Informatique de groupe **AM_IT_PO_002_01**	**ArcelorMittal** **Politique de cybersécurité**	ArcelorMittal

Informations sur le document

Brève description:

L'objectif de cette politique est de détailler la mise en place d'un programme de sécurité des systèmes d'information (ISSP) par le département informatique d'ArcelorMittal afin d'aligner en permanence la protection des systèmes d'information de l'organisation pour faire face aux risques de cybersécurité pertinents.

Scope:

Cette politique s'applique à tous les employés d'ArcelorMittal qui peuvent avoir accès aux systèmes d'information d'ArcelorMittal (y compris les sous-traitants) ; et à toutes les parties prenantes impliquées dans la gestion, la propriété et l'utilisation des systèmes d'information ArcelorMittal.

Propriétaires d'entreprise: Legrand Herve Auteur (préparé par): Lacaille Hugues	Date de création: 01/01/2013 Date de révision: 24/03/2020 Dernière révision le 16/06/2021 pour traduction en Français
	Date de mise en œuvre: 01/01/2013

Documents de référence

Reference ou date	Titre
AM_CC_PO_004_01	Politique de protection des données
AM_CC_PR_009_01	Procédure de protection des données

Validation

Validé par	Position	Date de validation
VAN LELYVELD ANDREW	Global IT Services & Security	05/03/2020

Approbation

Approuvé par	Position	Date d'approbation
LEGRAND HERVE	Group CIO & Group CISO	05/03/2020

1 Objectif

L'objectif de cette politique est de détailler la mise en place d'un programme de sécurité des systèmes d'information (ISSP) par le département informatique d'ArcelorMittal afin d'aligner en permanence la protection des systèmes d'information de l'organisation pour faire face aux risques de cybersécurité pertinents. Les rôles et les responsabilités sont définis pour appuyer la planification, la mise en œuvre et la mise à l'essai de l'ISPP. Un cycle d'amélioration continue garantira que le ISPP est maintenu aligné sur les menaces changeantes à la sécurité de l'information. L'ISPP met l'accent sur la protection des systèmes d'information contre la divulgation à des utilisateurs non autorisés (confidentialité), la modification inappropriée (intégrité) et le non-accès au besoin (disponibilité) :

La confidentialité signifie la préservation des restrictions autorisées à l'accès et à la divulgation, y compris les moyens de protéger la vie privée et les renseignements exclusifs;

- L'intégrité signifie se prémunir contre la modification ou la destruction inappropriées des informations, et comprend la non-répudiation et l'authenticité des informations;
- La disponibilité signifie assurer un accès rapide et fiable à l'information et son utilisation.

Avec l'importance croissante du traitement automatisé de l'information, la Politique sur la sécurité des TI est une condition nécessaire pour atteindre un niveau acceptable de sécurité de l'information :

- La sécurité de l'information concerne le contrôle de tous les actifs d'information de l'entreprise (pas seulement sur le support électronique);
- La sécurité informatique porte sur la composante informatique essentielle de la sécurité de l'information (création de plateformes IT sécuritaires et fiables).

2 SCOPE

La politique s'applique:

- À tous les employés d'ArcelorMittal qui peuvent avoir accès aux systèmes d'information ArcelorMittal (y compris les entrepreneurs à temps plein, à temps partiel);
- À toutes les parties prenantes impliquées dans la gestion, la propriété et l'utilisation des systèmes d'information ArcelorMittal.

La politique ne couvre pas directement les risques de sécurité de l'information liés au traitement manuel de l'information par l'utilisateur et s'appuie sur les principes de la gestion de la sécurité physique chez ArcelorMittal.

3 DEFINITIONS

Les composants et les principes sous-jacents de l'ISSP à ArcelorMittal sont les suivants ::

3.1 ArcelorMittal Cyber-Security Framework

Sur la base du cadre de cybersécurité standard du NIST (https://www.nist.gov/cyberframework), nous avons conçu notre propre cadre de cybersécurité aligné sur nos exigences légales et nos principaux risques commerciaux:

- **Partie conformité**: Nous avons défini un ensemble de contrôles de sécurité informatique de base requis pour mettre en place un niveau de protection de sécurité minimale contre les risques courants de cybersécurité (afin d'éviter les problèmes courants de confidentialité, d'intégrité et de disponibilité) et pour soutenir la conformité à nos exigences légales mondiales (fondement des exigences SOx et GDPR).

