IT global **Juridique et Compliance** **Ressources humaines**	**Politique d'utilisation TI**	ArcelorMittal

OBJET

La fiabilité et la performance de l'environnement informatique (« IT ») sont vitales pour l'activité d'ArcelorMittal. L'environnement informatique comprend un large éventail de systèmes, produits, réseaux, bases de données, ordinateurs, appareils mobiles, plateformes électroniques, détenus, loués ou contrôlés par ArcelorMittal (ensemble, les « ressources informatiques d'ArcelorMittal »).

La Politique d'utilisation des ressources informatiques vise à atteindre les objectifs suivants :

1. améliorer la sécurité de l'information et la propriété intellectuelle d'ArcelorMittal. Tous les utilisateurs de ressources informatiques (tels que définis ci-dessous) doivent comprendre que la sécurité informatique n'est pas une simple question de configurations systèmes et de dispositifs techniques. Elle dépend également du comportement des utilisateurs.

2. assurer le respect du Code d'éthique, de la législation et de la réglementation applicables en matière de gestion des ressources informatiques.

3. accroître la sensibilisation des personnes susceptibles d'utiliser des ressources informatiques d'ArcelorMittal quant à leurs responsabilités lors de l'utilisation de ces ressources.

1. PORTÉE

La présente Politique d'utilisation s'applique à toutes les personnes qui utilisent les ressources informatiques d'ArcelorMittal (les « Utilisateurs »), qu'elles soient employées d'ArcelorMittal ou de tiers tels que sous-traitants ou affiliés et que l'accès à ces ressources s'effectue depuis un site d'ArcelorMittal ou d'ailleurs.

2. SOMMAIRE

2.1. Accès aux ressources informatiques d'ArcelorMittal

2.1.1. Règles générales

Les ressources informatiques d'ArcelorMittal, incluant le courrier électronique et l'accès au Web, sont un instrument au service des affaires et du développement d'ArcelorMittal dans le monde.

Les ressources informatiques d'ArcelorMittal sont fournies à certains salariés et sous-traitants pour les besoins de leur activité professionnelle au sein d'ArcelorMittal. L'accès aux ressources informatiques d'ArcelorMittal doit être réservé aux personnes identifiées qui sont dans l'obligation d'y avoir accès et doit être ajusté et retiré en conséquence.

Toutes les Unités d'affaires doivent implémenter une procédure de départ au terme de laquelle les salariés ayant quitté ArcelorMittal ou les sous-traitants dont le contrat avec ArcelorMittal a expiré pour quelque raison que ce soit doivent restituer tous les appareils et équipements fournis par la société (ordinateurs portables, téléphones intelligents, tablettes, etc.) et tous les comptes utilisateurs doivent être immédiatement fermés.

Les utilisateurs doivent sécuriser tous les mots de passe des comptes, comme décrits à l'Annexe I (« Instructions de sécurité informatique pour les utilisateurs », Section 2 « Sécurité informatique »). Les comptes utilisateurs ne peuvent être partagés avec quiconque. Les Utilisateurs porteront en toutes occasions l'entière responsabilité de toutes activités ayant lieu sur leur compte.
Les utilisateurs doivent signaler au département IT et à leur encadrement tout incident de sécurité affectant une ressource informatique d'ArcelorMittal, y compris les cas de perte et de vol d'appareils. Aucune plainte ne doit être introduite auprès de la police locale, de l'Autorité de protection des données ou de toute autre agence gouvernementale sans l'approbation du service juridique.

2.1.2. Identifiant de salarié ArcelorMittal

Afin de réduire le risque d'accès illicite aux ressources informatiques d'ArcelorMittal, tous les Utilisateurs doivent posséder un identifiant de groupe valide, l'Identifiant de salarié (et sous-traitant) ArcelorMittal (« AMEI »). Veuillez consulter les règles définies dans la procédure ***Human Resource Identity and Secure Access to ArcelorMittal Information Assets***.

