Lineamientos Globales de AMG para usuarios finales sobre TI y Ciberseguridad.

Introducción

La información es un activo esencial de AMG. En nuestra práctica empresarial diaria, la información se comparte con muchas personas dentro y fuera de la empresa para preparar y tomar decisiones o para cumplir con las normas y lineamientos. Parte de esta información es crítica para las actividades de AMG y es, por tanto, sensible y necesita ser protegida.

Estos Lineamientos globales de AMG sobre TI y ciberseguridad para el usuario final ("Lineamientos ") pretende ser los Lineamientos generales sobre el uso y la protección de las tecnologías de la información (tanto las relacionadas con la oficina y la comunicación, o "TI", como las relacionadas con las operaciones y la producción, o "OT") y la ciberseguridad. En esta Política, la referencia a las TI y a los activos de TI de AMG debe entenderse que también se refiere a los activos de OT y de OT de la empresa.

Alcance

Estos Lineamientos aplica a todo AMG Advanced Metallurgical Group NV y/o sus filiales y entidades afiliadas de su propiedad o control ("**AMG**") y a sus empleados, directores, funcionarios, agentes y cualquier otra persona que, bajo la autoridad directa de AMG, haga uso de cualquier sistema de TI y/o sistemas relacionados, hardware, servicios, instalaciones y procesos que sean propiedad de AMG NV o de las filiales en su nombre, ya sea que utilicen las redes de AMG, los servidores o los proporcionados a través de entornos basados en la nube ("**usuarios finales de AMG**").

Además, aplica a cualquier dispositivo de propiedad personal que se utilice en relación con las actividades de AMG, siempre que el uso de estos dispositivos haya sido aprobado por la dirección general local de AMG.

Objetivo

AMG invierte continuamente en medidas para mantener y proteger sus sistemas de tecnología de la información y comunicación y para proteger la integridad de sus dispositivos y sistemas de TI y ciberseguridad. El objetivo de estos Lineamientos es preservar el valor y la reputación de AMG protegiendo la disponibilidad, integridad y confidencialidad de su información y establecer un marco para:

- Concientizacion por parte de los usuarios finales de AMG de la necesidad de adoptar medidas de TI y Ciberseguridad, con el fin de que comprendan la importancia de la protección de la información y de los datos y de las cuestiones de seguridad de la información y de los datos;
- Gestión de los riesgos asociados a la informática y la ciberseguridad mediante buenas prácticas
- Manejo seguro de la información y uso de los servicios de información
- Cumplimiento de los requisitos de TI y Ciberseguridad de AMG y de las normas aceptadas del sector; y
- Aplicación de estos Lineamientos.

Gobierno y aplicación de la Ley

El Consejo de Administración de AMG ha revisado y aprobado esta Política como parte de la POLÍTICA GLOBAL DE TECNOLOGÍA DE LA INFORMACIÓN Y CIBERSEGURIDAD DE AMG ("**Política Global de Tecnología de la Información y Ciberseguridad**"), que detalla los principios subyacentes por los que

AMG y su grupo global de filiales deben gestionar y salvaguardar la tecnología de la información, los datos y los recursos de la empresa.

La dirección general local de las filiales de AMG es responsable de la adopción y el cumplimiento de los Lineamientos dentro de su organización mediante la aplicación de la Política Global de TI y Ciberseguridad de AMG y Lineamientos de acuerdo con las leyes y reglamentos locales aplicables, informar a los usuarios finales sobre los Lineamientos y proporcionar formación periódica a sus usuarios finales.

Pueden aplicarse normas adicionales para las filiales de AMG y los usuarios finales de AMG que residen en la Unión Europea (UE) y están sujetos al Reglamento General de Protección de Datos (RGPD) de la UE relativo a la protección de datos personales.

Cada usuario final de AMG debe cumplir con estos Lineamientos. Si se encuentran pruebas de una infracción de los Lineamientos, se considerará una falta grave. La infracción puede dar lugar a medidas disciplinarias, incluido el despido, sin perjuicio de cualquier otra acción civil o penal que pueda emprenderse.

Buenas prácticas para los usuarios finales de AMG

AMG ha definido principios rectores y prioridades en su Política Global de TI y Ciberseguridad - para toda la dirección general de las filiales de AMG y sus departamentos de TI - que tienen como objetivo específico mejorar la Ciberseguridad dentro de AMG.

Las siguientes Buenas Prácticas se establecen para ser utilizadas por los usuarios finales de AMG. Cada una de las Buenas Prácticas es igualmente importante para mantener una defensa robusta ante incidentes de Cibercrimen. Los usuarios finales de AMG deberán seguir en todo momento los procedimientos e instrucciones de su departamento local de TI.

