INFORMATION SECURITY AND CYBERSECURITY POLICY

1. PURPOSE AND SCOPE

Purpose: To establish Davivienda Group's directives, governance frameworks, and general guidelines to protect information assets and technological infrastructure across the entire financial group, ensuring at all times the confidentiality, integrity, and availability of data belonging to our clients, collaborators, partners, third parties, and operations. Likewise, it seeks to establish guidelines for our subsidiary companies to implement a comprehensive management model that prevents, detects, responds to, recovers from, and maintains operational continuity in the face of cyber threats.

Scope: This policy applies to Davivienda Group and transversally across its subsidiaries, including its workforce (direct employees and contractors), as well as all stakeholders, third parties, suppliers, and business partners who generate, access, process, store, distribute, manage, or dispose of organizational information or act on its behalf.

2. POLICIES

The General Information Security and Cybersecurity Policies are established below, providing high-level guidelines regarding the implementation of strategic, tactical, and operational controls of the Governance Model:

2.1. Continuous Improvement and Evolution of Security Systems

Davivienda Group requires all its subsidiaries to maintain constant updating and evaluation of the maturity of the Information Security Management System (ISMS) and its governance model. Due to the constant evolution of cyber threats and the technological landscape, policies, standards, procedures, and tools must be periodically reviewed and updated, conducting, among others, vulnerability assessments, penetration testing (*ethical hacking*), and continuous investments in technological infrastructure.

2.2. Protection, Classification, and Integrity of Data and Assets

Information is a vital asset of Davivienda Group and its subsidiaries; therefore, it must be protected throughout its entire lifecycle against unauthorized access, modification, loss, improper disclosure, or destruction. Subsidiaries must implement:

- **Access Control:** Identification, authentication, authorization, and traceability mechanisms to prevent unauthorized access.
- **Cryptography and Encryption:** Cryptographic methods and encryption techniques to safeguard the confidentiality, integrity, and validity of sensitive data in transit, at rest, and in processing.
- **Physical and Environmental Security:** Areas with security levels commensurate with the value of the information and restricted access for confidential information.

2.3. Active Monitoring, Threat Intelligence, and Incident Response

Davivienda Group mandates that its subsidiaries must establish a formal threat management procedure encompassing intelligence, threat hunting, tracking, continuous monitoring (24/7), and timely response. In the event of adverse events and information security or cybersecurity incidents, rapid containment, reporting, and investigation frameworks must be executed to ensure resilience in cyberspace.

2.4. Individual Responsibilities, Human Resources, and Cybersecurity Culture

We understand that information security is a shared responsibility; therefore, subsidiaries must ensure:

- Ongoing training, awareness, and sensitization programs regarding security culture and cybersecurity.
- Formal mechanisms for the enforcement of individual responsibilities from onboarding through separation.
- Targeted fraud awareness and prevention initiatives aimed at clients.
- User commitment to adhere to protocols and immediately report any suspicious activity or incident.

2.5. Third Parties

All suppliers, contractors, partners, and third parties that access information assets or provide services to any of Davivienda Group's subsidiaries must strictly comply with the group's information security, cybersecurity, and privacy policies, standards, and procedures. Such compliance shall be formally supported through contractual clauses, risk assessments, periodic audits, and verification of equivalent security standards.

3. INFORMATION SECURITY AND CYBERSECURITY GOVERNANCE

- **Board-Level Oversight:** The strategic oversight directive regarding cybersecurity, technological risk, and information privacy across the group rests with the Board of Directors (through the Risk and Audit Committee or designated governing body), comprising qualified members with accredited experience in technology and cybersecurity.
- **Guidelines for Subsidiaries:** Each subsidiary of Davivienda Group must adopt and implement a governance structure aligned with group standards, defining roles and responsibilities to mitigate risks to technological infrastructure, business processes, and people.
- **Executive Leadership:** The management, execution, and maintenance of the Information Security and Cybersecurity Model shall be the responsibility of the corresponding executive leadership (Chief Information Security Officer – CISO / Chief Technology Officer – CTO / Security Directorate) in coordination with Senior Management.
- **Secure Development and Innovation:** All technological solutions developed or acquired within the group must incorporate a formal secure development methodology (security by design from inception) throughout their entire lifecycle.
- **Comprehensive Risk Management and Compliance:** Technological risks must be identified, assessed, treated, and monitored to maintain the organization's acceptable risk appetite level, ensuring strict compliance with applicable local and international regulations on cybersecurity, information security, and data protection/privacy.

4. ESCALATION CHANNELS AND INCIDENT REPORTING

Davivienda Group and its subsidiaries shall maintain a structured escalation procedure known to all users. Any collaborator, subsidiary, or third party must report anomalies, vulnerabilities, adverse events, or suspicious activities that could compromise information assets or cyberspace through the official corporate channel:

5. BUSINESS CONTINUITY PLAN AND AUDITS

- **Operational Continuity (BCP / DRP):** All critical business processes and associated information assets across Davivienda Group and its subsidiaries must have Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) specifically designed to address cyberattacks, regularly tested to guarantee operational resilience and the

continuous availability of banking and financial services.

- **Security in Communications and Transactional Channels:** The group's digital and transactional channels must integrate controls that protect network infrastructure, data transmission, and guarantee secure online operations that inspire maximum trust among clients.
- **Auditing and Inspection:** The effectiveness of the ISMS and IT infrastructure shall be evaluated periodically through internal audits and independent external audits that certify compliance with international standards and regulations issued by local and international regulatory bodies.
-

6. POLICY APPROVAL

This policy underwent the process of review and approval by the Board of Directors of Davivienda Group prior to its dissemination. Any updates thereto shall follow the same procedure, ensuring that a comprehensive review is conducted at least every five years to guarantee alignment with the Group's other policies.

Approval Date	Approving Body
October 20, 2026	Board of Directors – Davivienda Group