

# Information & Cyber Security Factsheet





Cyber-attacks pose a significant and growing threat to organisations worldwide, with potential consequences including operational disruption, unlawful access or theft of information, and reputational damage. Babcock recognises these risks and has implemented a comprehensive Information & Cyber Security framework to safeguard data and systems across the enterprise. Our approach aligns with international standards and regulatory requirements, ensuring robust governance, proactive risk management, and continuous improvement. This factsheet outlines our key policies, certifications, and initiatives demonstrating how we embed security into our culture, supply chain, and customer engagements to maintain trust and resilience in an evolving threat landscape.

## Governance & Risk Management

At Babcock, we take a structured approach to information and cyber security through our Cyber and Information Security Framework. This framework sets the direction, provides assurance, and guides how we manage security to maintain a strong and consistent posture.

Executive level responsibility for overseeing information security issues across all reporting countries, sectors, and functions within Babcock International Group is maintained by the Chief Information Security Officer (CISO).

Oversight is provided by the Security Executive Committee and the Group Executive Risk and Controls Committee, embedding cyber risk management into everything we do. It defines clear risk boundaries and applies unified controls across Babcock's technology landscape. All security measures follow secure-by-design principles, with practical, repeatable, and auditable controls to protect Babcock and our customers' assets throughout their lifecycle. We also collaborate closely with external stakeholders and the internal Group Executive Risk and Controls Committee to ensure cyber and information risk is effectively managed across all levels of the organisation.

## Key Policies & Practices

Our governance framework is set out in formal policies that align with international best practices:

- Information Security Policy - A top-level policy that establishes Babcock's commitment to information security and the operation of an ISO 27001-aligned Information Security Management System (ISMS). It defines governance structures, roles (e.g., ISMS Manager), and responsibilities, setting objectives and principles for protecting information across the enterprise. The policy underpins the Information Security criteria by demonstrating formal management commitment, a structured security program, and continuous improvement. It also supports Risk & Crisis Management through mandated risk assessments, security controls, and incident response procedures.



- Acceptable Use Policy (AUP) - Defines acceptable use of IT systems by employees, including data protection, prohibited activities, and user obligations. Enforced through annual mandatory training and login acknowledgments, it promotes an ethical, security-conscious culture and mitigates human-factor risks. The policy sets clear rules to prevent misuse of IT assets (e.g., unauthorised data storage or external transfers) and demonstrates strong internal controls and employee accountability. By shaping a risk-aware culture and reducing insider threats and compliance breaches, the AUP strengthens Governance and Risk Management.
- Management System (ISMS) - Certified to the ISO 27001:2022 standard for all core IT Services and use. This policy ensures senior leadership commitment to security, integration of security into business processes, and regular reviews of security performance.
- Supply Chain Cyber Security Policy - Sets requirements for suppliers and partners to meet Babcock's security standards, including compliance with government accreditations and our own controls. It addresses supplier risk assessments, contractual security clauses, and incident reporting obligations for third parties. The policy extends Governance and Risk Management to the supply chain, ensuring customer information is protected across the value chain. It demonstrates Babcock's proactive approach to third-party risk - an increasingly critical aspect of sustainable business operations.
- Other Key Policies - Beyond the core policies, Babcock maintains a comprehensive suite of security-related policies, including Security Incident Management, Data Protection, and Business Continuity. Together, these ensure governance spans all aspects of cyber and information security. All policies are regularly reviewed and updated within the Global Business Management System (BMS) to address emerging threats and requirements, reinforcing our company's commitment to strong security governance and continuous improvement.
- Cyber & Information Security Framework - An enterprise-wide governance framework that defines Babcock's approach to cyber risk management and establishes unified security controls. It ensures oversight through risk committees and integration into corporate governance, embedding risk appetite, board-level accountability, and cross-organisational responsibility for cybersecurity.

## Standards & Certifications

We adhere to all required international and government security standards for the secure installation and operation of information systems. This includes compliance with:



- UK Ministry of Defence (MoD) requirements and other industry-specific regulations - essential given Babcock's position as a prime defence contractor. By aligning its policies and controls with standards such as NIST (National Institute of Standards and Technology), ISO 27001:2022 and MoD DefStan 05-138 for supplier security, Babcock ensures its practices meet the rigorous benchmarks demanded by the sector.
- ISO Certifications - Babcock's core IT services are certified to ISO 27001:2022 (Information Security Management) and ISO 22301:2019 (Business Continuity Management) following rigorous external audits of processes and controls. These certifications provide independent assurance that our company operates a systematically managed security program and maintains robust continuity plans for critical operations. They demonstrate compliance with best practices, confirming Babcock's ability to protect data (ISO 27001) and effectively manage disruptions (ISO 22301).
- Cyber Essentials Plus - Babcock is accredited with Cyber Essentials Plus, a UK Government-backed certification required for many government contracts. This annually renewed accreditation confirms that our company has implemented essential technical controls to defend against common cyber threats, including secure configuration, access control, malware protection, patch management, and network security. It demonstrates compliance with national cybersecurity standards, regulatory requirements, and Babcock's commitment to strong baseline cyber hygiene and readiness.
- Continuous Improvement & Audits - Babcock's certifications and policies are continuously maintained through regular internal and external audits to ensure compliance and drive improvement. Management reviews of the ISMS, as required by ISO 27001, address any non-conformities with corrective actions. This ongoing cycle of auditing and enhancement keeps Babcock's cybersecurity practices aligned with emerging threats and evolving standards, highlighting the company's proactive approach within the sustainability context.

## Stakeholder Engagement

External Stakeholder Collaboration - Babcock actively collaborates with clients, industry partners, and government cyber agencies to manage risks and share best practices. This includes engagement with the UK National Cyber Security Centre (NCSC) and participation in defence industry security forums, as well as compliance with client-specific security requirements. Such cooperation ensures Babcock's cyber risk management aligns with stakeholder expectations and broader industry initiatives.

Customer Assurance & Engagement - Security is embedded in customer engagements and project delivery from the outset, with requirements integrated into project plans and contracts. Babcock provides regular



security briefings and reports to major clients and offers opportunities for audits or observation of security practices. This transparency builds trust and demonstrates Babcock's commitment to secure, efficient project execution - positioning strong cybersecurity as a value-added differentiator in bids and long-term relationships.

## Internal Culture & Workforce Development

### Security Awareness & Training

Babcock prioritises a strong security-aware culture, recognising that people are central to effective cyber defence. All employees must complete annual mandatory training, including the Acceptable Use Policy, phishing detection and proper data handling. This is reinforced through regular awareness campaigns, threat updates, and security tips to promote safe practices. A dedicated Security Knowledge Zone provides guidance, policies, process links, FAQs, and a calendar of upcoming training sessions. By empowering employees to identify and report risks, Babcock reduces human error and strengthens its overall security posture - demonstrating investment in human capital and internal capacity-building.

Professional Development - Babcock actively develops its cybersecurity talent to address current and future challenges. The company sponsors professional certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and ISO 27001 Lead Auditor for its security staff, while tackling the industry skills gap through apprenticeship and graduate schemes in cyber and information security. This "grow your own" approach ensures a pipeline of skilled professionals and reinforces Babcock's commitment to long-term resilience.