Royal BAM Group

Information Security Policy Statement

The Executive Committee of Royal BAM Group is committed to protect the security of information.

This policy is applicable to all Royal BAM Group activities and all its companies, employees and any other representatives (hereafter 'BAM').

BAM's key information security principles are:

- BAM wants to protect and manage information properly to ensure confidentiality, integrity and availability of information.
- BAM's policy on information security and supporting documents make use of generally accepted information security standards (such as ISO27001/2).
- The approach to information security is based on the 'security and privacy by design' principle, which entails that information security and privacy need to be embedded in the early stages of development of new processes, procedures, plans and systems.
- BAM is committed to a balanced, risk-based set of information security measures covering organisational, technical, physical and people measures, which are proportional to the risks.
- Information security measures need to be integrated into operational processes as much as possible, minimizing the overhead of dedicated security processes.
- Focus on continuous improvement to ensure the effectiveness of the measures taken while safeguarding that these remain proportional to business and threat development.

BAM's approach provides the framework to set and monitor objectives with key focus on:

Management system

- Deliver a clear framework in line with the requirements of ISO 27001-2022 for managing risks that could potentially harm BAM's information assets confidentiality, integrity and/or availability, for ensuring appropriate controls and for monitoring effectiveness.

People and communication

- Ensure awareness, knowledge and skills of BAM's employees to secure information and an acceptable use of BAM information assets.

Information technology security

- Minimise vulnerabilities and increase system security within BAM and towards third parties and clients.
- Identity & Access management in a secure and robust manner.

Physical security

- Control access to BAM's offices, facilities and systems commensurate with the identified risks and sensitivity.

Third party management

- Endorse appropriate third party due diligence and monitoring the compliance of information security responsibilities.

Incident management, disaster recovery and business continuity

- Ensure a structured approach to the management of information security incidents, disaster recovery and business continuity.

This policy is achieved by effective operation of the integrated management systems together with the active leadership, participation, professionalism and commitment of all internal stakeholders involved. The management systems aim to meet the requirements of BAM, its clients and other external stakeholders.

The Executive Committee regards the responsibility of management in implementing this policy statement to be fundamental to BAM meeting its standards and commitments.

BAM has appointed a Director Security for the Group to ensure awareness of this policy is promoted throughout the company, the effectiveness is monitored and areas for continual improvement identified and implemented.

Ruud Joosten
Chief Executive Officer
For and on behalf of the Executive Committee of Royal BAM Group

This policy statement has been approved electronically. Proof of approval can be seen upon request.