Globale Endbenutzer-Leitlinie für IT- und Cybersicherheit von AMG

Einführung

Informationen sind ein wesentlicher Vermögenswert von AMG. In unserem täglichen Geschäftsbetrieb werden Informationen mit vielen Menschen innerhalb und außerhalb des Unternehmens ausgetauscht, um Entscheidungen vorzubereiten und zu treffen oder um Regeln und Vorschriften einzuhalten. Einige dieser Informationen sind für die Tätigkeiten von AMG entscheidend und sind daher sensibel und müssen geschützt werden.

Diese globale Endbenutzer-Leitlinie für IT- und Cybersicherheit von AMG („**die Leitlinie**“) dient als allgemeine Richtlinie für die Nutzung und den Schutz der Informationstechnologie (sowohl Office-bezogene als auch kommunikationsbezogene IT oder „IT“ als auch operative und produktionsbezogene IT oder „OT“) und Cybersicherheit. In dieser Leitlinie sind Bezugnahmen auf die IT und IT-Assets von AMG auch als Bezugnahmen auf die OT und OT-Assets des Unternehmens zu verstehen.

Geltungsbereich

Diese Leitlinie gilt für alle AMG Advanced Metallurgical Group NV und/oder die in ihrem Besitz befindlichen oder von ihnen kontrollierten Tochtergesellschaften und verbundenen Unternehmen („**AMG**“) und für ihre Mitarbeiter, Geschäftsleitungsmitglieder, Organvertreter, Vertreter und alle anderen Personen, die unter der unmittelbaren Verantwortung von AMG IT- und/oder zugehörige Systeme, Hardware, Dienstleistungen, Anlagen und Prozesse benutzen, die sich im Besitz von AMG NV oder den Tochtergesellschaften befinden oder die anderweitig von AMG NV oder den Tochtergesellschaften in ihrem Auftrag zur Verfügung gestellt werden, unabhängig davon, ob sie die Netzwerke oder Server von AMG oder Cloud-basierte Netzwerke oder Server nutzen („**AMG-Endbenutzer**“).

Ferner gilt die Leitlinie für alle in persönlichem Besitz befindlichen Geräte, die in Verbindung mit den Tätigkeiten von AMG verwendet werden, sofern die Nutzung dieser Geräte vom lokalen AMG-Management genehmigt wurde.

Zweck

AMG investiert kontinuierlich in Maßnahmen, um ihre IT- und Kommunikationssysteme zu pflegen und zu schützen und um die Integrität ihrer IT- und Cybersicherheitsgeräte und -systeme zu schützen. Ziel dieser Leitlinie ist es, den Wert und das Ansehen von AMG durch den Schutz der Verfügbarkeit, Integrität und Vertraulichkeit ihrer Informationen zu erhalten und einen Rahmen festzulegen für:

- das Bewusstsein der AMG-Endbenutzer für die Notwendigkeit von IT- und Cybersicherheitsmaßnahmen, um zu gewährleisten, dass sie die Bedeutung des Schutzes der Informationen und Daten und der Informations- und Datensicherheitsaspekte verstehen;
- das Management der mit der IT- und Cybersicherheit verbundenen Risiken durch bewährte Praktiken;
- den sicheren Umgang mit Informationen und die sichere Nutzung von Informationsdiensten;
- die Einhaltung der IT- und Cybersicherheitsanforderungen von AMG und der anerkannten Branchenstandards; und
- die Durchsetzung dieser Leitlinie.

Geltung und Durchsetzung

Der Vorstand von AMG hat diese Leitlinie im Rahmen und als Ergänzung der GLOBALEN RICHTLINIE FÜR IT- UND CYBERSICHERHEIT (**„Globale IT- und Cybersicherheitsrichtlinie“**) überprüft und genehmigt, in der die Grundprinzipien aufgeführt sind, gemäß denen AMG und ihre weltweit operierende Gruppe von Tochtergesellschaften die IT, Daten und Ressourcen des Unternehmens verwalten und schützen.

Das lokale Management der Tochtergesellschaften von AMG ist für die Verabschiedung und Einhaltung dieser Leitlinie innerhalb ihres Unternehmens durch Umsetzung der globalen IT- und Cybersicherheitsleitlinie von AMG in Übereinstimmung mit den geltenden lokalen Gesetzen und Vorschriften verantwortlich, muss die Endbenutzer über diese Leitlinie informieren und regelmäßige Schulungen für ihre Endbenutzer anbieten.

