Annexe de Sécurité Monext

Référence	:	SEC/STD/201709-01
Date	:	27/08/2019
Version/Édition	:	1M
Classification	:	C0 (Publique)

Suivi du document

Date	Modifications	Pages / Chapitres	Edition / Révision
12/09/2017	Création du document	Tous	1A
07/12/2017	Modification du document	§1 ;§2 ;§9.1.10 ; §10.1.1	1B
13/12/2017	Modification du document	§12	1C
05/12/2018	Modification du document	Toutes	1D
20/02/18	Refonte du document	Toutes	1E
23/02/18	Ajout chapitre 1	1	1F
06/03/2018	Ajout de plusieurs parties + modifications du document	Toutes	1G
16/03/2018	Réorganisation des différents points	Toutes	1H
26/03/2018	Reformulation et correction partie Crypto	12	1I
26/03/2018	Relecture Classification des informations et des données	16	1J
27/03/2018	Modification partie Crypto	15	1K
07/02/2019	Modification du document	Toutes	1L
27/08/2019	Relecture et modification de syntaxe	Toutes	1M

TABLE DES MATIERES

1 Politique Globale de Sécurité du Système d'Information [PGSI]

La Politique Globale de Sécurité de l'Information établit les orientations générales dans lesquelles doivent être conduites l'identification, la réduction et la gestion des risques encourus par Monext.

La PGSI, accessible à tous les collaborateurs sur l'Intranet Monext, est basée sur une analyse de risques annuelle du métier de Monext, sur les bonnes pratiques ISO 27001 et sur la prise en compte du règlement GDPR.

La PGSI, revue chaque année, s'impose à chaque collaborateur de Monext ainsi que les employés temporaires, consultants et prestataires.

De ces orientations générales découlent divers documents consignant les procédures, règles, consignes et recommandations opérationnelles, réparties éventuellement par domaines spécialisés comme par exemple les règles relatives à la sécurité physique, les guides de développement, les guides de sécurité réseaux …

Les objectifs de Sécurité des Informations de Monext sont la préservation de quatre valeurs essentielles :

- **La confiance externe :** la confiance externe nous est accordée tant par clients que par les administrations, les institutions nationales et internationales avec lesquelles nous sommes en relation. Elle est le reflet de la perception que ces acteurs ont de notre aptitude à respecter nos valeurs affichées.
- **Le respect de la législation et de la réglementation :** au-delà même des obligations légales, ou des exigences professionnelles inhérentes à l'exercice de nos métiers, le respect de la législation et de la réglementation est une des valeurs qui doit guider le comportement de Monext.
- **La confiance interne :** la confiance interne nous est accordée par nos administrateurs, nos collaborateurs et nos partenaires. Elle est le reflet de la perception que ces acteurs ont de notre aptitude à respecter les valeurs internes affichées par Monext.
- **La valeur économique :** l'efficience économique est le garant de notre développement, de notre indépendance et de notre pérennité.

Dans le cadre de son métier, Monext se conforme aux règles de l'art et par conséquent sur son activité Monétique respectant le standard PCI DSS sur lequel Monext est audité chaque année pour prouver sa conformité.

De plus, Monext manipulant, dans le cadre de ses activités, des données identitaires et financières de ses clients et des clients de ses clients, applique la règlementation en vigueur en matière de protection des données personnelles.

MONEXT s'engage à ne pas effectuer d'actions qui porteraient volontairement atteinte ou qui compromettraient l'exploitation-même temporaire du système d'information de son client, de son patrimoine informationnel et des données.

