Direction exécutive** porte la responsabilité globale de la sécurité de l'information et s'assure de l'adéquation des moyens mis en œuvre avec les risques identifiés. Elle est chargée d'assurer le respect des engagements, de superviser leur mise en œuvre et de veiller à ce que les manquements éventuels soient sanctionnés ;
- **Le CTO du groupe** supervise et pilote la stratégie de sécurité. Il est membre du Comité de Direction du groupe ;
- **L'équipe chargée de la sécurité des systèmes d'informations** propose et planifie les actions ou projets de sécurité destinés à réduire les risques. Elle a un rôle de coordination pour la mise en œuvre et l'application des mesures de sécurité et de cyber-résilience. À ce titre, elle intervient sur l'ensemble du cycle, en couvrant les actions de prévention (sensibilisation, formation, etc.), de protection, de défense, de résilience / remédiation ou encore d'amélioration continue pour l'ensemble des activités du groupe ;
- **Les experts techniques** sont responsables de la mise en œuvre et du fonctionnement des dispositifs de sécurité opérationnelle dans leur périmètre (maintien en condition opérationnelle, veille technique, analyse et résolution des incidents, etc.), dans le respect des orientations définies. Ils peuvent contribuer à la formulation des besoins et attentes face aux risques ;
- **Les autres collaboratrices et collaborateurs** sont pleinement acteurs de la sécurité de l'information et tenus de respecter les règles et bonnes pratiques en vigueur ;
- **Les fonctions de contrôle :** Les fonctions de contrôle interne, de gestion des risques et, le cas échéant, d'audit contribuent à l'évaluation indépendante du dispositif de sécurité et à son amélioration continue ;

Ce dispositif s'appuie sur des **canaux de communication clairs et adaptés,** permettant une diffusion efficace de l'information auprès de l'ensemble des acteurs de la sécurité et de la résilience internes et externes en situation normale comme en situation de crise, y compris en cas d'indisponibilité de réseaux de communication numériques.

L'application des règles de sécurité fait l'objet d'un **suivi et de contrôles** réguliers. Des audits techniques et organisationnels sont effectués périodiquement et ponctuellement afin de mesurer l'efficacité et l'efficience des dispositifs en place et le respect des obligations et engagements. Les applications, bases de données et systèmes sont ainsi vérifiés à différents moments du cycle de vie, et en particulier lors de leur intégration dans le SI, lors d'évolutions majeures, ou de façon exceptionnelle en cas d'identification d'une vulnérabilité critique. Par ailleurs, le groupe met à disposition des mécanismes permettant de signaler tout incident, manquement ou situation susceptible d'affecter la sécurité des systèmes d'information.

Le dispositif prévoit, le cas échéant, des **modalités d'application adaptées des règles de sécurité**, afin de tenir compte de situations spécifiques tout en garantissant un niveau de protection équivalent. Ces modalités et les règles spécifiques sont formalisées et validées formellement après avis de l'équipe chargée de la sécurité des systèmes d'information qui tient à jour la liste des dérogations.

Enfin, le groupe collecte et publie **dans son rapport annuel des indicateurs** relatifs à la cybersécurité, la confidentialité et à la sécurité des données, tels que le nombre de violations de la sécurité de l'information constatés, le pourcentage d'employés sensibilisés et formés ou encore le nombre de tests effectués.

2.2.2. Sécurité liée aux ressources humaines

Le facteur humain constitue l'une des sources de vulnérabilité les plus courantes dans le maintien du niveau de sécurité des systèmes d'information et est à ce titre un point d'attention central du groupe en la matière. Le dispositif de sécurité du SI intègre des mesures relatives au facteur humain, combinant, d'une part, des actions de sensibilisation et de responsabilisation des utilisateurs, et, d'autre part, des mesures d'accompagnement et de sécurisation des usages visant à limiter le risque d'erreur humaine.

