

Cyber Information Security and Data Compliance policy

Cyber, data, and information security protect Ramboll's business, clients, partners, employees, and society. This policy defines the minimum requirements and behaviours for safeguarding information, systems, data, and digital assets, supporting the Ramboll Code of Conduct applying to Ramboll business, clients, partners and employees.

Our Cyber Information Security Principles

People first: Security supports people in doing their work safely. Ramboll enables secure behaviour through guidance, training, and tools.

Shared responsibility: Security is everyone's responsibility. All individuals must act securely, remain vigilant, and promptly report incidents, weaknesses, or suspicious activity.

Risk-based protection: Security risks are identified, assessed, and managed across all activities.

Resilience: Ramboll maintains resilient information systems through effective business continuity and incident management, ensuring the availability, integrity, and recovery of critical services and data.

Integrated governance: Security is managed through Ramboll's Cyber & Information Security Management System, aligned with ISO 27001 and CIS Controls.

Continual improvement: Ramboll is committed to continually improving cyber, data, and information security.

Regulatory Compliance

Ramboll complies with all laws and regulations that are applicable to Ramboll and its business related to:

- Cybersecurity
- Information security
- Data protection and privacy
- Artificial intelligence and automated systems
- Digital and technology governance

Ramboll has implemented a global data privacy framework (Binding Corporate Rules (BCR), which ensures the highest level of data privacy throughout the company.

Governance

The Group Executive Board sets direction and approves ambition and funding, while the Director of Cyber Information Security and Data Compliance owns and maintains the global cyber, information security, and data compliance and regulatory management system and its programme, and provides regular reporting on cyber, data, and information security and compliance risk and performance to the Audit & Risk Committee and the Group Executive Board.

Expected Behaviours

All employees, contractors, consultants, and third parties must follow this policy, including:

- Protect Ramboll and client information.
- Use only approved devices, platforms, and storage.
- Grant access on a need-to-know basis and review regularly.
- Keep credentials secure and devices protected.
- Stay alert to phishing and security threats.
- Handle confidential information responsibly and lawfully.