  Ils se composent des contrôles de sécurité de base que toutes les unités d'ArcelorMittal doivent intégrer dans leurs solutions et services informatiques. Les sites ArcelorMittal qui ne sont pas conformes aux exigences du cadre de sécurité informatique de base ne seront pas autorisés à se connecter / rester connectés au réseau mondial ArcelorMittal. La procédure de protection des données d'ArcelorMittal sur la mise en œuvre des exigences du règlement général de l'UE sur la protection des données (« GDPR») fait également référence aux contrôles de sécurité informatique de base, ce qui fait que le respect des contrôles de sécurité de base est une obligation légale.

La conformité aux contrôles de sécurité des IT de base doit être évaluée régulièrement (annuellement). Les contrôles de sécurité des IT de base sont examinés et mis à jour régulièrement (au besoin) pour s'assurer qu'ils continuent de faire face aux menaces les plus importantes à la sécurité.

L'évolution des contrôles de sécurité des IT de base requis est guidée par l'objectif de mettre en place une sécurité de l'information minimale efficace dans l'ensemble du groupe ArcelorMittal, tout en tenant compte de l'efficacité de la prestation des applications opérationnelles et des services IT. Les contrôles de sécurité des IT de base reposent sur le principe selon lequel toutes les données et applications se voient attribuer un propriétaire qui peut prendre des décisions quant à la personne à qui devrait pouvoir y accéder. Étant donné que cette décision est une décision d'entreprise, le propriétaire doit être de l'entreprise et posséder une bonne connaissance des processus d'entreprise et des données.

- **Partie basée sur les risques**: Sélection des meilleures pratiques internes et externes proposées pour améliorer notre niveau de maturité par rapport à nos principaux risques commerciaux : espionnage (risque de confidentialité : divulgation de nos secrets commerciaux, de nos propriétés intellectuelles ou de tout autre actif d'information sensible) et sabotage (risque de disponibilité : incapacité de nos outils de production à fonctionner comme prévu).

  Au-delà des contrôles de sécurité informatique de base couramment requis, chaque entité ArcelorMittal (site, unité, segment...) peuvent avoir besoin de mesures de cybersécurité supplémentaires pour atteindre un niveau de protection acceptable adapté à leur propre contexte. Un questionnaire d'évaluation de la maturité est utilisé pour évaluer leur posture actuelle en matière de cybersécurité et pour les comparer avec leurs pairs internes et externes ou avec leurs objectifs actuels et futurs. Les lacunes détectées sont utilisées pour proposer des priorités en matière d'assainissement et les pratiques exemplaires internes et externes connexes..

3.2. Autoévaluations et vérifications de la maturité en matière de cybersécurité

L'analyse comparative interne et externe est un aspect important pour réfléchir à nos mesures de cybersécurité déployées et les maintenir à un bon niveau de maturité. Des auto-évaluations et des audits sont effectués régulièrement pour comparer (interne et externe) notre niveau de maturité en matière de cybersécurité pour les segments et pour le groupe. Ces auto-évaluations et audits comprennent l'informatique (technologie de l'information) et l'OT (technologie des opérations), sont lancés et dirigés par le bureau CISO du groupe et coordonnés par les agents de sécurité du segment pour leurs segments spécifiques. Les agents de sécurité sectoriels communiquent les résultats sectoriels aux comités de gestion sectoriels applicables. Les résultats combinés de l'audit et des autoévaluations sont communiqués au comité de gestion du groupe et au comité d'audit par le bureau CISO du groupe.

3.3 Contrôles généraux SOX IT

La protection de l'intégrité de l'information financière est un exemple typique d'environnement nécessitant des contrôles de sécurité de niveau supérieur. Ces contrôles ont été définis au niveau du groupe dans le cadre des contrôles généraux des IT SOx. Le cadre est complété par des procédures décrivant les exigences en matière de collecte et d'essai de preuves imposées par la directive sur les SOx.