2 Système de gestion de la sécurité de l'information [SMSI]

[SMSI] 1	Monext a basé sa politique de sécurité sur la déclinaison opérationnelle des normes ISO 270xx et du standard PCI DSS. Cette politique est enrichie des différentes exigences de sécurité règlementaires.
[SMSI] 2	La Sécurité de l'Information utilise quatre attributs normalisés (DICP : la disponibilité, l'intégrité, la confidentialité et la traçabilité des preuves) sur lesquels s'expriment les niveaux de sécurité atteints ou les altérations provoquées sur les Composants Systèmes d'Information.
[SMSI] 3	La mise en œuvre au quotidien est pilotée par l'équipe en charge de la sécurité et sous le contrôle du RSSI de l'entreprise. Le périmètre de la SMSI Monext prend en compte l'ensemble des prestations réalisées pour nos clients ainsi que l'ensemble des services transverses permettant de garantir le respect des quatre exigences de sécurité (la disponibilité, l'intégrité, la confidentialité et la traçabilité des preuves).
[SMSI] 4	Chaque prestation fait l'objet d'une analyse de risque basée sur le respect des critères DICP et est intégrée dans l'outil PRDC (Processus, Risque, Dispositif et Contrôle) qui assure le fonctionnement selon le principe du PDCA (Plan, Do, Check et Act) pour garantir l'amélioration constante de nos différents processus métiers.
[SMSI] 5	La création de fiches de traitements et registres ainsi que la mise en œuvre d'analyses de risques ont été réalisées dans le cadre de la réglementation RGPD.
[SMSI] 6	Un outil de veille en matière de sécurité est mis en place (XMCO). Il génère des alertes mails permettant aux collaborateurs d'accéder rapidement aux contenus intéressants dans le cadre des activités de Monext et de leur service.
[SMSI] 7	Un outil de cyber surveillance est mis en place.

3 Authentifier les utilisateurs [AUTH]

[AUTH] 1	Identifiant unique par utilisateur et interdiction d'utiliser des comptes partagés entre plusieurs utilisateurs.
[AUTH] 2	Authentification forte avec mot de passe complexe pour les accès en production.
[AUTH] 3	Limiter le nombre de tentatives d'accès aux comptes utilisateurs sur les postes de travail et bloquer le compte lorsque la limite est atteinte.
[AUTH] 4	Imposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable.
[AUTH] 5	Moyens techniques pour faire respecter les règles relatives à l'authentification **:** blocage du compte en cas de non renouvellement du mot de passe.
[AUTH] 6	Les identifiants (ou logins) des utilisateurs ne sont pas ceux des comptes définis par défaut par les éditeurs de logiciels et désactiver les comptes par défaut.
[AUTH] 7	Utiliser un gestionnaire de mot de passe pour avoir des mots de passe différents pour chaque service, tout en ne retenant qu'un mot de passe maître.
[AUTH] 8	Stocker les mots de passe de façon sécurisée.
[AUTH] 9	Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.
[AUTH] 10	Les utilisateurs suivent les pratiques de l'organisation pour l'utilisation des informations secrètes d'authentification.

4 Gérer les habilitations [HAB]

[HAB] 1	Une politique traite la gestion des droits d'accès aux systèmes et aux différentes interfaces. Des niveaux d'habilitation différenciés sont mis en place : attribution des permissions et attribution des rôles selon la fonction métier de chaque collaborateur.
[HAB] 2	Mise en place de profils d'habilitation dans les systèmes en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions.
[HAB] 3	Une revue annuelle des habilitations est réalisée afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.
[HAB] 4	Mise à jour régulière de la politique de contrôle des accès.
[HAB] 5	Les tâches et les domaines de responsabilités incompatibles sont cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.

5 Tracer les accès [ACC]

[ACC] 1	Appliquer les procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).
[ACC] 2	Mise en place d'un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « *logs* ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité.
[ACC] 3	Les accès aux traces sont restreints aux équipes dont la mission le justifie.
[ACC] 4	Un outil de contrôle d'intégrité est déployé sur le serveur de log centralisé. L'objectif est de détecter des modifications non autorisées des fichiers de traces centralisés.
[ACC] 5	Une procédure assure que les gestionnaires du dispositif de gestion des traces notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable de traitement.
[ACC] 6	Les fichiers journaux sont conservés pendant une durée de un an (dont au moins 3 mois en ligne).

