Diretriz Global de TI e Segurança Cibernética da AMG para Usuários Finais

Introdução

A informação é um ativo essencial da AMG. Na nossa prática empresarial diária, a informação é compartilhada com muitas pessoas dentro e fora da empresa para preparar e tomar decisões ou para cumprir regras e regulamentos. Algumas dessas informações são críticas para as atividades da AMG e, portanto, são sensíveis e precisam ser protegidas.

Esta Diretriz Global de TI e Segurança Cibernética da AMG para Usuários Finais ("**a Diretriz**") destina-se a ser uma diretriz geral sobre o uso e proteção da Tecnologia da Informação (relacionada a escritório e comunicação e tecnologia da informação relacionada à Tecnologia Operacional ou "OT" em inglês) e Segurança Cibernética. Nesta Diretriz, a referência aos ativos de TI da AMG deve ser entendida como se referindo também aos ativos OT da empresa.

Escopo

Esta Diretriz se aplica a toda à AMG-Advanced Metallurgical Group NV e/ou suas subsidiárias próprias ou controladas e entidades afiliadas ("**AMG**") e a seus empregados, diretores, executivos, agentes ou quaisquer outras pessoas que, sob a autoridade direta da AMG, façam uso de uso de quaisquer sistemas de TI e/ou relacionados, *hardware*, serviços, instalações e processos de propriedade ou de outra forma disponibilizados pela AMG NV ou pelas subsidiárias em seu nome, seja utilizando as redes da AMG, servidores ou aqueles fornecidos através de ambientes baseados em nuvem ("**usuários finais da AMG**").

Além disso, a Diretriz se aplica a quaisquer dispositivos de propriedade pessoal que sejam usados em conexão com as atividades da AMG, desde que o uso desses dispositivos tenha sido aprovado pela gestão local da AMG.

Propósito

A AMG investe continuamente em medidas para manter e proteger sua tecnologia da informação e sistemas de comunicação e para proteger a integridade de seus dispositivos e sistemas de TI e segurança cibernética. O objetivo desta Diretriz é preservar o valor e a reputação da AMG, protegendo a disponibilidade, integridade e confidencialidade de suas informações e estabelecer uma estrutura para:

- Conscientização pelos usuários finais da AMG sobre a necessidade de medidas de TI e segurança cibernética, para garantir que eles entendam a importância da informação e proteção de dados e questões de segurança da informação e dados;
- Gestão de riscos associados a TI e segurança cibernética através de boas práticas;
- Manuseio seguro de informações e uso de serviços de informação;
- Conformidade com os requisitos de TI e segurança cibernética da AMG e padrões aceitos do setor; e
- Cumprimento desta Diretriz.

Governança e cumprimento

O Conselho de Administração da AMG revisou e aprovou esta Diretriz como parte e em adição à POLÍTICA GLOBAL DE TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA da AMG (**"Política Global de TI e Segurança Cibernética"**), que detalha os princípios básicos pelos quais a AMG e seu grupo global de subsidiárias devem gerenciar e proteger a tecnologia da informação, os dados e os recursos da empresa.

A gestão local das subsidiárias da AMG é responsável pela adoção e conformidade com esta Diretriz em sua organização, implementando a Política e Diretriz Global de TI e Segurança Cibernética da AMG, de acordo com as leis e regulamentos locais aplicáveis, informar os usuários finais sobre esta Diretriz e fornecer treinamento regular aos seus usuários finais.

Regras adicionais podem ser aplicadas às subsidiárias da AMG e aos usuários finais da AMG que residem na União Europeia (UE) e estão sujeitos ao Regulamento Geral de Proteção de Dados da UE (GDPR) relativo à proteção de dados pessoais.

Cada usuário final da AMG deve cumprir esta Diretriz. Se forem encontradas evidências de uma violação desta Diretriz, isso será visto como falta grave. A violação desta Diretriz pode levar a ação disciplinar, incluindo demissão, não obstante qualquer outra ação civil ou criminal que possa ser realizada.

Boas Práticas para usuários finais da AMG

A AMG definiu princípios orientadores e prioridades em sua Política Global de TI e Segurança Cibernética - para toda a gestão de subsidiárias da AMG e seus departamentos de TI - que visam especificamente aprimorar a segurança cibernética dentro da AMG.

As seguintes Boas Práticas são estabelecidas para uso pelos usuários finais da AMG. Cada Boa Prática é igualmente importante para manter uma defesa consistente contra incidentes de crimes cibernéticos. Os usuários finais da AMG devem sempre seguir os procedimentos e instruções do departamento de TI local.