2.1.3. Sécurité informatique pour Utilisateurs

Les utilisateurs doivent en toutes occasions respecter les ***Instructions de sécurité informatique pour les utilisateurs*** jointes en tant qu'Annexe I à la présente Politique.

2.2. Interdictions et restrictions d'utilisation

2.2.1. Règles générales

Les Utilisateurs ne peuvent utiliser les ressources informatiques d'ArcelorMittal :

- pour envoyer, télécharger, charger, distribuer ou diffuser tout contenu ou proposer de telles actions sur tout contenu qui serait illégal, diffamatoire, harcelant, abusif, frauduleux, illicite, obscène ou répréhensible d'une quelconque manière ;
- pour opérer une entreprise commerciale extérieure ou à des fins commerciales externes ;
- pour mener toutes activités illégales, telles celles liées au partage illégal de point à point de fichiers (ArcelorMittal ne sera nullement tenu aux coûts de toute action en justice à l'encontre d'un Utilisateur qui violerait ces lois, quelles que soient la situation, l'intention ou les visées de l'Utilisateur) ;
- pour mener toute activité susceptible de nuire à la réputation ou à l'image publique d'ArcelorMittal ;
- pour mener toute activité contraire au Code d'éthique ou à toute procédure ou politique d'ArcelorMittal.

Les Utilisateurs ne peuvent utiliser les ressources informatiques d'ArcelorMittal autrement que via les interfaces fournies par le Département IT.

2.2.2. Utilisation à des fins non professionnelles

Comme déjà mentionné ci-dessus (Cf. 2.1.1 Règles générales), les ressources informatiques d'ArcelorMittal sont mises à disposition de certains employés et sous-traitants à des fins professionnelles.

Néanmoins, une utilisation de certains éléments limités des ressources informatiques d'ArcelorMittal à des fins privées est acceptable dès lors que :

i. une telle utilisation n'impacte pas négativement le travail de l'Utilisateur ;
ii. une telle utilisation n'impacte pas négativement la disponibilité des ressources informatiques d'ArcelorMittal (exemple : la bande passante) ;
iii. rien dans l'action menée par l'Utilisateur ne peut laisser croire à ses interlocuteurs que cette action a été menée au titre de ses fonctions professionnelles ;
iv. les actions non professionnelles sont identifiées comme telles, et cela de façon claire et non ambiguë (exemple. "Message privé" ou "Document privé"), et sauvegardés dans un dossier distinct et séparé des éléments professionnels (exemple "Nom/Prénom – Messages Privés", "Nom/Prénom – Documents privés").

En l'absence d'indication « Privé » claire et visible dans le sujet d'un courrier électronique ou le nom d'un dossier, ce courrier ou ce dossier sera considéré comme une ressource informatique d'ArcelorMittal.

Dans le cadre de son utilisation à des fins non professionnelles, l'Utilisateur ne doit pas envoyer de messages hautement confidentiels ou extrêmement personnels. Les ressources informatiques ArcelorMittal ne permettent pas de traiter les messages ou dossiers privés séparément des autres messages ou dossiers. L'Utilisateur est ainsi informé que ses messages ou dossiers privés sont stockés de manière centralisée, y compris ceux marqués « Privé ».

L'Utilisateur quittant ses fonctions dans le groupe ArcelorMittal pourra, si et dans la mesure où la configuration ne lui permet pas de supprimer par lui-même ses messages et dossiers marqués « Privés », demander la suppression de ces messages et dossiers. Sauf cas de contestation ou litige impliquant ces éléments ou relatifs à ces éléments, par exemple quant au respect de la présente Politique par l'Utilisateur, ces messages et dossiers seront supprimés.

2.2.3. Données personnelles

Toutes les données personnelles contenues dans les ressources informatiques d'ArcelorMittal doivent être traitées dans le respect du Code d'éthique et, dans la mesure où elle est applicable, selon la ***Procédure de protection des données d'ArcelorMittal***.