6 Gérer les incidents [INC]

[INC] 1	Nous entendons par vulnérabilité ou faille de sécurité, toute faiblesse dans un système permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.
[INC] 2	Nous entendons par incident de Sécurité SI tout évènement qui va porter atteinte à la *disponibilité, à la confidentialité et/ou à l'intégrité* du Système d'Information de Monext.
[INC] 3	Les incidents liés à la sécurité de l'information sont traités conformément à l'IRP (Incidence Response Plan). Nous distinguons 3 filières : **F0** : les événements de sécurité qui sont suivis dans le cadre de l'activité surveillance du système d'information **F1** : les événements significatifs et/ou vulnérabilités qui sont suivis dans le cadre de plans d'action sécurité **F2** : les vulnérabilités critiques et/ou présentant un risque imminent et les incidents avérés qui sont suivi dans le cadre du processus de gestion des incidents de production
[INC] 4	L'équipe sécurité assure une surveillance du SI supplémentaire aux outils de détection déjà en place.
[INC] 5	Les incidents de filières F2 sont déclarés dans l'outil interne de gestion des incidents. Une priorité est précisée.
[INC] 6	La gestion d'incident de sécurité suit la méthodologie du CERT SG selon 6 étapes décrites dans l'IRP : - Préparation : Etre prêt à faire face à un incident. - Identification : Détecter l'incident. - Endiguement : Limiter l'impact de l'incident. - Remédiation : Supprimer la menace. - Restauration : Revenir à un état normal. - REX : Synthèse de l'incident et propositions d'améliorations / évolutions.
[INC] 7	La communication des incidents de sécurité est assurée dans le cadre de la communication des incidents de production.
[INC] 8	La violation de données avérée au sens RGPD donne lieu à la génération d'une notification.
[INC] 9	Des actions spécifiques et nécessaires afin de préserver les preuves sont prévues et décrites dans l'IRP MONEXT.
[INC] 10	Les connaissances recueillies suite à l'analyse et la résolution d'incidents sont utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.
[INC] 11	En cas de compromission d'un poste, rechercher la source ainsi que toute trace d'intrusion dans le système d'information de l'organisme, pour détecter la compromission d'autres éléments.
[INC] 12	Diffusion à tous les utilisateurs de la conduite à tenir et de la liste des personnes à contacter en cas d'incidents de sécurité ou de survenance d'un évènement inhabituel touchant aux systèmes d'information.

7 Sécuriser les postes de travail [BUR]

[BUR] 1	Chiffrement des postes de travail.
[BUR] 2	Mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.
[BUR] 3	Mise en place d'un « pare-feu » (« *firewall* ») logiciel, et limitation de l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.
[BUR] 4	Utilisation d'antivirus régulièrement mis à jour et mise en place d'une politique de mise à jour régulière des logiciels. Configuration des logiciels pour que les mises à jour de sécurité se fassent automatiquement dès que cela est possible.
[BUR] 5	Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation.
[BUR] 6	Limiter l'usage d'applications nécessitant des droits de niveau administrateur pour leur exécution.
[BUR] 7	Effacer de façon sécurisée les données présentes sur un poste préalablement à sa réaffectation à une autre personne.
[BUR] 8	Veille de sécurité sur les logiciels et matériels utilisés dans notre système d'information.
[BUR] 9	Installation des mises à jour critiques des systèmes d'exploitation sans délai en programmant une vérification automatique hebdomadaire.
[BUR] 10	Les utilisateurs s'assurent que les matériels non surveillés sont dotés d'une protection appropriée.
[BUR] 11	Des règles régissant l'installation de logiciels par les utilisateurs concernés sont établies et mises en œuvre. Un répertoire dédié aux logiciels autorisés est mis en place pour les utilisateurs non concernés. Il est interdit de télécharger et d'exécuter des applications téléchargées ne provenant pas de sources sûres.

8 Sécuriser l'informatique mobile [SEC-MOB]

[SEC-MOB] 1	Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles (ex : vol de matériel) et aux procédures prévues pour les limiter.
[SEC-MOB] 2	Mise en œuvre de mécanismes maîtrisés de sauvegardes ou de synchronisation des postes nomades, pour se prémunir contre la disparition des données stockées.
[SEC-MOB] 3	La connexion des supports mobiles (clés USB, disques durs externes …) est limitée à l'indispensable.
[SEC-MOB] 4	Concernant les *Smartphones*, en plus du code PIN de la carte SIM, activer le verrouillage automatique du terminal et exiger un secret pour le déverrouiller (mot de passe, schéma, etc.).
[SEC-MOB] 5	Concernant les *Smartphones*, quatre autres règles élémentaires sont mises en place : chiffrement du téléphone, mise à jour du système, interdiction de « jail-break » ou root sur le téléphone et téléchargement d'application seulement depuis les plateformes adéquates et officielles (Play-Store ou App Store).

