Politique d’utilisation des Technologies de l'Information et des Télécommunications

La présente Politique définit les conditions générales d’utilisation des Technologies de l’Information et des Télécommunications.

Sous ce terme sont regroupés : la connexion à Internet, la messagerie électronique, les systèmes de communication et plus généralement l’ensemble des moyens informatiques mis à la disposition de l’utilisateur par l’entreprise (PC, Smartphones, etc.).

Cette politique précise les droits et obligations que l’employeur et l’utilisateur sont tenus de respecter afin d’instaurer un usage convenable des TIC, dans le respect des dispositions légales et réglementaires en vigueur.

Ces principes d’utilisation sont basés sur les principes de loyauté et de confiance réciproques.

eramet

1. PRINCIPES

CHAMPS D'APPLICATION

La présente politique s'applique à l'ensemble du personnel de la Société, tous statuts confondus (salariés, intérimaires, stagiaires, prestataires de service…), et plus généralement à l'ensemble des personnes ayant accès aux ressources informatiques de l'entreprise, de façon permanente ou temporaire, dans les locaux de l'entreprise, ou à l'extérieur par un accès à distance à partir du réseau administré par l'entreprise.

TERMINOLOGIE

L'expression « utilisateur » désigne donc toute personne qui, quel que soit son statut, est amenée à créer, consulter et mettre en œuvre les ressources informatiques mises à disposition par la Société et/ou le Groupe Eramet.

DROIT EN VIGUEUR

Des lois et des textes réglementaires définissent les droits et obligations des personnes utilisant les moyens informatiques.

Il est rappelé que toute personne présente sur le sol français doit respecter la législation française, notamment :

- la loi du 20 juin 2018 n° 2018-493, mettant en œuvre le règlement Union Européenne du 27/04/2016 dit RGPD (règlement général sur la protection des données personnelles)
- la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**;**
- la législation relative à la fraude informatique (article 323-1 à 323-7 du Code pénal).

Il est également rappelé l'existence d'un accord de groupe en vigueur sur le droit à la déconnexion dont bénéficie chaque collaborateur.

LE DROIT D'ACCES

Pour accéder au réseau tout utilisateur reçoit un mot de passe et un identifiant qui lui sont individuels.
Il est responsable de la protection de son mot de passe en assurant qu'il ne soit pas divulgué et qu'il réponde à un standard de sécurité suffisant en termes de nombre de caractère et complexité au regard des consignes et procédures diffusées par le service informatique.
Cet identifiant et mot de passe doivent rester personnels et ne pas être partagés.

LA FINALITE D'ACCES

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder sont autorisés dans le cadre de l'activité professionnelle des utilisateurs.
L'utilisateur doit veiller à la bonne utilisation de ces moyens informatiques et donc le devoir d'en conserver l'intégrité, comme dans le cas de tout autre outil mis à sa disposition dans le cadre de son travail.

Les administrateurs systèmes disposent de certains droits d'accès privilégiés afin d'administrer et contrôler ces systèmes. Ceux-ci doivent respecter une clause de stricte confidentialité

2. MODALITES DE MISE EN ŒUVRE

Organisation

La Direction des Ressources Humaines et les instances représentatives des employés s'engagent à déployer localement cette politique dans le cadre légal applicable et à informer l'ensemble des employés de sa mise en œuvre.

La Direction des Systèmes d'Information s'engage à suivre les modalités décrites dans cette politique. L'ensemble des employés s'engagent à suivre les règles décrites dans la Politique.

Gouvernance

La Direction des Ressources Humaines du groupe Eramet est responsable du déploiement de la Politique et du respect des engagements de bon usage des outils informatiques à l'échelle du groupe Eramet. Ce document est maintenu à jour conjointement par la Direction des Relations Sociales et la Direction Informatique.

Méthode

REGLES GENERALES DE SECURITE

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale de ses ressources et indirectement à celle de son entreprise. Ainsi, l'utilisateur ne doit pas modifier les paramètres de sécurité de son équipement.

L'utilisation de ces ressources doit être rationnelle et honnête afin d'en éviter la saturation ou le détournement à des fins personnelles.

Enfin, il appartient aux utilisateurs de respecter les règles de protection de la confidentialité. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations de type courrier électronique dont l'utilisateur n'est destinataire ni directement ni en copie.

REGLES DE SECURITE PARTICULIERES

L'utilisateur doit appliquer les consignes, procédures et recommandations de sécurité de l'entreprise notamment dans les domaines suivants :

Protection des données

L'Utilisateur doit se tenir informé et respecter les procédures relatives à la classification, au stockage, à la transmission et à la destruction de l'information ainsi qu'à la sécurisation des mots de passe.