Zusätzliche Regelungen können für Tochtergesellschaften von AMG und AMG-Endbenutzer gelten, die innerhalb der Europäischen Union (EU) ansässig sind und der Datenschutz-Grundverordnung der EU (DSGVO) in Bezug auf den Schutz personenbezogener Daten unterliegen.

Jeder AMG-Endbenutzer muss diese Leitlinie befolgen. Eine nachweisliche Verletzung dieser Leitlinie wird als schwerwiegendes Fehlverhalten angesehen. Die Verletzung dieser Leitlinie kann zu Disziplinarmaßnahmen einschließlich Entlassung führen und darüber hinaus können zivil- oder strafrechtliche Klagen erhoben werden.

Bewährte Praktiken für AMG-Endbenutzer

AMG hat in ihrer globalen IT- und Cybersichtsheitsrichtlinie für das Management aller AMG-Tochtergesellschaften und ihre IT-Abteilungen Leitprinzipien und Prioritäten festgelegt, die speziell dazu dienen sollen, die Cybersicherheit bei AMG zu verbessern.

Die folgenden bewährten Praktiken wurden für die Verwendung durch AMG-Endbenutzer erstellt: Jede bewährte Praktik ist gleichermaßen wichtig, um eine zuverlässige Abwehr von Fällen von Internet-Kriminalität aufrechtzuerhalten. AMG-Endbenutzer müssen jederzeit die Verfahren und Anweisungen von ihrer lokalen IT-Abteilung befolgen.

Bewährte Praktiken:

1. Denken Sie, bevor Sie klicken: Klicken Sie nicht auf unbekannte Links, Pop-ups oder Downloads.
2. Verwenden Sie starke, komplexe Passwörter gemäß den Anweisungen Ihrer IT-Abteilung. Passwörter sind vertraulich – geben Sie sie nie an Dritte weiter.
3. Deaktivieren Sie nie einen Cybersicherheitsmechanismus und versuchen Sie nie, seine Funktion zu gefährden.
4. Bewahren Sie vertrauliche Informationen gemäß den Anweisungen Ihrer Einheit oder Ihres Vorgesetzten sicher auf und sammeln Sie keine Informationen, die Sie nicht benötigen.
5. Lassen Sie Ihre AMG-Computerausrüstung nicht unbeaufsichtigt. Schützen Sie AMG vor Diebstahl von Ausrüstung und Daten.
6. Ihre AMG-Computer und -Geräte sind für geschäftliche Zwecke von AMG zu benutzen. Eine beschränkte Nutzung für private Zwecke ist jedoch in angemessenem Rahmen zulässig. Ihre Computer und Geräte sind Eigentum von AMG und auf ihnen darf nur von AMG zugelassene Software verwendet werden.
7. Senden Sie vertrauliche Dateien nur, wenn dies notwendig ist und wenn möglich in verschlüsselter Form. Falls Sie große Dateien senden, nutzen Sie eine sichere Datenübertragung. Bitte wenden Sie sich an Ihren Vorgesetzten und/oder Ihre lokale IT, um die genaue Vorgehensweise zu erfahren.
8. Verwenden Sie keine USB-Sticks, CDs, DVDs oder Festplatten, sofern sie nicht vom IT-Management genehmigt wurden, und verbinden Sie keine nicht von AMG stammenden Geräte mit dem Netzwerk von AMG.
9. Halten Sie Ihren Arbeitsplatz im Büro und im Homeoffice sauber und ordentlich.
10. Melden Sie Ihrem Vorgesetzten, Ihrer IT-Abteilung und/oder der Rechts- und Compliance-Abteilung alle verdächtigen IT-Aktivitäten.

Zulässige Nutzung von Computern, Mobilfunkgeräten und Dienstleistungen von AMG

Die gesamte IT von AMG wird AMG-Endbenutzern für geschäftliche Zwecke zur Verfügung gestellt. Eine beschränkte private Nutzung dieser Geräte ist zulässig, sofern diese Nutzung für private Angelegenheiten erfolgt und angemessen ist (d. h. dass sie die Arbeit des AMG-Endbenutzers nicht beeinträchtigt, keinen ungewöhnlich hohen zeitlichen oder räumlichen Aufwand verursacht und dass AMG keine unangemessenen Kosten entstehen und dass sie dem Ansehen von AMG nicht schaden).