2.2.4. Données classifiées/à accès restreint

Les Utilisateurs ne peuvent utiliser une quelconque information d'ArcelorMittal à laquelle ils auraient accès à partir des ressources informatiques d'ArcelorMittal en violation de toute restriction d'utilisation, exigence de confidentialité et/ou classification des données comme restreintes mentionnées dans le document contenant cette information. Des instructions complémentaires sur la classification des données sont fournies à l'Annexe II.

2.3 Rôle du Département IT

Il incombe au Département IT de maintenir, dans des conditions de maîtrise des coûts, la stabilité, la sécurité et l'efficience opérationnelle des ressources informatiques d'ArcelorMittal. Tous les membres du Département IT doivent suivre la Politique de sécurité IT (« IT Security Policy ») et mettre en œuvre le Cadre de sécurité IT (« IT Security framework ») sur toutes les plateformes sous leur responsabilité.

Le fonctionnement et la maintenance courante des ressources informatiques d'ArcelorMittal requièrent le suivi des actifs IT, les inventaires, la sauvegarde des données, les analyses de tendances, le scanning, le

nettoyage ou la surveillance des données stockées, la tenue du journal de l'activité, la surveillance des schémas d'utilisation générale et de trafic réseau, et toutes les autres activités requises aux fins de la sécurité de l'information, la gestion des coûts IT, le respect des contrats signés avec des tiers (p. ex. les contrats de licence de logiciels) et la fourniture de services IT.

Les membres du Département IT ne sont autorisés à accéder à ou utiliser une quelconque ressource informatique d'ArcelorMittal, que si cela est nécessaire pour qu'ils puissent effectuer leur travail dans le cadre de leurs fonctions. Les membres du Département IT doivent respecter la plus stricte confidentialité pour les informations auxquelles ils ont accès pour effectuer leur travail dans le cadre de leur fonction.

2.4 Utilisation de comptes privés, d'équipements privés et des médias sociaux à des fins professionnelles

2.4.1. Comptes non ArcelorMittal

Il est interdit aux Utilisateurs d'utiliser des comptes non ArcelorMittal, y compris des comptes courriel privés (Gmail, Yahoo…), à des fins professionnelles. En règle générale, tous les courriels ou documents professionnels doivent être envoyés et reçus par un courriel de la société ou une autre ressource informatique d'ArcelorMittal.

À titre exceptionnel, en cas d'urgence et de nécessité de faire face à un besoin professionnel particulier et urgent, les Utilisateurs peuvent recourir à un compte courriel privé, pour un temps limité et pour autant que (i) les Utilisateurs mettent toujours en copie le compte courriel fourni par la société ou une autre ressource informatique d'ArcelorMittal et (ii) les Utilisateurs effacent dès que possible toutes les informations professionnelles enregistrées sur leur compte courriel privé et (iii) l'échange d'informations ne porte pas sur des données qualifiées « Très restreintes », telles que définies dans les instructions relatives à la classification des données ci-jointes (voir Annexe II).

2.4.2. Équipements privés

ArcelorMittal ne promeut en aucune manière le recours à des équipements privés au travail. Toutefois, ArcelorMittal reconnaît que certains salariés peuvent vouloir utiliser leur propre équipement à des fins professionnelles. Selon la **procédure Global Mobile Device d'ArcelorMittal**, les régions/segments définissent dans quelle mesure les Utilisateurs sont autorisés à faire usage de leurs équipements privés dans un contexte professionnel, compte tenu des contraintes de sécurité IT définies ci-après.

