ArcelorMittal and Cyber Security

ArcelorMittal (or the "Company") is committed to applying the best-practice and standards in Cyber Security, and with respect to information protection, disclosure, and reporting.

ArcelorMittal continually monitors legal requirements and best practices in the United States, the European Union including Luxembourg, where ArcelorMittal is incorporated, to make improvements to its Cyber Security and General Data Protection Regulation ("GDPR") standards and procedures when necessary.

ArcelorMittal established an Information Systems Security Program ("ISSP") managed by the IT Department to continuously align the protection of the Group's information systems to address relevant cyber security risks.

The ISSP is focusing on protecting information systems against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability):

- Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.
- Integrity means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- Availability means ensuring timely and reliable access to and use of information.

ArcelorMittal Cyber Security Framework. Response readiness and tabletop exercises

ArcelorMittal has a robust IT Cyber Crisis Response Plan in place which provides a documented framework for handling high severity Cyber Security incidents and facilitates coordination across multiple parts of the ArcelorMittal group (the "Group"). ArcelorMittal collaborates with its peers in the areas of threat intelligence, vulnerability management, as well as detection, response, and recovery exercises. ArcelorMittal routinely performs simulations and exercises at both a technical and management level. ArcelorMittal incorporates external expertise and reviews in all aspects of its program. ArcelorMittal Cyber Security programme also includes awareness training for employees groupwide.

ArcelorMittal Cyber Security controls and practices are based on the NIST Cyber Security framework. https://www.nist.gov/cyberframework. ArcelorMittal Cyber Security Baseline Control Framework with a set of mandatory cyber security controls with quarterly review and reporting groupwide.

Based on the standard NIST Cyber Security Framework (https://www.nist.gov/cyberframework), ArcelorMittal designed its own Cyber Security Framework aligned with the legal requirements and its main business risks:

- **Compliance part**: ArcelorMittal defined a set of required Baseline IT Security Controls to have a minimum-security protection level in place against the common cyber security risks (to avoid common

Confidentiality, Integrity and Availability issues), and to support the compliance to our global legal requirements (foundation for Sarbanes-Oxley Act or "SOX" and GDPR requirements).

ArcelorMittal's Baseline IT Security Controls consist of the basic security controls that all units of the Company must embed in their IT solutions and services. ArcelorMittal sites that do not comply with the requirements of the Baseline IT Security framework will not be allowed to connect / stay connected to the ArcelorMittal global network. The ArcelorMittal Data Protection Procedure on implementing the requirements of the GDPR reference our Baseline IT Security Controls, which makes compliance to these baseline security controls a legal obligation. Compliance with the Baseline IT Security Controls is assessed on a yearly basis. The Baseline IT Security Controls are reviewed and updated regularly (on an as-needed basis), to make sure they continue to address the most important Cyber Security threats

The evolution of the required Baseline IT Security Controls is guided by the objective of putting in place an effective minimum information security standard across the Group, while considering the efficiency of delivery of business applications and IT services. The Baseline IT Security Controls rely on the principle that all data and applications have an assigned owner who decides on who can access the applicable application. Because this decision is a business decision, the owner should be from business and possess a good knowledge of business processes and the data.

- **Risk Based Approach**: Selection of internal and external best practices proposed to improve our maturity level against our main business risks:
  - **espionage** (Confidentiality risk: disclosure of our trade secrets, intellectual properties, or any other sensitive information assets) and
  - **sabotage** (Availability risk: inability of our production tools to work as expected). Beyond the commonly required Baseline IT Security Controls, each ArcelorMittal entity (site, unit, segment…) may need additional cyber security measures to achieve an acceptable protection level adapted to their own context.