Parmi les mesures de responsabilisation et de sensibilisation des utilisateurs :

- les utilisateurs sont régulièrement **informés et sensibilisés** sur leurs responsabilités en termes de sécurité du SI afin de s'assurer que chacun est conscient des enjeux et des risques. Chaque collaborateur est sensibilisé à la sécurité du SI dès son arrivée. Cette sensibilisation présente les enjeux propres au groupe, les grands principes de la PSSI, les bonnes pratiques de sécurité et les responsabilités de chacun. La charte informatique est remise à chaque collaborateur lors de son intégration au sein du groupe. Les documents sont librement accessibles sur l'intranet et des rappels sont effectués à intervalles réguliers auprès de l'ensemble des collaborateurs ;
- La Direction ainsi que les responsables de chaque domaine opérationnel sont formés à la bonne mise en œuvre des *Business Continuity Plan* (BCP) et *Disaster Recovery Plan* (DRP).

- les obligations en matière de respect du secret professionnel et de clauses de confidentialité sont inscrites dans le contrat de travail des collaborateurs ; la charte informatique est annexée au règlement intérieur, assortie de **sanctions et mesures disciplinaires en cas de non-respect ;**
- tous les utilisateurs participent à des **tests et à des formations obligatoires** (sur une plateforme dédiée et par une formation interne) aux principes de sécurité. Des campagnes régulières de sensibilisation et de tests (ex: *phishing*) sont conduites à l'échelle du groupe afin d'évaluer et de renforcer le niveau de vigilance des collaborateurs face aux menaces cyber ;
- les utilisateurs ont le devoir (inscrit dans le règlement intérieur et la charte informatique) de signaler et faire remonter tout dysfonctionnement, anomalie, comportement suspect ou incident de sécurité potentiel, conformément aux procédures internes et dans les meilleurs délais. Il doit également signaler à son manager ou sa hiérarchie toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation. Le groupe a défini un **processus d'escalade clair et documenté** pour ces cas de figure ;
- enfin, les collaborateurs sont sensibilisés au **RGPD** et des procédures pour s'assurer de l'archivage et de la suppression des données personnelles conformément à ce règlement ont été déployées pour toute personne concernée, y compris les clients et partenaires commerciaux. ABC arbitrage supprime les données après une période définie et ne collecte pas de données personnelles auprès de tiers (sauf si la loi l'exige, par exemple pour garantir un dispositif anti-blanchiment d'argent / financement terrorisme robuste, ainsi que décrit dans la politique).

Parmi les mesures d'accompagnement et de sécurisation des usages, qui vise à réduire le risque humain par les procédures et les outils :

- La procédure de **gestion des mouvements de personnel** (arrivées, départs ou mutations) inclut la mise à jour des accès et des droits associés ;
- Les **fonctions / droits d'accès** sont séparés et des validations à 2 niveaux sont en place ;
- Les **postes utilisateurs sont protégés** sur la base des recommandations *Zero Trust*, à savoir : authentification forte et basée sur le contexte, *device posture*, micro-segmentation du réseau et chiffrement des échanges sur le réseau avec *Transport Layer Security* (TLS) et sur les disques du groupe ;
- La **gestion des équipements** de postes utilisateurs repose sur des outils centralisés permettant d'appliquer de manière homogène les politiques de sécurité et d'en assurer le suivi dans le temps ;
- Le groupe a mis en place un **système d'authentification unique (SSO)** qui permet aux utilisateurs d'accéder à plusieurs applications et services à l'aide d'un seul jeu d'identifiants de connexion. Cela permet de réduire les risques liés à la compromission des identifiants et à améliorer le niveau global de sécurité des accès ;
- ABC arbitrage fournit également à chaque employé un **Gestionnaire de Mots de Passe** d'entreprise, utile lorsque les sites tiers ne prennent pas en charge l'authentification unique (SSO).

2.2.3. Au niveau du système d'information

La sécurité du système d'information du groupe repose sur un ensemble de mesures couvrant la gestion des actifs, le contrôle des accès et des identités, la sécurité de l'exploitation, la protection des données, la prévention des menaces et la maîtrise des risques liés aux tiers. Ces dispositifs visent à assurer un niveau de protection cohérent et proportionné aux enjeux du groupe.