9 Protéger le réseau informatique interne [RES]

[RES] 1	Limiter les accès Internet en bloquant les services non nécessaires et qui peuvent faire courir un risque à la sécurité de notre SI.
[RES] 2	Les responsabilités en termes d'administration des équipements réseau et sécurité (en particulier des firewalls) sont formellement assignés. Les équipements réseau sont administrés via des protocoles chiffrés (ssh, https ...).
[RES] 3	Les serveurs de production sont positionnés dans des VLANs dédiés et isolés du reste du réseau. Ils sont protégés par des firewalls qui filtrent finement toutes les connexions entrantes et sortantes : avec Internet et avec le reste du réseau. Les serveurs frontaux qui ont vocation à être accessibles depuis Internet sont positionnés dans une DMZ.
[RES] 4	Gestion des réseaux Wi-Fi avec utilisation d'un chiffrement à l'aide d'un mot de passe complexe. Les réseaux ouverts aux invités sont séparés du réseau interne. Des scans des réseaux sans fil visant à détecter des Access Point sans fil autorisés et non autorisés sont réalisés sur tous les sites notamment dans les zones sensibles que sont les datacenters.
[RES] 5	Imposer un VPN pour l'accès à distance ainsi que une authentification forte de l'utilisateur.
[RES] 6	Aucune interface d'administration n'est accessible directement depuis Internet. La télémaintenance doit s'effectuer à travers un VPN.
[RES] 7	Le trafic réseau est monitoré par une sonde IDS.
[RES] 8	Des périmètres de sécurité sont définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.
[RES] 9	Les exigences liées à la sécurité de l'information sont intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants.
[RES] 10	Les informations liées aux services d'application transmises sur les réseaux publics sont protégées.
[RES] 11	Mise en place d'un système prévenant des dénis de services.

10 Sécuriser les serveurs [SERV]

[SERV] 1	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées.
[SERV] 2	Utiliser des comptes de moindres privilèges pour les opérations courantes.
[SERV] 3	Politique spécifique de mots de passe pour les administrateurs avec changement des mots de passe, au moins lors de chaque départ d'un administrateur et en cas de suspicion de compromission.
[SERV] 4	Installation des mises à jour critiques sans délai que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire.
[SERV] 5	Les scripts de contrôle de conformité par rapport à nos standards de sécurité sont exécutés mensuellement, sur tous les serveurs de production.
[SERV] 6	Les accès distant aux environnements de production réalisés depuis l'extérieur du SI intègrent une authentification à double facteur.
[SERV] 7	Des scans de vulnérabilités sont réalisés mensuellement afin de détecter d'éventuelles failles de sécurité. Des scans ASV sont obligatoires par le standard PCI-DSS.
[SERV] 8	Des tests d'intrusion sont régulièrement opérés par des tiers experts en sécurité offensive sur notre SI.
[SERV] 9	Un outil de File Integrity Monitoring contrôle régulièrement tous les serveurs de production du SI (OSSEC).
[SERV] 10	Réception d'alerte à chaque fois qu'un équipement est « infecté », qu'une alarme anti-malware est émise ou qu'une définition d'anti-malware n'est pas à jour. Le suivi est assuré jusqu'à la résolution.
[SERV] 11	Des programmes de test de conformité et des critères associés sont déterminés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.

11 Sauvegarder et prévoir la continuité d'activité [PCA]

[PCA] 1	Réalisation de sauvegardes fréquentes des données, que celles-ci soient sous forme papier ou électronique. 3 politiques de sauvegardes génériques sont utilisées : totale mensuelle, totale hebdomadaire et incrémentale quotidienne. Ces sauvegardes sont conservées pendant une durée de 13 mois.
[PCA] 2	Stocker les sauvegardes sur un site extérieur.
[PCA] 3	Protéger les données sauvegardées sur disque et chiffrées.
[PCA] 4	S'agissant de la reprise et de la continuité d'activité, un plan de reprise et de continuité d'activité informatique est rédigé, incluant la liste des profils intervenants.
[PCA] 5	Tester régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité quand le dispositif est prévu.
[PCA] 6	Tous les composants des matériels contenant des supports de stockage sont vérifiés pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant leur mise au rebut ou leur réutilisation.

