Guide de l'utilisateur final AMG Global IT et Cybersécurité

Introduction

L'information est un actif essentiel d'AMG. Dans notre pratique professionnelle quotidienne, les informations sont partagées avec de nombreuses personnes à l'intérieur et à l'extérieur de l'entreprise afin de préparer et de prendre des décisions ou de se conformer aux règles et réglementations. Certaines de ces informations sont critiques pour les activités d'AMG et sont, par conséquent, sensibles et doivent être protégées.

La présente directive mondiale d'AMG relative aux technologies de l'information et à la cybersécurité à l'intention des utilisateurs finaux (" **la directive** ") est conçue comme une directive générale sur l'utilisation et la protection des technologies de l'information (à la fois les technologies de l'information liées au bureau et à la communication ou " IT ", et les technologies de l'information liées à l'exploitation et à la production ou " OT ") et de la cybersécurité. Dans le présent document, les références aux technologies de l'information et aux biens informatiques d'AMG doivent être comprises comme faisant également référence aux technologies de l'information et aux biens informatiques de la société.

Portée

Cette directive s'applique à tous les AMG Advanced Metallurgical Group NV et/ou à ses filiales et entités affiliées détenues ou contrôlées (" **AMG** ") ainsi qu'à ses employés, directeurs, responsables, agents et toute autre personne qui, sous l'autorité directe d'AMG, utilisent les systèmes informatiques et/ou connexes, le matériel, les services, les installations et les processus détenus ou autrement mis à disposition par AMG NV ou les filiales en son nom, que ce soit en utilisant les réseaux, les serveurs d'AMG ou ceux fournis par des environnements basés sur le cloud (" **utilisateurs finaux d'AMG** ").

En outre, la ligne directrice s'applique à tout appareil appartenant à un particulier et utilisé dans le cadre des activités d'AMG, à condition que l'utilisation de ces appareils ait été approuvée par la direction locale d'AMG.

Objectif

AMG investit continuellement dans des mesures visant à maintenir et à protéger ses technologies de l'information et ses systèmes de communication et à protéger l'intégrité de ses dispositifs et systèmes informatiques et de cybersécurité. L'objectif de cette directive est de préserver la valeur et la réputation d'AMG en protégeant la disponibilité, l'intégrité et la confidentialité de ses informations et d'établir un cadre pour :

- sensibilisation des utilisateurs finaux d'AMG à la nécessité de prendre des mesures en matière d'informatique et de cybersécurité, afin de s'assurer qu'ils comprennent l'importance de la protection des informations et des données et des questions de sécurité des informations et des données ;
- la gestion des risques liés à l'informatique et à la cybersécurité par le biais de bonnes pratiques ;
- le traitement sécurisé des informations et l'utilisation des services d'information ;
- la conformité aux exigences d'AMG en matière d'informatique et de cybersécurité et aux normes industrielles reconnues
- l'application de la présente ligne directrice.

Gouvernance et mise en œuvre

Le Conseil de direction d'AMG a examiné et approuvé la présente directive dans le cadre et en complément de la POLITIQUE GLOBALE D'AMG EN MATIÈRE DE TECHNOLOGIE DE L'INFORMATION ET DE CYBERSÉCURITÉ (**" Politique globale en matière de TI et de cybersécurité ")**, qui détaille les principes sous-jacents selon lesquels AMG et son groupe mondial de filiales doivent gérer et protéger les TI, les données et les ressources de la société.

La direction locale des filiales d'AMG est responsable de l'adoption et de la conformité à cette directive au sein de son organisation en mettant en œuvre la politique et la directive mondiales d'AMG en matière d'informatique et de cybersécurité, conformément aux lois et réglementations locales applicables, en informant les utilisateurs finaux de cette directive et en fournissant une formation régulière à ses utilisateurs finaux.

Des règles supplémentaires peuvent s'appliquer aux filiales d'AMG et aux utilisateurs finaux d'AMG qui résident dans l'Union européenne (UE) et sont soumis au Règlement général sur la protection des données (RGPD) de l'UE concernant la protection des données personnelles.

Chaque utilisateur final d'AMG doit se conformer à cette directive. Si des preuves d'une violation de cette directive sont trouvées, cela sera considéré comme une faute grave. La violation de cette directive peut entraîner des mesures disciplinaires, y compris le licenciement, sans préjudice de toute autre action civile ou pénale qui pourrait être entreprise.

Bonnes pratiques pour les utilisateurs finaux de l'AMG

AMG a défini des principes directeurs et des priorités dans sa politique globale en matière d'informatique et de cybersécurité - pour l'ensemble de la direction des filiales AMG et ses services informatiques - qui visent spécifiquement à renforcer la cybersécurité au sein d'AMG.

Les Bonnes Pratiques suivantes sont établies pour être utilisées par les utilisateurs finaux d'AMG. Chaque bonne pratique est également importante pour maintenir une défense solide contre les incidents cybercriminels. Les utilisateurs finaux d'AMG doivent suivre à tout moment les procédures et instructions de leur service informatique local.