La **gestion des actifs informatiques** vise à identifier, classifier et protéger les ressources du système d'information tout au long de leur cycle de vie, en tenant compte de leur sensibilité et des risques associés :

- Les questions de sécurité et de protection sont prises en compte dès la phase d'acquisition de matériel, logiciels et services numériques. Les solutions et prestataires retenus doivent permettre un haut niveau de sécurité informatique, qui soit cohérent avec l'analyse des risques. Le groupe applique ainsi des critères de sélection exigeants des prestataires, pouvant inclure des tests préalables des solutions proposées et des accords de niveau de service (SLA) robustes. Cette attention perdure tout au long du cycle de vie des actifs concernés, y compris lors de leur retrait ou mise hors service ;
- Pour les prestataires critiques, le groupe dispose de prestataires ou solutions de *back-up*. Ces prestataires ou solutions de repli font l'objet d'un suivi afin de s'assurer qu'un basculement puisse être opéré de manière effective en cas de besoin ;
- En cas de sinistre, les parties prenantes concernées, y compris les prestataires de services critiques et les investisseurs, sont informées de manière appropriée de la mise en œuvre des dispositifs de continuité et de reprise. La Direction est responsable de la coordination de ces communications, ainsi que de la mise en place des ajustements nécessaires des flux d'information ou des processus opérationnels, afin d'assurer une information cohérente et en temps utile ;
- Un inventaire précis des systèmes d'information, actifs et applications est établi et régulièrement mis à jour. Leur sensibilité et risque associés sont évalués, afin d'assurer une compréhension correcte des menaces, des vulnérabilités et des impacts potentiels ;
- Les actifs sont protégés par des mesures de sécurité adaptées, efficaces et proportionnées à leur niveau de sensibilité et aux risques identifiés, qui sont régulièrement évalués et ajustés si nécessaire ;
- Une classification Disponibilité / Intégrité / Confidentialité / Preuve (DICP) établit les besoins et priorités de protection sur les actifs les plus sensibles pour déployer des mesures adaptées ;
- L'exposition des actifs sensibles aux risques d'erreur, d'usage non conforme ou de malveillance, qu'elle soit interne ou externe, est soumis à contrôles, aux contrôles des accès et à des mécanismes de prévention et de détection ;
- Des dispositifs sont mis en place afin de garantir la continuité, la récupération et la restauration des actifs sensibles en cas d'incident majeur ou de sinistre, dans des délais compatibles avec les exigences opérationnelles ;
- Le paramétrage et configuration des équipements vise à protéger les utilisateurs et diminuer au maximum les risques en renforçant la configuration et bannissant les protocoles de communications obsolètes ou vecteurs d'infection au profit de ceux recommandés par les agences NIST, NSA et ANSSI ;

- La gestion des serveurs, des plateformes Cloud et réseaux est automatisée rendant une application rapide et à grande échelle des configurations et un meilleur suivi de l'historique.

Les **contrôles des accès et des identités** garantissent que seules les personnes dûment habilitées accèdent aux systèmes, aux données et aux infrastructures, dans des conditions maîtrisées et traçables :

- Les habilitations et accès aux actifs et informations sont accordés selon le "principe de moindre privilège" et en cohérence avec les profils utilisateurs ;
- Les accès et actions réalisées sur les systèmes d'information ou sur les sites sont suivis (traçabilité et imputation) et identifiés de manière formelle et non ambiguë via des comptes *ad personam* ;
- Les bases de données et les plateformes de trading utilisent du matériel appartenant aux sociétés du groupe dans un environnement sécurisé, fonctionnant sur des systèmes privés. Aucun tiers n'est autorisé. L'accès éventuel de tiers dans les locaux est accompagné par une personne habilitée, qui assume la responsabilité de leurs déplacements et agissements ;
- Le recours aux comptes génériques est exceptionnel et dûment motivé, avec une attention particulière et des mesures de sécurité spécifiques ;
- La liste des personnels habilités ou autorisés à accéder à des sites, équipements, applications sécurisées ou données sensibles est régulièrement vérifiée.

La **sécurité de l'exploitation** vise à assurer le fonctionnement fiable, sécurisé et maîtrisé des systèmes d'information, ainsi que la détection et le traitement des incidents opérationnels.