3.4 Gestion de projet

Les risques de sécurité informatique et les exigences de conformité, y compris le traitement des données personnelles conformes au GPDR, doivent faire partie des spécifications du projet dès le début pour éviter les problèmes et les dépenses inutiles par la suite. Tous les nouveaux projets informatiques doivent être partagés avec l'agent de conformité et de sécurité informatique concerné, ainsi qu'avec le correspondant de la protection des données, qui à leur tour informeront les équipes de projet s'ils doivent être considérés comme importants pour la sécurité informatique en général et la conformité Sox, et quels contrôles de sécurité devront être mis en œuvre..

Pour garantir la conformité au GDPR, tous les projets ou systèmes informatiques impliquant des données personnelles doivent les traiter avec la plus haute protection possible de la vie privée afin que, par défaut, les données personnelles ne soient pas rendues accessibles à un nombre indéfini de personnes au sein ou au-delà d'ArcelorMittal. Cela inclut, mais sans s'y limiter, de s'assurer que seules les données nécessaires doivent être traitées, que les périodes de stockage des données sont réduites au minimum et que l'accessibilité aux données personnelles est limitée. En outre, pour tous les nouveaux projets informatiques, des mesures techniques et organisationnelles doivent être mises en place de manière à sauvegarder les principes de confidentialité et de protection des données dès les premières étapes de la conception des opérations de traitement (voir « Politique de confidentialité dès la conception et par défaut »).

3.5 Sensibilisation de l'utilisateur final

La mise en œuvre d'un programme de sécurité des systèmes d'information ne signifie pas que toute la responsabilité de la sécurisation des données incombe aux services informatiques. Cette attitude affaiblirait considérablement la sécurité globale de l'entreprise et conduirait à la situation dangereuse dans laquelle la plupart des employés ne se sentent pas responsables de la sécurité de leurs propres données. Il appartient à chaque direction de segment/unité de construire et d'organiser, en étroite coordination avec le bureau CISO du groupe, la sensibilisation de leurs utilisateurs finaux. La sensibilisation à la sécurité et la formation sur la confidentialité des données devraient être obligatoires lors de l'adhésion à l'entreprise et devraient être répétées au moins une fois par an par la suite. Des messages de sensibilisation à la sécurité de l'information sont diffusés régulièrement ou en fonction des besoins, par exemple en ce qui concerne les cyberattaques.

3.6 Sécurité du traitement en vertu du Règlement Général sur la Protection des Données

Les services informatiques doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au risque, conformément aux exigences de l'article 32, paragraphe 1, du GPDR, y compris, mais sans s'y limiter à:

- Anonymisation et cryptage des données personnelles ;
- Capacité d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et des services de traitement;
- Capacité de rétablir la disponibilité et l'accès aux données personnelles en temps opportun en cas d'incident physique ou technique;
- Un processus permettant de tester, d'évaluer et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles visant à assurer la sécurité du traitement [1].

[1] Veuillez vous référer à la « Politique sur la pseudonymisation et l'anonymisation » et à la « Politique sur les contrôles cryptographiques ».

4 RESPONSABILITES

4.1 Bureau Group CISO

La responsabilité première du bureau du Groupe CISO est de développer, mettre en œuvre et gérer la sécurité des systèmes d'information au niveau du groupe. Cela comprend plusieurs activités comme la production de rapports sur les résultats de l'analyse de sécurité, la production de rapports sur les résultats des vérifications et des autoévaluations ainsi que d'autres rapports de gestion consolidés liés à la cybersécurité. Le bureau se chargera également de lancer des initiatives de groupe au besoin pour favoriser l'amélioration globale de la cybersécurité pour le groupe et sera responsable de faciliter la mise en œuvre du Conseil de sécurité des IT (IT&OT). Le bureau agit à titre de centre de compétence en matière de sécurité des IT à l'appui des équipes IT, dans le contexte des projets de TI et de la gestion des incidents de sécurité.