Buenas prácticas:

1. Piensa antes de hacer clic: no hagas clic en enlaces desconocidos, ventanas emergentes o descargas.
2. Utilice contraseñas fuertes y complejas, según las instrucciones de su departamento de TI. Las contraseñas son confidenciales: no las compartas nunca.
3. Nunca desactive ni intente comprometer ningún mecanismo de ciberseguridad.
4. Almacena de forma segura la información confidencial, según lo definido por tu unidad o director, y no recojas información que no necesites.
5. No deje el equipo informático de AMG sin vigilancia. Proteja a AMG contra el robo de equipos y datos.
6. El ordenador y los dispositivos de AMG deben utilizarse para fines empresariales de AMG. Sin embargo, se permite un uso personal limitado y razonable. Su ordenador y dispositivos son propiedad de la empresa AMG y sólo debe utilizar el software aprobado por AMG.
7. Envíe archivos confidenciales sólo cuando sea necesario y, si es posible, de forma encriptada. Si envía archivos de gran tamaño, utilice una transferencia de datos segura. Póngase en contacto con su gerente y/o con el departamento de TI local para conocer las directrices.
8. No utilice USBs, CDs, DVDs o discos duros a menos que sean aprobados por la dirección general de TI y no conecte equipos que no sean de AMG a la red de AMG.
9. Mantenga un escritorio de trabajo limpio y ordenado en la oficina y cuando trabaje desde casa.
10. Informe de cualquier actividad sospechosa de TI a su gerente, al departamento de TI y/o a Legal & Compliance.

Uso aceptable de los ordenadores, teléfonos móviles y servicios de AMG

Todos los equipos informáticos de AMG se proporcionan a los usuarios finales de AMG para fines empresariales. Se permite un uso personal limitado de estas instalaciones siempre que dicho uso se dedique a asuntos privados y sea razonable (es decir, que no perjudique el trabajo del usuario final de AMG, que no ocupe una cantidad anormal de tiempo o espacio, que no incurra en costos indebidos para AMG o que no perjudique la reputación de AMG).

Los usuarios finales de AMG no descargarán, almacenarán, publicarán, difundirán o distribuirán ningún material de Internet o de cualquier otro medio electrónico, que en general se considere inapropiado (incluyendo cualquier material que se considere inapropiado de acuerdo con los Lineamientos de Medios Sociales o el Código de Conducta Empresarial de AMG). Además, los usuarios finales de AMG no utilizarán los equipos de AMG de forma que constituyan actividades ilegales o delictivas según la legislación aplicable.

Supervisión del uso

Con el fin de gestionar sus sistemas informáticos y reforzar la seguridad, AMG podrá -en la medida permitida por la legislación aplicable- registrar la actividad de los usuarios finales de AMG. Las razones para llevar a cabo dicha monitorización se limitarán, en general, a: garantizar el funcionamiento eficaz del sistema; investigar o detectar el uso no autorizado de los sistemas; prevenir o detectar delitos; e investigar las infracciones sospechosas o conocidas de estos Lineamientos..

Notificación y comunicación de incidentes

Los usuarios finales de AMG informarán **sin demora** a su dirección general local y al director o departamento de TI local de todas las infracciones sospechosas o conocidas de estos Lineamientos. Tales eventos pueden incluir, pero no están limitados a:

- Eventos o incidentes de Ciberseguridad inusuales o perturbadores;
- Posibles incidentes de ciberseguridad informática, como correos electrónicos sospechosos;
- Pérdida, daño o sospecha de manipulación del hardware o software de AMG;
- Sospecha de divulgación de información sensible o confidencial, incluidos los datos personales;
- Vulnerabilidades de ciberseguridad que puedan afectar a la información o los sistemas de AMG.

La dirección general local informará sin demora al Consejo de Administración de AMG de cualquier incidente o evento de este tipo.

Esta obligación de informar es fundamental ya que AMG puede tener la obligación de informar a terceros y a las autoridades en caso de que los datos personales se vean comprometidos como resultado de cualquier incidente de Ciberseguridad.

En situaciones urgentes o delicadas en las que necesite asesoramiento o si tiene preocupaciones que no pueden ser abordadas a través de su dirección general local o departamento de TI, por favor, póngase en contacto con la oficina de Cumplimiento Corporativo de AMG (a la atención del Jefe de Cumplimiento de AMG: compliance@amg-nv.com) de acuerdo con la política de AMG Speak Up & Reporting Policy, disponible en la página web de AMG.

Termino de relación laboral

Cuando un usuario final de AMG deja de trabajar para AMG por cualquier motivo, todos los equipos, datos y documentos de AMG deben ser devueltos sin demora. Todos los privilegios del sistema de información y el acceso a la información y a los dispositivos informáticos se terminarán inmediatamente.

El usuario final de AMG deberá

- devolver todo el equipo proporcionado por AMG (por ejemplo, ordenador portátil, llaves de memoria USB, móvil / teléfono inteligente);
- devolver toda la información relacionada con AMG, ya sea digital, analógica (es decir, grabaciones y/o CDs, DVDs) o impresa.

Versiones

Version	*Date*	*Who involved?*	*Main changes*
0.1	February 2, 2022	Rainer Steger (RS)	Main setup of the document
0.2	February 8, 2022	Project Moore	Review and input best practices
0.3	February 10, 2022	RS and Ludo Mees (LM)	Review of input Project Moore and additional changes
0.4	February 17, 2022	Michelle Witton and RS	Review of Good Practices
0.5	February 25, 2022	Jackson Dunckel (JD)	Final review and approval
1.0	February 25, 2022	JD, LM, RS	Final version