12 Sécuriser les échanges [SEC- ECHG]

[SEC- ECHG] 1	Les flux entrants et sortants qui contiennent des données sensibles sont chiffrés. Dans le cadre de ses activités monétiques, le PAN est chiffré.
[SEC- ECHG] 2	Les protocoles garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers sont SFTP, HTTPS et FTPS.
[SEC- ECHG] 3	Les logiciels en charge du chiffrement autorisés sont : OpenSSL et OpenSSH.
[SEC- ECHG] 4	La confidentialité des secrets (clé de chiffrement, mot de passe, etc.) est assurée en les transmettant via un canal distinct.
[SEC- ECHG] 5	Il est interdit d'envoyer des données sensibles en clair par email, messagerie instantanée, chat, SMS, ou autres technologies de messagerie.
[SEC-ECHG] 6	Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications est contrôlé par une procédure de connexion sécurisée.
[SEC-ECHG] 7	Des mesures de transfert formelles sont mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.
[SEC-ECHG] 8	L'information transitant par la messagerie électronique est protégée selon la classification.
[SEC-ECHG] 9	Lors de la réception d'un certificat électronique, celui-ci doit contenir une indication d'usage conforme à ce qui est attendu, être valide et non révoqué, et posséder une chaîne de certification correcte à tous les niveaux.

13 Protéger les locaux [SEC-PHY]

[SEC-PHY] 1	L'ensemble des accès et l'ensemble des issues de secours sont placés sous protection d'un système de détection d'intrusion et un système de vidéo protection 24h/24h. Une vérification périodique est prévue.
[SEC-PHY] 2	Un système d'alarme incendie fonctionne en permanence sur les sites. La procédure d'évacuation en cas d'incendie est portée à la connaissance de tous les collaborateurs. Des exercices de mise en situation sont organisés annuellement. Les sites Monext sont situés en zones non-inondables.
[SEC-PHY] 3	Distinction des zones des bâtiments selon les risques.
[SEC-PHY] 4	L'historique des passages est enregistré pour garantir la traçabilité des accès.
[SEC-PHY] 5	Une procédure de gestion des visiteurs est en place.
[SEC-PHY] 6	Les remontées d'alertes (tentative d'accès à des salles non autorisées ou à des salles autorisées hors horaires spécifiés, etc.) sont loguées et stockées.
[SEC-PHY] 7	Protection physique des matériels informatiques par des moyens spécifiques (système anti-incendie dédié, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation, etc.).

14 Encadrer les développements informatiques [DEV]

[DEV] 1	Les développements et les tests sont dans des environnements informatiques distincts de celui de la production et sur des données fictives ou anonymisées.
[DEV] 2	Les exigences de sécurité des données (DICP) sont intégrées dès la conception de l'application ou du service. Ces exigences peuvent se traduire par des choix d'architecture de fonctionnalités …
[DEV] 3	Éviter le recours à des zones de texte libre ou de commentaires.
[DEV] 4	Un guide général de développement donne les orientations sur la manière de développer. Le code produit respecte les politiques de gestion des Logs, de gestion des identités et des mots de passe et de gestion des correctifs de sécurité.
[DEV] 5	Les développeurs sont formés annuellement aux techniques de développement sécurisé notamment à l'OWASP.
[DEV] 6	Les données et les comptes de test sont systématiquement supprimés avant toute livraison en production.
[DEV] 7	Mise en place d'un outil de mesure de la qualité du code en continue (SonarQube).

15 Chiffrer, garantir l'intégrité ou signer [CRYPTO]

[CRYPTO] 1	Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information est élaborée et mise en œuvre.
[CRYPTO] 2	Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques est élaborée et mise en œuvre tout au long de leur cycle de vie.
[CRYPTO] 3	Le chiffrement des données sensibles est réalisé via des clefs de chiffrement de données.
[CRYPTO] 4	Les clés secrètes sont protégées : mise en œuvre de droits d'accès restrictifs et mot de passe sûr.
[CRYPTO] 5	Les collaborateurs habilités à manipuler les clefs de chiffrements (maîtres des clefs) signent un formulaire spécifique par lequel ils reconnaissent avoir pris connaissance et accepter leurs responsabilités.

