ELEVION GROUP MINIMUM INFORMATION SECURITY REQUIREMENTS

This policy defines the minimum information security requirements for Elevion Group to address key information security risks and realize synergies via intragroup collaboration. The policy applies to all Elevion Group entities.

Key Policy Requirements

- Entities must comply with the following minimum information security requirements:
    1. **Information Asset Inventory:** Must be up-to-date and include all relevant information assets.
    2. **Backup & Offline Backup:** Must follow specific rules to ensure resilience against ransomware attacks.
    3. **Endpoint Detection and Response (EDR) & Identity Protection:** EDR solutions must be installed on all workstations, laptops, and servers, with identity protection activated.
    4. **Periodic Health Checks of Active Directory:** Monthly health checks using group-defined tools.
    5. **Vulnerability Management:** Continuous identification and remediation of vulnerabilities.
    6. **Mobile Device Management (MDM):** All mobile devices accessing company resources must be managed using MDM solutions.
    7. **Conditional Access and Hardening of Entra:** Entra must be configured and hardened according to group standards.
    8. **Multi-Factor Authentication (MFA) for VPN:** VPN access must be protected by MFA.
    9. **Annual Review of Firewall Rules:** Annual review and documentation of firewall rules.
    10. **Segmented Network:** Network segmentation principles must be followed.
    11. **E-mail Security:** DMARC must be configured for all domains.
    12. **Business Continuity and Disaster Recovery (BCP/DRP):** BCP and DRP plans must be in place and tested annually.
    13. **Annual Review of Access Rights:** Annual review and documentation of access rights.
    14. **Security Relevant Vendors Identified and Risks Managed:** All vendors with access to systems and data must be identified and assessed.
    15. **User Information Security Awareness:** Annual information security training for all users, with regular phishing simulations.
- Non-compliance must be addressed with an action plan.
- Compliance status must be reported via the Information Security Dashboard/Elevion Group GRC tool.
- Compliance status must be reported monthly and included in the agenda of the entity's Board of Directors.