En toutes occasions, l'accès aux ressources informatiques d'ArcelorMittal ne peut s'effectuer à l'aide d'un équipement privé (téléphone intelligent, tablette) que si des contrôles de sécurité appropriés ont été mis en place comme prescrit par le Département IT (comme la fixation d'un conteneur ArcelorMittal dans l'appareil). Conformément à la procédure Global Mobile Device, des règles de sécurité strictes doivent être acceptées par l'Utilisateur, qui doit également s'engager par écrit à les respecter. Les départements IT ou RH locaux ou toute autre fonction à laquelle les régions / secteurs professionnels auront confié cette responsabilité devront (i) veiller à ce qu'un accord soit signé par chaque Utilisateur autorisé et (ii) à en conserver une copie dans le respect des lois en vigueur.

Le conteneur ArcelorMittal de l'équipement privé est considéré comme une ressource informatique d'ArcelorMittal.

En cas d'infraction à cette Section 2.4.2 (« équipements privés ») par un Utilisateur, ArcelorMittal se réserve le droit de bloquer tout accès aux ressources informatiques d'ArcelorMittal au départ de cet appareil, nonobstant les autres droits et recours dont la société pourrait disposer pour une infraction à cette Politique d'utilisation selon le droit en vigueur.

Toute continuation de l'utilisation de l'équipement en infraction à la présente Section 3.4.2 se fera au risque connu de l'Utilisateur et ArcelorMittal décline toute responsabilité pour un quelconque dommage à cet équipement.

2.4.3. Médias sociaux

Lorsqu'ils utilisent les médias sociaux dans un contexte de travail sur leurs propres ressources informatiques, les Utilisateurs et les salariés doivent respecter les règles définies dans la ***procédure Médias sociaux***.

2.5 Audits et investigations informatiques

Il convient de rappeler que le rôle du département Assurance interne (IA) d'ArcelorMittal est (i) d'aider le Comité d'audit et le Management exécutif à faire face à leurs responsabilités en matière de contrôle interne, gestion du risque et gouvernance d'entreprise de manière créatrice de valeur, indépendante et objective (ii) d'établir une fonction IA de classe mondiale comportant un réseau homogène d'équipes d'audit locales décentralisées entretenant des relations fortes (mais indépendantes) avec le management local ; avec des compétences maison, dont IT, SOx, forensic et gestion du risque ; composée de professionnels formés utilisant une méthodologie commune, des pratiques d'audit et des outils de documentation aux normes de l'IIA (Institute of Internal Auditors).

Par conséquent, le département IA d'ArcelorMittal peut, dans le cadre de la mission ci-dessus, inspecter toutes les ressources informatiques d'ArcelorMittal sans notification préalable. En cela, le département IA d'ArcelorMittal agira en conformité avec les normes précitées et n'inspectera pas ces ressources sans raison. D'une manière générale, le département investiguera des activités potentiellement inappropriées en cas de fraude/corruption, de suspicion de fraude/corruption ou de violation du Code d'éthique ou de toute autre procédure d'ArcelorMittal.

Une telle inspection doit recevoir l'approbation préalable de la direction du département Internal Assurance ou de celle du Forensic. Toute demande d'accès aux ressources informatiques doit être adressée au CIO de région/segment ou au Group IT Security Officer.

ArcelorMittal IA n'accédera pas aux courriels et dossiers privés dûment marqués comme tels, en conformité avec la Section 2.2.2 ci-dessus ("Utilisation à des fins non professionnelles"), sans en avoir informé l'Utilisateur par avance et l'avoir convoqué, sauf en cas d'urgence menaçant la disponibilité et/ou la sécurité d'une ressource informatique ArcelorMittal requérant un accès immédiat.

2.6 Filtrage et suivi de l'utilisation

Pour tout motif légitime, ArcelorMittal se réserve le droit de bloquer l'accès à certains sites web et protocoles. Les courriels et autres documents empruntant les ressources informatiques d'ArcelorMittal seront automatiquement scannées pour détection de virus ou pour d'autres raisons de sécurité.