Boas práticas:

1. Pense antes de clicar: não clique em *links*, *pop-ups* ou *downloads* desconhecidos.
2. Use senhas fortes e complexas, conforme instruído pelo seu departamento de TI. As senhas são confidenciais – nunca as compartilhe.
3. Nunca desabilite ou tente comprometer qualquer mecanismo de segurança cibernética.
4. Armazene com segurança as informações confidenciais, conforme definido por sua unidade ou gerente, e não colete informações que você não precisa.
5. Não deixe seu computador da AMG sem vigilância. Proteja a AMG contra roubo de equipamentos e dados.
6. Seu computador e dispositivos AMG devem ser usados para fins comerciais da AMG. No entanto, o uso pessoal razoável limitado é permitido. Seu computador e dispositivos são propriedade da empresa AMG e devem usar somente *softwares* aprovados pela AMG.
7. Envie arquivos confidenciais somente quando necessário e, se possível, criptografados. Se enviar arquivos grandes, use a transferência segura de dados. Entre em contato com seu gerente e/ou TI local para obter orientações.
8. Não use USBs, CDs, DVDs ou discos rígidos, a menos que sejam aprovados pela gestão de TI e não conecte equipamentos que não sejam da AMG à rede da AMG.
9. Mantenha uma mesa de trabalho limpa e organizada no escritório e ao trabalhar em casa.
10. Relate qualquer atividade suspeita de TI ao seu gerente, departamento de TI e/ou Jurídico e *Compliance*.

Uso aceitável de computador, celular, equipamento e serviços AMG.

Todas as Tecnologias da Informação da AMG são fornecidas aos usuários finais da AMG para fins comerciais. O uso pessoal limitado dessas instalações é permitido desde que tal uso seja dedicado a assuntos privados e seja razoável (ou seja, não prejudicará o trabalho do usuário final da AMG, não tome muito tempo ou espaço, não incorra em custos indevidos para a AMG ou prejudique a reputação da AMG).

Os usuários finais da AMG não devem baixar, armazenar, publicar, divulgar ou distribuir qualquer material da Internet ou qualquer outra mídia eletrônica que seja geralmente considerada inadequada (incluindo qualquer material considerado inadequado de acordo com as Diretrizes de Mídia Social da AMG ou Código de Conduta. Além disso, os usuários finais da AMG não devem usar equipamentos da AMG de maneira que constitua atividades ilegais ou criminosas de acordo com leis aplicáveis.

Monitoramento de uso

Para gerenciar seus sistemas de TI e reforçar a segurança, a AMG pode – até onde permitido pela lei aplicável – registrar a atividade do usuário final da AMG. As razões para realizar tal monitoramento serão, em geral, limitadas a: garantir a operação efetiva do sistema; investigar ou detectar o uso não autorizado dos sistemas; prevenir ou detectar crimes; e investigação de violações suspeitas ou conhecidas desta Diretriz.

Relato e Comunicação de Incidente

Os usuários finais da AMG devem informar **imediatamente** sua gerência local e gerente de TI local ou departamento de TI sobre todas e quaisquer violações suspeitas ou conhecidas desta Diretriz. Tais eventos podem incluir, mas não estão limitados a:

- Eventos ou incidentes incomuns ou prejudiciais de segurança cibernética;
- Possíveis incidentes de segurança cibernética de TI, como e-mails suspeitos;
- Perda, dano ou suspeita de adulteração de *hardware* ou *software* da AMG;
- Suspeita de divulgação de informações sensíveis ou confidenciais, incluindo dados pessoais;
- Vulnerabilidades de segurança cibernética que podem afetar as informações ou os sistemas da AMG.

A gestão local informará prontamente o Conselho de Administração da AMG sobre qualquer incidente ou evento.

Essa obrigação de comunicação é fundamental, pois a AMG pode ter obrigações de informar terceiros e autoridades caso os dados pessoais sejam comprometidos como resultado de qualquer incidente de segurança cibernética.

Em situações urgentes ou delicadas em que você precisar de aconselhamento ou se tiver dúvidas que não podem ser tratadas por meio de sua gerência local ou departamento de TI, entre em contato com o escritório de *Compliance* Corporativa da AMG (em atenção ao Diretor de *Compliance* da AMG: compliance@amg-nv.com) de acordo com a Política de Manifestação e Denúncia da AMG, disponível no site da AMG.

Fim de contrato

Quando um usuário final da AMG deixa de trabalhar para a AMG por qualquer motivo, todos os equipamentos, dados e documentos da AMG devem ser devolvidos imediatamente, assim como todos os privilégios do sistema de informação e acesso às informações e aos dispositivos de TI serão retirados.

O usuário final da AMG deve:

- devolver todo o equipamento fornecido pela AMG (por exemplo: *notebook*, *desktop*, *smartphone* e acessórios);
- devolver todas as informações relacionadas à AMG, sejam digitais, analógicas (ou seja, gravações e/ou CDs, DVDs) ou impressas.

Controle de Versões

Versão	***Data***	***Pessoas envolvidas***	***Principais mudanças***
0.1	02 de fevereiro de 2022	Rainer Steger (RS)	Configuração principal do documento
0.2	8 de fevereiro de 2022	Project Moore	Revisão e inserção de melhores práticas
0.3	10 de fevereiro de 2022	RS e Ludo Mees (LM)	Revisão de inserção do Projeto Moore Project Moore e mudanças adicionais
0.4	17 de fevereiro de 2022	Michelle Witton e RS	Revisão de Boas Práticas
0.5	25 de fevereiro de 2022	Jackson Dunckel (JD)	Revisão final e aprovação
1.0	25 de fevereiro de 2022	JD, LM, RS	Versão final