AMG 全球 IT 和网络安全终端用户指南

介绍

信息是 AMG 的重要资产。在我们的日常业务实践中，信息与公司内外的许多人共享，以便准备和做出决策或遵守规则和法规。其中一些信息对 AMG 的活动至关重要，因此很敏感，需要加以保护。

本 AMG 全球 IT 和网络安全终端用户指南（“指南”）旨在作为使用和保护信息技术（办公和通信相关的 IT 或“IT”，以及运营和生产相关的信息技术或“OT”）和网络安全。在本指南中，提及 AMG 的 IT 和 IT 资产应理解为也指公司的 OT 和 OT 资产。

范围

本指南适用于所有 AMG Advanced Metallurgical Group NV 和/或其拥有或控制的子公司和附属实体（“AMG”）及其员工、董事、高级职员、代理人和任何其他在 AMG 直接授权下，使用 AMG NV 或其子公司代表其拥有或以其他方式提供的任何 IT 和/或相关系统、硬件、服务、设施和流程，无论是利用 AMG 的网络、服务器还是通过基于云的环境提供的网络、服务器（“AMG End -用户”）。

此外，该指南适用于与 AMG 活动相关的任何个人拥有的设备，前提是这些设备的使用已获得当地 AMG 管理层的批准。

目的

AMG 不断投资采取措施维护和保护其信息技术和通信系统，并保护其 IT 和网络安全设备和系统的完整性。

本指南的目的是通过保护其信息的可用性、完整性和机密性来维护 AMG 的价值和声誉，并建立一个框架：

- AMG 终端用户意识到 IT 和网络安全措施的必要性，以确保他们了解信息和数据保护以及信息和数据安全问题的重要性；
- 通过良好实践管理与 IT 和网络安全相关的风险；
- 安全处理信息和使用信息服务；
- 符合 AMG 的 IT 和网络安全要求以及公认的行业标准；
- 本指南的执行。

管理和执行

AMG 管理委员会已审查并批准本指南，作为 AMG 全球信息技术和网络安全政策（“全球 IT 和网络安全政策”）的一部分和补充，该政策详细说明了 AMG 及其全球子公司集团应遵循的基本原则管理和保护公司的 IT、数据和资源。

AMG 的子公司当地管理层负责通过实施 AMG 全球 IT 和网络安全政策和指南，根据适用的当地法律和法规，在其组织内采用和遵守本指南，告知终端用户有关本指南的信息，并为其提供定期培训。

其他规则可能适用于居住在欧盟 (EU) 内的 AMG 子公司和 AMG 终端用户，并受有关个人数据保护的欧盟通用数据保护条例 (GDPR) 的约束。

每个 AMG 终端用户都应遵守本指南。如果发现违反本指南的证据，将被视为严重的不当行为。违反本指南可能会导致纪律处分，包括解雇，尽管可能会采取任何进一步的民事或刑事诉讼。

AMG 终端用户的良好实践

AMG 在其全球 IT 和网络安全政策中为所有 AMG 子公司管理层及其 IT 部门定义了指导原则和优先事项，专门旨在加强 AMG 内部的网络安全。

为 AMG 终端用户制定了以下良好实践。每个良好实践对于保持对网络犯罪事件的强大防御同样重要。 AMG 终端用户应始终遵守当地 IT 部门的程序和指示。

良好做法：
1.点击前三思：不要点击未知链接、弹出窗口或下载。
2. 按照 IT 部门的指示使用强而复杂的密码。密码是机密的——永远不要分享它们。
3. 切勿禁用或试图破坏任何网络安全机制。
4. 安全地存储您的单位或经理定义的机密信息，不要收集您不需要的信息。
5. 不要让您的 AMG 计算机设备无人看管。保护 AMG 免受设备和数据盗窃。
6. 您的 AMG 计算机和设备将用于 AMG 业务目的。但是，允许有限的合理个人使用。您的计算机和设备是 AMG 公司的财产，并且只能使用 AMG 批准的软件。
7. 仅在必要时发送机密文件，并尽可能以加密方式发送。如果发送大文件，请使用安全数据传输。请联系您的经理和/或当地 IT 以获取指导。
8. 不要使用 USB、CD、DVD 或硬盘驱动器，除非得到 IT 管理部门的批准，并且不要将非 AMG 设备连接到 AMG 的网络。
9. 在办公室和在家工作时，保持办公桌干净整洁。
10. 向您的经理、IT 部门和/或法律与合规部报告任何可疑的 IT 活动。

可接受使用 AMG 电脑、手机设备和服务
所有 AMG IT 均出于商业目的提供给 AMG 终端用户。允许对这些设施进行有限的个人使用，前提是此类使用专用于私人事务且是合理的（即不会减损 AMG 终端用户的工作、占用异常的时间或空间、为 AMG 或损害 AMG 的声誉）。

AMG 终端用户不得从互联网或任何其他电子媒体下载、存储、发布、传播或分发通常被认为不合适的任何材料（包括根据 AMG 的社交媒体指南或商业守则认为不合适的任何材料）执行）。此外，AMG 终端用户不得以构成适用法律规定的非法或犯罪活动的方式使用 AMG 设备。

使用监控
为了管理其 IT 系统并加强安全性，AMG 可以在适用法律允许的范围内记录 AMG 终端用户的活动。进行此类监控的原因通常仅限于： 确保系统的有效运行；调查或检测系统未经授权的使用；预防或侦查犯罪；对涉嫌或已知违反本指南的行为进行调查。
事件报告和沟通
AMG 终端用户应立即通知其当地管理层和当地 IT 经理或部门所有和任何涉嫌或已知违反本指南的行为。此类事件可能包括但不限于：
- 异常或破坏性网络安全事件或事件；
- 可能的 IT 网络安全事件，例如可疑电子邮件；
- AMG 硬件或软件的丢失、损坏或疑似篡改；
- 涉嫌泄露敏感或机密信息，包括个人数据；
- 可能影响 AMG 信息或系统的网络安全漏洞。

当地管理层将及时通知 AMG 管理委员会任何此类事件或事件。
此报告义务至关重要，因为 AMG 可能有义务通知第三方和当局，以防个人数据因任何网络安全事件而受到损害。
在您需要建议的紧急或敏感情况下，或者如果您有无法通过当地管理或 IT 部门解决的疑虑，请按照以下方式联系 AMG 的企业合规办公室（AMG 首席合规官：compliance@amg-nv.com） AMG Speak Up & Reporting Policy，可在 AMG 网站上找到。

终止雇佣关系

当 AMG 终端用户因任何原因停止为 AMG 工作时，必须立即归还所有 AMG 设备、数据和文件。 所有信息系统特权以及对信息和 IT 设备的访问将立即终止。
AMG 终端用户必须：
- 归还 AMG 提供的所有设备（例如笔记本电脑、USB 存储钥匙、手机/智能手机）；
- 返回所有 AMG 相关信息，无论是数字、模拟（即录音和/或 CD、DVD）还是硬拷贝。

版本控制

版本	*日期*	*谁参与?*	*主要变化*
0.1	2022 年 2 月 2 日	Rainer Steger (RS)	文档的主要设置
0.2	2022 年 2 月 8 日	Project Moore	审查并输入最佳实践
0.3	2022 年 2 月 10 日	RS and Ludo Mees (LM)	审查输入摩尔项目和其他更改
0.4	2022 年 2 月 17 日	Michelle Witton and RS	审查良好实践
0.5	2022 年 2 月 25 日	Jackson Dunckel (JD)	最终审核通过
1.0	2022 年 2 月 25 日	JD, LM, RS	最终版