Les bonnes pratiques :

1. Réfléchissez avant de cliquer : ne cliquez pas sur des liens inconnus, des fenêtres pop-up ou des téléchargements.
2. Utilisez des mots de passe forts et complexes, conformément aux instructions de votre service informatique. Les mots de passe sont confidentiels - ne les partagez jamais.
3. Ne désactivez jamais ou ne tentez jamais de compromettre un mécanisme de cybersécurité.
4. Stockez en toute sécurité les informations confidentielles, telles que définies par votre unité ou votre responsable, et ne recueillez pas d'informations dont vous n'avez pas besoin.
5. Ne laissez pas votre équipement informatique AMG sans surveillance. Protégez AMG contre le vol de matériel et de données.
6. Votre ordinateur et vos appareils AMG doivent être utilisés à des fins professionnelles pour AMG. Toutefois, une utilisation personnelle limitée et raisonnable est autorisée. Votre ordinateur et vos appareils sont la propriété de l'entreprise AMG et ne doivent utiliser que des logiciels approuvés par AMG.
7. N'envoyez des fichiers confidentiels que lorsque cela est nécessaire et, si possible, sous forme cryptée. Si vous envoyez des fichiers volumineux, utilisez un transfert de données sécurisé. Veuillez contacter votre responsable et/ou votre service informatique local pour obtenir des directives.
8. N'utilisez pas d'USB, de CD, de DVD ou de disques durs à moins qu'ils ne soient approuvés par la direction informatique et ne connectez pas d'équipement non AMG au réseau d'AMG.
9. Gardez un bureau propre et bien rangé au bureau et lorsque vous travaillez à domicile.
10. Signalez toute activité informatique suspecte à votre responsable, au service informatique et/ou au service juridique et de conformité.

Utilisation acceptable des ordinateurs, des équipements et des services de téléphonie mobile de l'AMG.

Toutes les TI d'AMG sont fournies aux utilisateurs finaux d'AMG à des fins professionnelles. Une utilisation personnelle limitée de ces installations est autorisée à condition qu'elle soit consacrée à des questions d'ordre privé et qu'elle soit raisonnable (c'est-à-dire qu'elle ne porte pas atteinte au travail de l'utilisateur final d'AMG, n'occupe pas une quantité anormale de temps ou d'espace, n'entraîne pas de coûts indus pour AMG et ne porte pas atteinte à la réputation d'AMG).

Les utilisateurs finaux d'AMG ne téléchargeront pas, ne stockeront pas, ne publieront pas, ne diffuseront pas ou ne distribueront pas de matériel provenant d'Internet ou de tout autre média électronique, qui est en général jugé inapproprié (y compris tout matériel jugé inapproprié conformément aux directives relatives aux médias sociaux ou au code de conduite des affaires d'AMG). En outre, les utilisateurs finaux d'AMG ne doivent pas utiliser l'équipement d'AMG d'une manière qui constitue des activités illégales ou criminelles en vertu de la loi applicable.

Contrôle de l'utilisation

Afin de gérer ses systèmes informatiques et de renforcer la sécurité, AMG peut - dans la mesure où la loi applicable le permet - enregistrer l'activité de l'utilisateur final d'AMG. Les raisons d'entreprendre une telle surveillance seront en général limitées à : assurer le fonctionnement efficace du système ;

enquêter ou détecter l'utilisation non autorisée des systèmes ; prévenir ou détecter les délits ; et enquêter sur les violations suspectées ou connues de la présente Ligne directrice.

Rapports d'incidents et communication

Les utilisateurs finaux d'AMG doivent informer **rapidement** leur direction locale et le responsable ou le service informatique local de toute violation présumée ou avérée de la présente directive. De tels événements peuvent inclure, mais ne sont pas limités à :

- des événements ou incidents inhabituels ou perturbateurs en matière de cybersécurité ;
- d'éventuels incidents de cybersécurité informatique tels que des courriels suspects ;
- la perte, les dommages ou l'altération présumée du matériel ou du logiciel d'AMG ;
- la divulgation présumée d'informations sensibles ou confidentielles, y compris de données personnelles ;
- Les vulnérabilités en matière de cybersécurité susceptibles d'avoir un impact sur les informations ou les systèmes d'AMG.

La direction locale informera rapidement le conseil d'administration de l'AMG de tout incident ou événement de ce type.

Cette obligation de déclaration est essentielle car AMG peut avoir l'obligation d'informer des tiers et des autorités si des données personnelles sont compromises à la suite d'un incident de cybersécurité.

Dans les situations urgentes ou sensibles où vous avez besoin de conseils ou si vous avez des préoccupations qui ne peuvent être traitées par votre direction locale ou votre service informatique, veuillez contacter le bureau de conformité d'AMG (à l'attention du responsable de la conformité d'AMG : compliance@amg-nv.com) conformément à la politique de dénonciation d'AMG, disponible sur le site Web d'AMG.

Résiliation du contrat de travail

Lorsqu'un utilisateur final d'AMG cesse de travailler pour AMG pour quelque raison que ce soit, tous les équipements, données et documents d'AMG doivent être restitués sans délai. Tous les privilèges du système d'information et l'accès aux informations et aux dispositifs informatiques seront immédiatement résiliés.

L'utilisateur final d'AMG doit :

- restituer tout le matériel fourni par AMG (par exemple, ordinateur portable, clés USB, téléphone portable/intelligent) ;
- retourner toutes les informations relatives à l'AMG, qu'elles soient numériques, analogiques (c'est-à-dire des enregistrements et/ou des CD, DVD) ou sur papier.

Contrôle de la version

Version	*Date*	*Qui est impliqué ?*	*Principaux changements*
0.1	2 février 2022	Rainer Steger (RS)	Configuration principale du document
0.2	8 février 2022	Projet Moore	Examen et apport des meilleures pratiques
0.3	Février10 2022	RS et Ludo Mees (LM)	Examen de l'entrée du projet Moore et des modifications supplémentaires
0.4	17 février 2022	Michelle Witton et RS	Examen des bonnes pratiques
0.5	25 février 2022	Jackson Dunckel (JD)	Examen final et approbation
1.0	25 février 2022	JD, LM, RS	Version finale