- Le respect des bonnes pratiques est garanti par la formalisation de procédures d'exploitation associées à des responsabilités claires. Les changements font l'objet d'un processus formalisé, incluant une analyse de risque, et d'une validation ;
- Les ressources, traitements informatiques et l'état des infrastructures sous-jacentes sont supervisés pour détecter les anomalies et dysfonctionnements éventuels et pouvoir ainsi les analyser et traiter. En cas d'incident ou de dysfonctionnement, les alertes sont remontées aux équipes ;
- Les matériels et systèmes obsolètes sont identifiés par les référents techniques, qui établissent un plan d'évolution ou de conservation en fonction des risques identifiés.

La **protection des données** repose sur des mesures destinées à garantir leur confidentialité, intégrité, disponibilité et conformité aux exigences réglementaires, tout au long de leur cycle de vie :

- Les moyens de protection de la confidentialité et de l'intégrité des données, y compris sensibles, sont définis en amont grâce à des protocoles et mesures de sécurité spécifiques, tels que - mais non limité à - des protocoles de sécurité, des registres des données, le chiffrement, les certificats électroniques, etc. Ces services sont configurés en respectant les bonnes pratiques recommandées par les organismes agréés (ex : ANSSI) et sont contrôlés dans le temps ;
- Ainsi que décrit dans la politique de gestion des données personnelles, le groupe veille à la protection, la confidentialité, la non altération, la disponibilité et la sécurité des Données personnelles qui lui sont confiées. Il prend l'ensemble des mesures

nécessaires afin de fournir une information claire et transparente sur la collecte et le traitement de ces données et veille à la mise en place de mesures techniques et organisationnelles nécessaires pour les protéger et assurer que leur traitement est conforme à la réglementation applicable ;

- Les données personnelles contenant des Données sensibles peuvent faire l'objet d'un traitement dans des cas très limités et sous conditions strictes (consentement de la personne, données déjà dans le domaine public, traitement essentiel à une action en justice ou explicitement autorisé par la législation nationale).

En sus des mesures précédemment décrites, la **protection contre les malveillances** vise à prévenir, détecter et limiter les impacts des attaques ou comportements susceptibles de compromettre la sécurité des systèmes d'information :

- Tous les équipements sont protégés par une solution antivirale, lorsqu'applicable ;
- Toute connexion distante (sites distants, bureaux extérieurs, tiers, etc.) est authentifiée de manière sûre et réalisée en utilisant une solution permettant le chiffrement des flux ;
- La navigation Internet est contrôlée et journalisée et une liste des sites non autorisés est établie et mise à jour régulièrement. Une procédure exceptionnelle de filtrage est activée en cas de découverte ou d'alerte sur des flux ou sites identifiés comme malveillants ;
- Des analyses quotidiennes des vulnérabilités internes et externes sont réalisées et des tests d'intrusion (*pen-tests*) sont réalisés :
    - tous les jours sur nos ressources exposées à l'extérieur
    - toutes les semaines sur nos ressources internes
    - tous les ans par des auditeurs externes (différents à chaque itération).

Les **relations avec les tiers** sont encadrées afin de maîtriser les risques liés aux accès externes, à l'hébergement ou au traitement d'informations, dans des conditions de sécurité équivalentes aux exigences internes :

- Lors de toute collaboration avec un tiers, les risques sont évalués et l'accès aux tiers n'est autorisé qu'aux environnements utiles à la prestation ;
- Des garanties contractuelles sont systématiquement mises en place, couvrant par exemple l'engagement de responsabilité et de confidentialité, la protection des données, les moyens organisationnels et techniques mis en œuvre, l'audit, les conditions de réversibilité, etc ;
- Afin d'assurer la protection des Données personnelles et ainsi que décrit dans sa Politique de protection des données personnelles, le groupe met en place les sécurités nécessaires avec ses sous-traitants éventuels, notamment via un contrat écrit et un accord de confidentialité spécifique. Il s'assure qu'ils présentent des garanties techniques et organisationnelles appropriées et qu'ils traitent les données conformément à ses exigences et à sa politique de gestion des données à caractère personnel.