L'utilisateur doit verrouiller systématiquement son ordinateur dès qu'il quitte son poste de travail afin que le contenu ne soit pas accessible.

L'utilisateur doit signaler au service informatique toute tentative de violation de son compte et de façon générale, toute anomalie qu'il peut constater.

Si l'utilisateur doit envoyer des données confidentielles, celui-ci doit prendre soin de l'adresser aux seules personnes habilitées dans le cadre de leur activité et après avoir vérifié leur identité. Des solutions de chiffrement sont mises à disposition par l'entreprise. Il lui appartient de se rapprocher du service informatique.

L'utilisateur ne doit pas utiliser les services personnels (dropbox, email perso…) pour échanger ou stocker des données professionnelles.

Règles pour les postes de travail

L'utilisateur est responsable des équipements (PC, laptop, smartphone, tablette, etc…) et outils qui lui ont été confiés. Il s'engage à les protéger afin qu'ils ne soient perdus ou volés. Ils ne peuvent être cédés, prêtés ou transmis à des tiers. Il s'interdit de modifier les configurations établies.

Les mises à jour doivent être réalisées dans les délais qui seront communiqués par le service informatique.
En cas de perte, de casse ou de vol, il doit contacter de toute urgence le service informatique de la Société et/ou du groupe Eramet.

Règles relatives au logiciel/ matériel

Il est interdit d'introduire tout nouveau matériel, programme ou logiciel en dehors de ceux supervisés par le service informatique, sauf sur leur autorisation. Il en est de même pour les logiciels dits « Libres ».

Règles pour les supports amovibles

L'utilisation d'une clé USB, disque dur, de CD/DVD est autorisée sous réserve que l'utilisateur effectue un contrôle antivirus visé par le service informatique et que cela réponde à un besoin professionnel.

Le stockage de données sur ces types de supports doit être destiné au seul moyen de transfert court terme et non pas pour archiver ou sauvegarder des données. Les données doivent être conservées sur les services de fichiers fournis par la Société (Serveur de Fichiers, Sharepoint ,..)

Lorsqu'ils ne sont pas utilisés les supports amovibles doivent être stockés dans des lieux sécurisés.
La connexion de support amovible personnel est interdite.
L'utilisation du poste de travail comme une station de recharge électrique, par exemple d'un téléphone portable n'est pas autorisée.

Règles de sauvegarde des données

Toutes les données professionnelles stockées sur le poste de travail ou les équipements doivent également être stockées sur une ressource réseau de l'entreprise. Les données sur le disque dur du PC doivent être réduites au minimum.

Il appartient à l'utilisateur d'assurer un tri des documents qu'il reçoit (par email ou autre) et de les stocker sans délais à l'endroit prévu par son département/équipe (serveur de fichier, sharepoint…).

Protection contre la « Fraude » et le « Phishing » et anomalies

L'utilisateur doit être particulièrement vigilant quant aux messages provenant de l'extérieur dont l'expéditeur n'est pas connu ou dont le

contenu est suspect. En cas de doute il doit se rapprocher de son service informatique.

Il est rappelé que l'origine d'un email n'est jamais certaine et que le nom de l'émetteur affiché n'est jamais une garantie de sa bonne identité. Le contenu d'un email sensible doit être confirmé par échange téléphonique si besoin.

Il est interdit de faire des manipulations anormales qui pourraient engendrer l'introduction de logiciels parasites, ou de virus.

Règles de sécurité relatives au télétravail et en situation de mobilité

L'utilisateur doit s'assurer en toute circonstance que son environnement de travail est adéquat afin de préserver l'intégrité et la confidentialité des données. Il utilisera les filtres d'écran de sécurité pour limiter les risques.

L'utilisateur ne doit pas utiliser d'équipements ou de réseaux publics (hôtel, cybercafé…) à des fins professionnelles.

Règle de gestion des arrivées/ départs/ absences au regard des données

L'utilisateur a un devoir d'anticipation dans la transmission de ses données.

Ainsi, en cas de départ de l'entreprise ou en cas d'absence prolongée anticipée, il doit veiller à la transmission des données professionnelles, pour la bonne marche du service, aux personnes concernées.

Il est interdit à un utilisateur de supprimer l'ensemble de ses données professionnelles du réseau et de son poste de travail.

S'il n'a pas préparé son départ, la Société se réserve le droit d'agir sur les différents dossiers, fichiers, répertoires, courriers électroniques à caractère professionnel. Toute donnée personnelle stockée sur les ressources informatiques qui n'aurait pas été récupérée après le départ de l'entreprise de l'utilisateur fera l'objet d'une destruction.

