EUROBANK

eurobank.gr

EUROBANK S.A.
8 Othonos Str., 105 57 Athens, GR

GCR. 154558160000

June 2026

Information Security and Cyber Resilience

High-level public statement of principles and commitments

Eurobank S.A. is committed to protecting information, personal data, transactions and digital services, and to maintaining the resilience of its information and communication technology systems.

1. Purpose and scope

This Public Policy Statement describes the high-level principles and commitments that guide Eurobank S.A. (the "Bank") in managing information security, cybersecurity and digital operational resilience. It applies across the Bank's operations and business lines and covers information assets, ICT systems, digital channels, employees and contractors within scope, and relevant third parties, suppliers and service providers.

2. Governance and accountability

The Board of Directors has overall accountability for setting, approving and overseeing the arrangements supporting the Bank's ICT and Security Risk Management Framework and for ensuring a high level of digital operational resilience.

The Chief Information Security Officer (CISO), who heads Group Corporate Security, reports directly to a Deputy Chief Executive Officer who participates in the Board of Directors and the Executive Board. Group Corporate Security operates as an independent second line of defence function and monitors adherence to the ICT and Security Risk Management Framework. The CISO provides regular formal reporting to the Board on ICT and security risks and cybersecurity performance.

Information security responsibilities are allocated across the Bank under a three-lines-of-defence model. Employees and contractors within scope are required to comply with the security requirements applicable to their roles and access.

3. Core principles

- **Risk-based protection**. Security measures are proportionate to the nature, criticality and risk of the information, systems and services concerned.
- **Confidentiality, integrity and availability**. Information and personal data are protected against unauthorised access, disclosure, alteration, loss, destruction or unavailability.

- **Predict, Prevent, Detect, Respond and Recover**. The Bank applies a multi-layered approach to anticipate threats, reduce risk, identify suspicious activity, respond to incidents and support recovery.
- **Security and resilience by design**. Security and resilience considerations are incorporated, as appropriate, into the design and material change of systems, products, services and digital channels.
- **Continuous improvement**. The security framework is reviewed and enhanced to reflect evolving threats, technologies, business needs and legal, regulatory and supervisory requirements.
- **Accountability**. Security roles and responsibilities are defined, communicated and supported through governance, training, monitoring and assurance.

4. Security and resilience commitments

- Identify, assess, manage, monitor and report ICT and security risks through established governance and risk management processes.
- Apply layered technical and organisational safeguards, including strong authentication, role-based access controls, encryption and de-identification techniques where appropriate to the risk and processing context.
- Maintain capabilities for security monitoring, threat detection, incident response, recovery, business continuity and disaster recovery.
- Conduct risk-based security assessments, testing and assurance activities, including vulnerability assessments and independent reviews where appropriate.
- Provide information security and cybersecurity training and awareness to all employees and contractors.
- Promote customer awareness of emerging cyber threats and online fraud through appropriate communication and education initiatives.

5. Third-party security

Third parties, suppliers and service providers with access to Bank information, personal data, systems or services are subject to binding security and data protection requirements. These may include contractual obligations, risk-based due diligence, security assessments, monitoring and audits, as appropriate to the nature and risk of the service. Identified risks and deficiencies are addressed through the Bank's applicable governance and remediation processes.

6. Standards, certification and assurance

The Bank's security and resilience framework takes account of applicable legal and regulatory requirements, including the Digital Operational Resilience Act (DORA), and recognised international standards. Eurobank maintains ISO/IEC 27001 and ISO/IEC 27701 certifications. The Bank also performs internal audits and is subject to external assessments and assurance activities in accordance with applicable requirements.

7. Incident management and reporting

The Bank maintains processes for identifying, escalating, assessing, responding to and recovering from information security and ICT-related incidents. Incidents are reported to competent authorities and affected parties where required by applicable law and regulation. Material matters are escalated through the relevant governance channels.

8. Monitoring, compliance and review

The effectiveness of the security framework is monitored through risk assessments, control monitoring, testing, audits, incident analysis and management reporting. Non-compliance is addressed under applicable internal governance, employment and contractual arrangements. This statement is reviewed periodically and updated when material changes in risks, regulation, technology or the Bank's operating environment warrant it.

Related public information

This statement should be read together with the following public information:

- Eurobank Sustainability Statement
- Eurobank Security Hub - How we protect your transactions
- Eurobank Business Continuity Statement
- Eurobank GDPR information