2.2.4. Utilisation d'outils d'intelligence artificielle

L'utilisation d'outils d'intelligence artificielle (IA) dans le cadre professionnel est strictement limitée aux usages autorisés par le groupe et s'exerce **dans un environnement contrôlé et**

sécurisé. Elle doit respecter l'ensemble des règles internes, des obligations légales et des principes éthiques applicables. L'Administrateur réseau se réserve la possibilité de mettre en œuvre des mesures de filtrage, de contrôle, de limitation et de traçabilité des usages, afin de garantir la sécurité des systèmes d'information et la conformité des pratiques.

Les utilisateurs ont le devoir (inscrit dans le règlement intérieur et la charte informatique) de **veiller à la préservation de la confidentialité des informations** et, le cas échéant, au respect du secret professionnel, en s'abstenant de saisir dans un outil d'IA toute donnée sensible, stratégique ou confidentielle et en ayant un usage conforme à la réglementation relative à la protection des données à caractère personnel, tant pour les données saisies dans les requêtes que pour les contenus générés. Une vigilance particulière doit également être portée aux enjeux de propriété intellectuelle et au fait que les contenus générés par l'IA restent soumis aux droits d'auteur et aux règles de propriété intellectuelle applicables. Les utilisateurs doivent veiller à ce que l'exploitation (reproduction, diffusion, modification) des contenus ne porte pas atteinte aux droits des tiers.

Les utilisateurs sont expressément informés que les systèmes d'IA sont susceptibles de produire des résultats inexacts, incomplets, biaisés ou erronés. En conséquence, tout contenu généré par une IA doit impérativement faire l'objet d'un **contrôle humain critique, systématique et approfondi** avant toute utilisation, diffusion ou prise de décision. L'IA ne saurait en aucun cas se substituer au jugement, à l'expertise ou à la responsabilité des utilisateurs.

De manière générale, les utilisateurs doivent faire preuve de discernement et de prudence dans l'utilisation de l'IA, respecter les législations en vigueur et signaler toute difficulté ou questionnement. Ils doivent participer aux actions de formation spécifiques à l'usage de l'IA.

2.2.5. Gestion des incidents, continuité et résilience

Le dispositif de résilience du groupe repose sur un ensemble structuré de plans d'intervention, de gestion de crise et de reprise après sinistre, conçus pour faire face aux événements susceptibles d'affecter le fonctionnement normal des activités. Ils ont pour objectif de **limiter les impacts des événements perturbateurs sur la stabilité** opérationnelle du groupe et de préserver sa réputation. Ils définissent un cadre de gouvernance, de prise de décision et de communication adapté aux situations exceptionnelles, permettant une réponse coordonnée et proportionnée.

Ces dispositifs s'inscrivent dans une approche globale de continuité d'activité et font l'objet de revues et d'exercices réguliers afin de garantir leur pertinence et leur efficacité dans le temps.

- Le groupe a mis en place un **Plan de Continuité d'Activité** (PCA ou BCP) et **un Plan de reprise d'activité** (DRP) mais également des Plans de Secours Informatique et de Continuité pour toutes ses lignes d'activités. Ces plans sont conçus pour faire face à tous types de scénarios (malveillances, événements accidentels, sécurité physique, aléas climatiques et environnementaux, intrusion, vols, dégradation, etc.), y compris très improbables. Ils sont fondés sur une analyse des impacts potentiels sur les opérations du groupe. Ils couvrent la gestion de la remontée d'alerte, l'organisation

décisionnelle et opérationnelle, les procédures, les actions de communication, le plan de retour à la normale ;