Règles particulières pour les téléphones portables

Tout comme le poste de travail, le téléchargement d'applications doit être limité aux applications autorisées par la Société ou le Groupe.
En cas de perte ou de vol, l'utilisateur doit immédiatement prévenir le service informatique pour procéder sans délai à l'effacement définitif du téléphone et de son contenu.

Règles particulières pour la messagerie

Une adresse de messagerie (email) sera fournie aux utilisateurs dans le cadre de leurs fonctions. Cette adresse email sera fermée au départ de l'utilisateur et la boite email sera détruite après le départ du collaborateur.

Il appartient à l'utilisateur de ne pas rediriger toute ou partie des mails de la boite de messagerie professionnelle qui lui est confiée, vers un système de messagerie hors Groupe Eramet, quel qu'en soit le motif.

Il doit limiter le nombre de destinataires de ses mails au strict nécessaire.
Il est recommandé de partager des documents en envoyant par email uniquement le lien vers ledit document échangé sur un outil de partage fourni par le service informatique (ex : un Sharepoint). Pour prévenir les risques de virus, il est demandé de vérifier l'origine et l'authenticité des messages, et il est conseillé, dans le doute, de détruire les messages provenant d'un inconnu qui comportent une pièce jointe, sans la lire ou l'extraire.

Pour les règles d'applications spécifiques qui n'auraient pas été décrites ci-dessus, il appartiendra à l'utilisateur de se conformer aux notes de services ou procédures en la matière qui pourront être diffusées pour assurer le bon fonctionnement des moyens informatiques.

RESPECT DE LA LEGISLATION

Législation en matière de propriété intellectuelle

Les obligations en matière de droits de propriété imposent à l'utilisateur de respecter les droits d'auteur et de propriété intellectuelle et de ne pas copier, modifier, diffuser ou utiliser des informations, des documents, des œuvres (textes, images, photographies, œuvres musicales ou audiovisuelles, logo de la Société et/ou du groupe Eramet), des logiciels et des licences associées dont il ne détiendrait pas les droits requis (droits d'utilisation, de modification, de reproduction...).

Les utilisateurs ne doivent utiliser que les logiciels couverts par le contrat de Licence de la Société et/ ou du groupe Eramet selon les termes de la licence.

Il est interdit à tout salarié de sortir de l'entreprise des copies des données de la Société et/ou du groupe Eramet, hormis en cas d'autorisation formelle pour un usage limité au cadre strict de son travail, ou dans les cas précis d'opérations de sauvegarde ou de maintenance réalisées par le service informatique.

Respect de la législation sur le droit des personnes et le respect de la vie privée

Sont strictement interdits la consultation, la diffusion ou le téléchargement de sites, d'images ou de fichiers notamment à caractère injurieux, diffamatoire, servant à provoquer la violence ou la haine raciale, religieux ou sexuels, pédophiles et violences faites aux enfants.

Respect de toute disposition d'ordre public et de toute disposition non contraire aux bonnes mœurs

Sont strictement interdits la consultation, la diffusion ou le téléchargement de sites, d'images ou de fichiers notamment à caractères pornographiques, jeux d'argent, armes, violences de toutes sortes.

Respect de la législation sur les données personnelles (« RGPD »)

Tout utilisateur qui procède ou accède à un traitement de données à caractère personnel, relatives aux personnels internes de la Société et/ou du groupe Eramet ou à des tiers (clients, partenaires, candidats...) doit se conformer strictement à la réglementation applicable et les directives établies associées au traitement. Il sera notamment attentif à respecter la finalité des traitements, la confidentialité, la protection et la durée de conservation de ces données.

MODE D'UTILISATION DES SYSTEMES D'INFORMATION : INTERNET, MESSAGERIE, RESEAUX SOCIAUX...

L'utilisateur doit faire usage à titre professionnel des systèmes d'information confiés par l'entreprise dans le cadre de ses activités professionnelles et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent, ainsi que dans le respect de la législation en vigueur comme rappelé ci-dessus.

A titre exceptionnel, une utilisation à des fins extra-professionnelles est tolérée au regard des obligations familiales impérieuses et des nécessités de la vie courante pour l'utilisation d'Internet et de la messagerie.

Cet usage doit s'effectuer en dehors du temps de travail (pendant les temps de pause). Il ne doit pas entraver la rapidité du réseau (risque de saturation), ni mettre en péril l'intégrité du réseau.