Management reporting structure and frequency

The Audit & Risk Committee is responsible for overseeing cybersecurity risk, information security, and technology risk, as well as management's actions to identify, assess, mitigate, and remediate material issues. The Audit & Risk Committee receives regular quarterly reports from the Chief Information Security Officer and the Chief Cybersecurity Risk Officer on the Company's cybersecurity risk profile and enterprise cybersecurity program and meets with the Chief Information Security Officer at least quarterly. The Audit & Risk Committee annually reviews and recommends the Company's information security policy and information security program to the ArcelorMittal Board of Directors (the "Board") for approval. At least annually, the Board reviews and discusses the Company's technology strategy with the Chief Information Officer and approves the Company's technology strategic plan.

The key ArcelorMittal cybersecurity oversight responsibilities

- Oversee ArcelorMittal's cybersecurity plan, business continuity program, information protection management strategy and related risks to all these areas.
- Review ArcelorMittal's cyber insurance policies to ensure appropriate coverage.

- Review ArcelorMittal's development and training plan for critical IT staff as well as succession planning.

Cyber Security Maturity Self Assessments and Audits

Internal and external benchmarking is an important aspect to self-reflect on our deployed Cyber Security measures and keeping it at a good maturity level. Self-assessments and independent 3rd party audits are performed on a regular basis to benchmark (Internal & External) our Cyber Security Maturity Level for segments and for the Group.
These self-assessments and independent 3rd party audits include IT (Information Technology) and OT (Operations Technology), are launched and led by the Group CISO office and coordinated by segment Security Officers for their specific segments.
As a 3rd party auditor, we use the services of Ernst and Young ("E&Y"), I-Tracing and PricewaterhouseCoopers ("PWC). Segment Security Officers communicate segment results to the applicable segment management committees. The combined results of the Audit/Self Assessments are reported to the Group Management Committee and the Audit & Risk Committee by the Group CISO Office which are 100 % independent.

Project management

ArcelorMittal IT Security Risks and Compliance Requirements, including processing of personal data, which is GDPR compliant, are part of project's specification from the start to avoid issues and unnecessary expenses afterwards. All new IT projects are shared with the concerned IT Compliance & Security officer, and Data Protection correspondent as well, who in turn advises project teams whether they need to be considered as significant for IT Security in general and SOX compliance, and which security controls need to be implemented. To ensure GDPR compliance, all IT projects or systems involving Personal Data process are designed with the highest possible privacy protection so that by default Personal Data is not made accessible to an indefinite number of persons within or beyond ArcelorMittal. This includes, but is not limited to, ensuring that only the data necessary is processed, data storage periods are kept at a minimum, and the accessibility to the Personal Data is limited. In addition, for all new IT projects, technical and organisational measures are put in place in such a way to safeguard privacy and data protection principles at the earliest stages of the design of the processing operations.

End-user awareness

The implementation of an Information Systems Security Program does not mean that all responsibility for securing data rests with the IT departments. It is up to each segment/unit leadership to build and organize, in close coordination with the Group CISO Office, the awareness of their end-users. Security awareness and data privacy training are mandatory upon joining the Group and are repeated at least annually thereafter. Information security awareness messages are disseminated on a regular basis or on a need to know basis, for instance, in relation to cyberattacks.

Use of external independent advisor and board of directors' engagement

ArcelorMittal continued an industry leading practice of engaging an independent cybersecurity advisor for the fourth year in a row and reviewed a cyber crisis simulation exercise that was used by our senior leaders to prepare for a possible cyber crisis. The Audit & Risk Committee regularly receives reports from its independent advisor regarding our cybersecurity program. ArcelorMittal has been using E&Y for cybersecurity audits, as well as I-Tracing (French based company specializing in Cyber Security) and this year (2021) ArcelorMittal is using PWC for cybersecurity.

BUSINESS BENEFITS

- Minimize risk of data leak or loss.
- Protect ArcelorMittal information assets from unauthorized access, modification, disclosure, and destruction.
- Provide ArcelorMittal employees with guidance when using ArcelorMittal information systems (including fulltime, part-time, contractors).
- Promote a proactive position for ArcelorMittal about the protection of the organization's information systems with relevant cyber security risks.