4.2 Segment / Clusters / Divisions commerciales / Unités

La principale responsabilité des divisions commerciales / unités des segments / clusters est d'intégrer la sécurité informatique à tous les niveaux dans leurs solutions et services informatiques. Un agent de sécurité IT doit être affecté aux niveaux appropriés de son organisation, responsable de la coordination du déploiement et du soutien de la politique et des cadres de sécurité IT, y compris la coordination des autoévaluations et des vérifications pour leurs segments, au besoin. Les segments et les divisions commerciales peuvent décider d'impartir la responsabilité de l'exécution des activités IT, y compris les contrôles de sécurité IT, à des fournisseurs de services spécialisés. Toutefois, la responsabilité de la conformité aux cadres de sécurité IT ne peut pas être transférée.

4.3 Conseil de sécurité informatique

Tous les segments du CIO supervisent la cybersécurité dans leur champ d'application. Ils peuvent déléguer cette responsabilité à un responsable de la conformité et de la sécurité informatique. Tous les segments sont représentés au sein d'un Conseil de sécurité informatique organisé et coordonné par le Bureau CISO du Groupe. Les éléments du Programme de sécurité des systèmes d'information seront présentés au Conseil de sécurité IT aux fins de validation. Les rapports sur la conformité à notre cadre de cybersécurité seront en premier lieu adressés au Conseil de sécurité IT.

4.4 Propriétaires d'informations commerciales

Les entreprises assurent la propriété de toutes les informations et applications internes. Les propriétaires d'informations commerciales doivent jouer un rôle actif dans les contrôles de sécurité IT, en ce qui concerne l'accès et la gestion du changement. La gestion de l'accès aux ressources informatiques repose sur le fait que tous les employés et le personnel externe ont un identifiant d'employé (et d'entrepreneur) ArcelorMittal (AMEI) unique, validé par l'entreprise responsable (tel que défini dans la procédure sur l'identité des ressources humaines et l'accès sécurisé aux actifs d'information ArcelorMittal). Les propriétaires d'information et d'applications appuieront les évaluations visant à définir les profils de risque liés à l'information et à prendre les dispositions nécessaires pour définir et mettre en œuvre des contrôles de sécurité de niveau supérieur aux fins d'atténuation.

5. Utilisateurs finaux

Toutes les informations internes doivent être, par principe, considérées comme confidentielles (utilisation interne uniquement), sauf indication contraire, par tous les employés et sous-traitants d'ArcelorMittal et ne doivent pas être envoyées ou partagées avec des tiers, y compris les visiteurs et les sous-traitants, sans l'accord approprié du propriétaire de l'information. Les utilisateurs devraient avoir accès aux informations et aux applications dont ils ont besoin pour exercer leurs fonctions, et pas plus. Les utilisateurs sont responsables de toutes les actions effectuées sous leurs identifiants utilisateur. Les utilisateurs finaux utilisent les moyens disponibles pour se familiariser avec les menaces à la sécurité et soutenir activement le déploiement et la mise en œuvre des contrôles de sécurité IT. Les utilisateurs doivent s'engager activement à noter et à signaler tout écart ou anomalie à leur service informatique ou à leur agent de sécurité informatique.

6. Correspondants en protection des données

Le correspondant protection des données coordonnera toutes les mesures nécessaires afin de s'assurer que les filiales relevant de son champ d'application respectent leurs obligations en vertu des « Règles d'entreprise contraignantes » ("BCR") qui est également la procédure de protection des données ArcelorMittal. De plus, le correspondant en protection des données supervisera la conformité de ces filiales avec le BCR et surveillera la formation au sein des filiales.

7. Avantages commerciaux

Les avantages de la Politique sur la sécurité IT comprennent, sans toutefois s'y limiter, les éléments suivants ::

- Minimiser le risque de fuite ou de perte de données;
- Protéger les ressources d'informations ArcelorMittal contre l'accès, la modification, la divulgation et la destruction non autorisés;
- Fournir aux employés d'ArcelorMittal des conseils lors de l'utilisation des systèmes d'information d'ArcelorMittal (y compris les sous-traitants à temps plein, à temps partiel) ;
- Promouvoir une position proactive pour ArcelorMittal sur la protection des systèmes d'information de l'organisation avec des risques de cybersécurité pertinents.

---- Fin du document ----