Messagerie électronique

Les messages « emails » adressés à l'aide des outils informatiques mis à disposition par l'entreprise sont présumés professionnels. Pour une utilisation personnelle, les messages doivent être explicitement identifiés dans leur objet par la mention «personnel».

Répertoires et fichiers

En conséquence, il est demandé à l'utilisateur d'explicitement identifier avec la mention «personnel» le répertoire dans lequel il peut placer des fichiers personnels dans son disque dur. Il ne devra pas placer dans ce répertoire de fichiers professionnels.

Il est rappelé qu'il s'agit d'une tolérance et que la Société ne garantit pas de sauvegarde de ce répertoire.

Il reste interdit de stocker des données personnelles (photos, musique, vidéos…) sur un espace de stockage partagé (serveur de fichiers, espace SharePoint).

Réseaux Sociaux & publication sur l'Internet

L'utilisateur ne doit pas émettre d'informations confidentielles sur Internet (réseaux sociaux, sites, forums, listes de diffusions...), ne pas se livrer à des actions mettant en péril la sécurité informatique, ne pas émettre d'opinions personnelles qui pourraient nuire à la réputation de l'entreprise ou lui porter préjudice. Il doit se conformer aux lois et réglementations en vigueur.

OBJET ET ENCADREMENT DES CONTROLES

Les dispositifs de sécurité informatique mis en place par le groupe Eramet et/ou la Société, enregistrent les traces des informations qui transitent sur le réseau.

Afin de préserver la sécurité, l'intégrité et la confidentialité du Système d'Information, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable.

Ainsi, les dispositifs d'analyse et de contrôle suivants sont mis en œuvre à des fins de sécurité, de diagnostic de dysfonctionnement ou de contrôle de conformité des postes de travail et des systèmes implémentés :

Au système d'information

La configuration de sécurité des systèmes génère des enregistrements (logs) – date et heure, identifiant utilisé pour la connexion, services accédés -, qui peuvent être remontés et exploités pour les finalités ci-dessus mentionnées.

Au poste de travail

Un dispositif d'analyse et de blocage des codes malveillants, virus et intrusions est mis en place. La configuration de sécurité des postes de travail (y compris smartphones) génère des enregistrements (logs) – date et heure, identifiant utilisé pour la connexion, messages générés par les dispositifs de sécurité (antivirus...) - qui peuvent être remontés et exploités pour les finalités ci-dessus mentionnées.

Pour Internet

Il est mis en place un dispositif filtrant l'accès à des sites dangereux et/ou contraires à la législation et aux bonnes mœurs.
Les informations enregistrées, pour chaque accès à Internet sont notamment les suivantes : Adresse des sites consultés (URL), Utilisateur (login), type de flux (HTTPs, HTTP, FTP), et le volume des données reçues et transmises. Elles peuvent être remontées et exploitées pour les finalités ci-dessus mentionnées.

Pour la messagerie

Il est mis en place un dispositif de blocage / mise en quarantaine pour les emails dangereux.

Les informations enregistrées sont notamment l'émetteur, le(s) destinataire(s), les informations techniques d'identification du message, les liens et pièces jointes liés au mail.

Pour le téléphone

Les informations enregistrées au niveau des infrastructures téléphoniques professionnelles sont les suivantes : les numéros de téléphone appelés, la durée, la date et heure de l'appel, et les éléments de facturation.

Les informations issues des dispositifs d'analyse, de contrôle et d'enregistrement peuvent être utilisées dans les cas suivants :

- Sur demande des autorités (administratives, judiciaires ou de police)
- En cas d'incidents ou d'utilisation abusive (virus, intrusion, saturation des ressources, pannes…)
- En cas d'acte de malveillance avéré ou suspecté.

ACCES AUX DONNEES

Il est rappelé que les courriers ou fichiers créés ou reçus à l'aide de l'outil informatique mis à disposition par l'employeur pour les besoins du poste sont présumés avoir un caractère professionnel.
La société peut donc accéder aux messages, répertoires et dossiers professionnels à tout moment, même hors la présence de l'intéressé.

Concernant les emails et répertoires caractérisés comme « personnels », il n'est pas fait obstacle à ce que :

- Ces documents soient contrôlés par les outils automatiques de sécurité (i.e. antivirus…)
- Le service informatique puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré, notamment de sécurité, de continuité de service ou de voir sa responsabilité engagée, afin de prendre des mesures conservatoires, en présence ou non de l'Utilisateur et en l'ayant informé.

Concernant les emails caractérisés comme « personnels », il n'est pas fait obstacle à ce que les administrateurs de réseaux puissent accéder aux messageries « emails » et à leur contenu dès lors qu'il existe un risque avéré en termes de sécurité ou de continuité du service.