- Les dispositifs de continuité et de reprise font l'objet de **tests et d'exercices réguliers**, adaptés aux activités concernées et réalisés au minimum sur une base annuelle sur les environnements les plus critiques, afin d'en vérifier l'efficacité opérationnelle ;
- La **protection est adaptée aux exigences de disponibilité** des équipements, locaux et servitudes indispensables au fonctionnement des systèmes d'information et au risque encouru. Par exemple, elle est calibrée pour les besoins en termes de Délai Maximal d'Indisponibilité Admissible (DMIA) et de Pertes de Données Maximales Acceptables (PDMA). La conception de l'architecture intègre la continuité de service et l'ensemble des équipements matériels est redondant afin d'éviter toute perturbation majeure en cas de défaillance et faciliter la continuité ou la reprise des activités critiques en cas d'incident ;
- L'organisation et les moyens mobilisés sont pensés pour limiter l'impact des chocs, susceptibles de perturber ou d'interrompre le fonctionnement normal des ressources du SI ;
- Le système d'information fait l'objet d'une surveillance visant à détecter d'éventuels incidents de cybersécurité. Les **événements d'audit et la télémétrie des systèmes et réseaux sont centralisés** et des alertes sont émises en cas de franchissement de seuil ou d'avarie. Les enregistrements critiques sont protégés. En sus des mécanismes automatiques d'alerte, les utilisateurs ont l'obligation de signaler toute anomalie de sécurité ;
- Des **indicateurs** permettent de recenser et caractériser les atteintes à la sécurité de l'information et à la cybersécurité (origine, impact, etc.) ;
- L'ensemble des équipements matériels fait l'objet de **contrats de maintenance**, dont une large majorité prévoit une assistance 24h/24 avec un délai d'intervention ou de remplacement garanti ;
- Un **processus de traitement des infections et d'application des correctifs** de sécurité est défini pour tous les composants du SI et connu des référents techniques. Des procédures d'urgence sont prévues en cas d'alerte critique. Les évènements d'infection sont suivis et font l'objet de reporting et d'analyse ;
- En cas d'avarie ou d'incident, une **cellule de gestion de crise est activée** selon une gouvernance définie, afin de qualifier la situation et de coordonner les décisions et actions à mettre en œuvre. L'analyse des incidents de sécurité donne lieu à un plan d'action (actions préventives et curatives) permettant d'améliorer les mesures existantes ou d'en créer de nouvelles.
- En cas d'incident, des **contrôles et vérifications** appropriés sont réalisés afin d'assurer l'intégrité et la cohérence des données, préalablement à la remise en fonctionnement complète des systèmes, y compris pour les données reconstruites.

3. Suivi, contrôle et amélioration continue

Le groupe est engagé dans une **démarche d'amélioration continue** sur ces sujets : des contrôles et évaluations réguliers, internes et / ou externes, sont réalisés afin d'apprécier l'efficacité globale du dispositif et d'identifier les axes d'amélioration. Le référentiel et les

règles de sécurité du groupe sont revues et mis à jour au moins une fois par an ou à chaque événement pertinent et *a minima* en cas d'évolution de l'activité, de changement organisationnel important ou d'évolution de l'environnement technique ou règlementaire, ainsi qu'en retour d'expérience des traitements d'incidents.

Le groupe contrôle régulièrement l'efficacité de sa stratégie de protection et de résilience opérationnelle numérique. À cet effet, l'équipe technique veille au maintien de l'état de l'art des technologies et des pratiques, tout en assurant une veille active sur les nouvelles menaces et vulnérabilités.

Un système d'alerte anonyme est mis en place pour permettre aux employés et aux tiers de signaler toute suspicion de dysfonctionnement sans risque de représailles. Toute personne qui le juge nécessaire peut lancer une alerte via l'adresse mail lanceurdalerteabc@gmail.com ou par courrier, à l'adresse 18, rue du 4 septembre, 75002 Paris. Une information de la bonne réception du signalement ainsi que du délai raisonnable et prévisible nécessaire quant à l'examen de sa recevabilité et des modalités pour les suites données au signalement lui sera apportée dans les meilleurs délais. Dans le cas d'un courrier anonyme, aucune confirmation de réception ou information sur les suites données ne pourra être transmise à l'émetteur. Les signalements font l'objet d'un traitement selon une procédure formalisée, garantissant leur analyse, leur suivi, ainsi que la mise en œuvre de mesures correctives ou disciplinaires appropriées en cas de manquement avéré. Tous les détails sont disponibles dans la procédure publique dédiée.