AMG-Endbenutzer dürfen keine Materialien aus dem Internet oder sonstige elektronische Medien, die im Allgemeinen als unangemessen gelten (darunter Materialien, die gemäß den Social-Media-Leitlinien oder dem Verhaltenskodex von AMG als unangemessen gelten) herunterladen, speichern, veröffentlichen, verbreiten oder verteilen. Ferner dürfen AMG-Endbenutzer AMG-Geräte nicht in einer Weise nutzen, die nach geltendem Recht illegale oder kriminelle Aktivitäten darstellt.

Überwachung der Nutzung

Um ihre IT-Systeme zu verwalten und die Sicherheit zu erhöhen, darf AMG – im gesetzlich zulässigen Rahmen – die Aktivität des AMG-Endbenutzers aufzeichnen. Die Gründe für eine solche Überwachung sind grundsätzlich auf folgende beschränkt: Sicherstellung des reibungslosen Betriebs des Systems, Untersuchung oder Aufdeckung der unbefugten Nutzung des Systems, Verhütung oder

Aufdeckung von Straftaten und Untersuchung von vermuteten oder bekannten Verletzungen dieser Leitlinie.

Meldung und Berichterstattung von Vorfällen

AMG-Endbenutzer müssen ihr lokales Management und ihren lokalen IT-Manager oder ihre IT-Abteilung **unverzüglich** über sämtliche vermuteten oder bekannten Verletzungen dieser Leitlinie informieren. Zu diesen Ereignissen zählen unter anderem folgende:

- ungewöhnliche oder störende Cybersicherheitsereignisse oder -vorfälle;
- mögliche IT-Cybersicherheitsvorfälle wie beispielsweise verdächtige E-Mails;
- Verlust, Beschädigung oder vermutete Manipulation von Hardware oder Software von AMG;
- Verdacht einer Offenlegung von sensiblen oder vertraulichen Informationen, einschließlich personenbezogener Daten;
- Cybersicherheitsschwachstellen, die sich wahrscheinlich auf die Informationen oder Systeme von AMG auswirken.

Das lokale Management wird den Vorstand von AMG unverzüglich über derartige Vorfälle oder Ereignisse informieren.

Diese Meldepflicht ist entscheidend, da AMG möglicherweise verpflichtet ist, Dritte und Behörden zu informieren, falls es infolge eines Cybersicherheitsvorfalls zu einer Sicherheitsverletzung bei personenbezogenen Daten kommt.

In dringenden oder heiklen Situationen, wenn Sie Beratung benötigen oder Bedenken haben, die nicht über Ihr lokales Management oder Ihre IT-Abteilung ausgeräumt werden können, wenden Sie sich bitte an das Corporate Compliance Office von AMG (z. Hd. AMG Chief Compliance Officer: compliance@amg-nv.com) in Übereinstimmung mit der Melde- und Berichterstattungsrichtlinie von AMG, die auf der Website von AMG verfügbar ist.

Beendigung des Arbeitsverhältnisses

Wenn die Beschäftigung eines AMG-Endbenutzer bei AMG aus irgendeinem Grund endet, muss er alle Geräte, Daten und Dokumente von AMG unverzüglich zurückgeben. Alle Rechte in Bezug auf das Informationssystem und den Zugang zu Informationen und IT-Geräten enden mit sofortiger Wirkung.

Der AMG-Endbenutzer muss:

- alle von AMG bereitgestellten Geräte (z. B. Laptop, USB-Speichersticks, Mobiltelefon/Smartphone) zurückgeben;
- alle AMG-bezogenen Informationen zurückgeben, unabhängig davon, ob sie ihm in digitaler, analoger (d. h. Aufzeichnungen und/oder CDs, DVDs) oder in Papierform vorliegen.

Versionskontrolle

Version	*Datum*	*Beteiligte*	*Wichtigste Änderungen*
0.1	2. Februar 2022	Rainer Steger (RS)	Hauptstruktur des Dokuments
0.2	8. Februar 2022	Project Moore	Überprüfung und Input bewährte Praktiken
0.3	10. Februar 2022	RS und Ludo Mees (LM)	Überprüfung Input Project Moore und zusätzliche Änderungen
0.4	17. Februar 2022	Michelle Witton und RS	Überprüfung der bewährten Praktiken
0.5	25. Februar 2022	Jackson Dunckel (JD)	Abschließende Überprüfung und Genehmigung
1.0	25. Februar 2022	JD, LM, RS	Endgültige Version