16 Classification des informations et des données [CLASSIF]

[CLASSIF] 1	Tout document porte la mention de son classement sur chacune de ses pages. Aucun document ne pourra être considéré comme validé et donc comme diffusable sans cette mention. Par défaut le niveau de classification défini au sein de Monext est le niveau C2 « restreint ».
[CLASSIF] 2	**C4 Sécrète** : Ces données ou fichiers contiennent des informations qui présentent un caractère stratégique pour Monext, et dont la diffusion non contrôlée peut nuire à leur image ou à leur sécurité. Elles nécessitent un contrôle de leur diffusion et la mise en place de moyens de sécurité en regard avec leur sensibilité. Leur confidentialité doit être garantie par l'ensemble de leurs destinataires.
[CLASSIF] 3	**C3 Confidentielle :** Ces données contiennent des informations qui présentent un caractère sensible pour Monext, et dont la diffusion non contrôlée peut nuire à leur image ou à leur sécurité. Elles nécessitent un contrôle de leur diffusion. Leur confidentialité doit être garantie par l'ensemble de leurs destinataires.
[CLASSIF] 4	**C2 Restreinte :** Ces données contiennent des informations importantes Monext, et dont la diffusion non contrôlée peut nuire à leur image ou à leur sécurité. Elles nécessitent un contrôle de leur diffusion.
[CLASSIF] 5	**C1 Interne :** Ces données ou fichiers contiennent des informations importantes pour Monext qui nécessitent un contrôle de leur diffusion. Leur divulgation ne saurait cependant porter préjudice à leur image de marque ou à leur sécurité. Il s'agit des documents internes à l'organisation. Ces derniers ne doivent pas être communiqués en externe sans motif valable.
[CLASSIF] 6	**C0 Publique :** Ces données ont vocation à être diffusées à un large public, sans restriction particulière. Il s'agit notamment des informations disponibles sur Internet, dans des conférences ouvertes, etc. Information rendue publique après autorisation d'une entité habilitée à communiquer à l'extérieur du Groupe.
[CLASSIF] 7	Les exigences en matière d'engagements de confidentialité ou de non-divulgation, sont identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation.

17 Sécuriser les actifs [ACT]

[ACT] 1	Les accords contractuels avec les salariés et les sous-traitants précisent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.
[ACT] 2	Les règles d'utilisation correcte de l'information, les actifs associés à l'information et les moyens de traitement de l'information sont identifiés, documentés et mis en œuvre.
[ACT] 3	Tous les collaborateurs restituent la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord.
[ACT] 4	Les propriétaires d'actifs vérifient les droits d'accès des utilisateurs à intervalles réguliers.
[ACT] 5	Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.
[ACT] 6	Les matériels sont entretenus correctement pour garantir leur disponibilité permanente et leur intégrité.
[ACT] 7	Les matériels, les informations ou les logiciels des locaux de l'organisation ne sortent pas sans autorisation préalable.
[ACT] 8	Des mesures de sécurité sont appliquées aux matériels utilisés hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.
[ACT] 9	S'assurer que les salariés et les sous-traitants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

18 Sécuriser les fournisseurs [FOU]

[FOU] 1	Politique de gestion des fournisseurs qui établit la liste des fournisseurs essentiels.
[FOU] 2	Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisation doivent être acceptées par le fournisseur et documentées.
[FOU] 3	Les exigences applicables liées à la sécurité de l'information sont établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker ou communiquer des données du système d'information.
[FOU] 4	Les accords conclus avec les fournisseurs essentiels incluent des exigences sur le traitement des risques liés à la sécurité de l'information associé à la chaîne d'approvisionnement des produits et des services informatiques.
[FOU] 5	Les organisations surveillent, vérifient et audite à intervalles réguliers la prestation des services assurés par les fournisseurs essentiels.
[FOU] 6	Les changements effectués dans les prestations de service des fournisseurs, comprenant le sont gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques.

19 Sensibiliser les collaborateurs [RH]

[RH] 1	Effectuer une sélection préalable à l'embauche du personnel (ces contrôles peuvent inclure par exemple, les antécédents professionnels et le casier judiciaire). Les collaborateurs signent un accord de confidentialité.
[RH] 2	Processus formalisé de départ d'un collaborateur pour la suppression des accès physique et logiques, et remise des matériels.
[RH] 3	Tous les collaborateurs font l'objet d'une sensibilisation à la sécurité du SI, et sur le RGPD au moment du recrutement et une fois par an.
[RH] 4	Tous les collaborateurs intervenant sur le SI Monext ont pris connaissance du Règlement Intérieur, de la Charte de sécurité informatique et de la clause de confidentialité des contrats.
[RH] 5	Contrôle de l'application des mesures et consignes de sécurité pour l'ensemble des collaborateurs.