Si ArcelorMittal ne pratique pas de surveillance routinière de l'utilisation individuelle de ses ressources informatiques, la société ne s'en réserve pas moins le droit de contrôler l'utilisation de toute ressource informatique d'ArcelorMittal pour tout motif professionnel légitime, pour des raisons de sécurité, en cas d'infraction à cette Politique d'utilisation ou de suspicion à cet égard, conformément à la fois au droit en vigueur et à la Procédure de Protection des données d'ArcelorMittal, le cas échéant.

2.7 Accès par le management

Il est de la plus haute importance d'assurer que les ressources informatiques d'ArcelorMittal, dont le rôle est d'appuyer l'activité d'ArcelorMittal, restent en tout temps et en toutes circonstances accessibles aux Utilisateurs en fonction des besoins de l'activité.

Pour cette raison, en cas de risque d'interruption de l'activité, l'accès à toute ressource informatique d'ArcelorMittal détenue par un Utilisateur peut être octroyé à d'autres, moyennant l'approbation préalable du management de l'Utilisateur, à toute fin de continuité de l'activité pour laquelle cet accès est pertinent, y compris en cas de maladie, absence, congés de l'Utilisateur, ainsi qu'en cas de suspension ou de résiliation du contrat de travail ou autre pour quelque motif que ce soit.

Les demandes de ce genre doivent être adressées au CIO de région/segment ou au Group IT Security Officer.

Néanmoins, ArcelorMittal n'accédera pas aux courriels et dossiers privés dûment marqués comme tels, en conformité avec la Section 2.2.2 ci-dessus ("Utilisation à des fins non professionnelles"), sans en avoir informé l'Utilisateur par avance et l'avoir convoqué, sauf en cas d'urgence menaçant la disponibilité et/ou la sécurité d'une ressource informatique ArcelorMittal requérant un accès immédiat.

2.8 Accès par des tiers extérieurs à ArcelorMittal

Les Utilisateurs doivent avoir conscience de ce qu'ArcelorMittal peut être contraint de révéler ou de mettre à disposition de tiers des ressources informatiques d'ArcelorMittal (et particulièrement leur contenu), ainsi que d'éventuels messages ou dossiers marqués « Privés », suite à diverses exigences légales, y compris assignations, ordonnances de justice, mandats de perquisition, requêtes. Toute notification ou communication ne peut se faire que sous la supervision du département juridique.

2.9 Mise en œuvre de cette Politique d'utilisation

Il incombe à chaque Utilisateur de veiller à ce que l'usage qu'il fait des ressources informatiques d'ArcelorMittal soit légal et conforme à cette Politique d'utilisation. Les salariés ayant enfreint cette Politique d'utilisation peuvent encourir des sanctions disciplinaires, y compris le licenciement. Les sanctions disciplinaires pour infraction à cette Politique d'utilisation entrent dans le cadre des règlements disciplinaires normaux d'ArcelorMittal au niveau local. Si les activités sont illégales ou si ArcelorMittal suspecte qu'elles pourraient l'être, il peut être fait appel aux autorités compétentes, telle la police locale.

2.10 Procédures liées

La Politique d'utilisation des ressources informatiques se fonde sur le Code d'éthique.

En outre, comme mentionné ci-dessus, les procédures suivantes sont liées à la présente Politique d'utilisation des ressources informatiques :

- Instructions de sécurité informatique pour les utilisateurs (Annexe I)
- Politique de Sécurité IT
- Procedure Baseline IT Security Controls Framework
- Procedure Human Resource Identity and Secure Access to ArcelorMittal Information Assets
- Procédure de protection des données personnelles
- Procédure Médias sociaux
- Procédure Global Mobile Device
- Directives relatives à la classification des données (Annexe II)

Toutes les procédures sont disponibles sur le portail GPPM. Une représentation graphique est jointe – Annexe III – pour permettre aux Utilisateurs de mieux saisir les interrelations entre ces procédures.

****