AMG Global IT and Cybersecurity End-user Guideline

Introduction

Information is an essential asset of AMG. In our day-to-day business practice, information is shared with many people inside and outside of the company in order to prepare and take decisions or to comply with rules and regulations. Some of this information is critical to AMG's activities and is, therefore, sensitive and needs to be protected.

This AMG Global IT and Cybersecurity End-user Guideline ("**the Guideline**") is intended as a general guideline on the use and protection of Information Technology (both office and communication related IT or "IT", and operational and production related information technology or "OT") and Cybersecurity. In this Guideline, reference to AMG's IT and IT assets should be understood to also refer to the company's OT and OT assets.

Scope

This Guideline applies to all AMG Advanced Metallurgical Group NV and/or its owned or controlled subsidiaries and affiliated entities ("**AMG**") and to its employees, directors, officers, agents and any other persons whom, under the direct authority of AMG, make use of any IT and/or related systems, hardware, services, facilities and processes owned or otherwise made available by AMG NV or the subsidiaries on its behalf, whether utilizing AMG's networks, servers or those provided through cloud-based environments ("**AMG End-users**").

In addition, the Guideline applies to any personally owned devices that are used in connection with AMG's activities, provided the use of these devices has been approved by local AMG management.

Purpose

AMG continually invests in measures to maintain and protect its information technology and communication systems and to protect the integrity of its IT and Cybersecurity devices and systems. The objective of this Guideline is to preserve AMG's value and reputation by protecting the availability, integrity and confidentiality of its information and to establish a framework for:

- awareness by AMG End-users of the need for IT and Cybersecurity measures, to ensure they understand the importance of information and data protection and information and data security issues;
- management of risks associated with IT and Cybersecurity through good practices;
- secure handling of information and use of information services;
- compliance with AMG's IT and Cybersecurity requirements and accepted industry standards; and
- enforcement of this Guideline.

Governance and enforcement

The AMG Management Board has reviewed and approved this Guideline as part of and in addition to the AMG GLOBAL INFORMATION TECHNOLOGY AND CYBERSECURITY POLICY (**"Global IT and Cybersecurity Policy"**), which details the underlying principles by which AMG and its global group of subsidiaries shall manage and safeguard the company's IT, data and resources.

AMG's subsidiaries local management is responsible for adoption and compliance with this Guideline within their organization by implementing the AMG Global IT and Cybersecurity Policy and

Guideline, in accordance with applicable local laws and regulations, inform End-users regarding this Guideline and provide regular training to its End-users.

Additional rules may apply for AMG's subsidiaries and AMG End-users that reside within the European Union (EU) and are subject to the EU General Data Protection Regulation (GDPR) concerning the protection of personal data.

Each AMG End-user should comply with this Guideline. If evidence is found of a breach of this Guideline it will be viewed as serious misconduct. Violation of this Guideline may lead to disciplinary action, including dismissal, notwithstanding any further civil or criminal action which may be undertaken.

Good Practices for AMG End-users

AMG has defined guiding principles and priorities in its Global IT and Cybersecurity Policy - for all AMG subsidiary management and its IT departments - that specifically aim to enhance Cybersecurity within AMG.

The following Good Practices are established for use by AMG End-users. Each Good Practice is equally important to maintain a robust defense to Cybercrime incidents. AMG End-users shall follow at all times the procedures and instructions from their local IT department.

Good practices:

1. Think before you click: don't click on unknown links, pop-ups or downloads.
2. Use strong, complex passwords, as instructed by your IT department. Passwords are confidential – don't ever share them.
3. Never disable or attempt to compromise any cybersecurity mechanism.
4. Securely store confidential information, as defined by your unit or manager, and don't collect information you don't need.
5. Don't leave your AMG computer equipment unattended. Protect AMG against equipment and data theft.
6. Your AMG computer and devices are to be used for AMG business purposes. However, limited reasonable personal use is permitted. Your computer and devices are AMG company property and must only use AMG-approved software.
7. Send confidential files only when necessary and, if possible, as encrypted. If sending large files use secure data transfer. Please contact your manager and/or local IT for guidelines.
8. Do not use USBs, CDs, DVDs or hard drives unless they are approved by IT management and do not connect non-AMG equipment to AMG's network.
9. Keep a clean and tidy work desk in the office and when working from home.
10. Report any suspicious IT activity to your manager, IT department and/or Legal & Compliance.

Acceptable use of AMG computer, mobile phone equipment and services

All AMG IT are provided to AMG End-users for business purposes. Limited personal use of these facilities is permitted provided that such use is dedicated to private matters and is reasonable (i.e. it will not detract from the AMG End-user's work, take up an abnormal amount of time or space, incur undue costs for AMG or impair AMG's reputation).

AMG End-users shall not download, store, publish, disseminate or distribute any material from the internet or any other electronic media, that is in general deemed inappropriate (including any material that is deemed inappropriate pursuant to AMG's Social Media Guidelines or Code of Business Conduct). Furthermore, AMG End-users shall not use AMG equipment in a manner that constitutes illegal or criminal activities under applicable law.

Usage monitoring

In order to manage its IT systems and enforce security, AMG may – to the extent permitted by applicable law – log AMG End-user's activity. The reasons for undertaking such monitoring will in general be limited to: ensuring the effective operation of the system; investigating or detecting the unauthorized use of the systems; preventing or detecting crime; and investigation of suspected or known breaches of this Guideline.

Incident Reporting and Communication

AMG End-users shall **promptly** inform its local management and local IT manager or department of all and any suspected or known breaches of this Guideline. Such events may include, but are not limited to:

- unusual or disruptive Cybersecurity events or incidents;
- possible IT Cybersecurity incidents such as suspicious emails;
- loss, damage or suspected tampering with AMG hardware or software;
- suspected disclosure of sensitive or confidential information, including personal data;
- Cybersecurity vulnerabilities likely to impact AMG information or systems.

Local management will promptly inform the AMG Management Board of any such incident or event.

This reporting obligation is critical since AMG may have obligations to inform third parties and authorities in case personal data are compromised as a result of any Cybersecurity incident.

In urgent or sensitive situations where you require advice or if you have concerns that cannot be addressed through your local management or IT department, please contact the AMG's Corporate Compliance office (attn AMG Chief Compliance Officer: compliance@amg-nv.com) in accordance with the AMG Speak Up & Reporting Policy, available on AMG's website.

Termination of employment

When an AMG End-user ceases working for AMG for any reason, all AMG equipment, data and documents must be returned without delay. All information system privileges and access to information and to IT devices will be terminated immediately.

The AMG End-user must:

- return all equipment provided by AMG (e.g. laptop computer, USB memory key's, mobile / smart phone);
- return all AMG related information whether digital, analog (i.e. recordings and or CDs, DVDs) or hardcopy.

Version Control

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