Kiteworks

NIS 2 Compliance Best Practices Checklist for Small Businesses

Unlike the first NIS Directive, the NIS2 Directive's scope now includes small and medium–sized enterprises (SME's) as they play a crucial role in the essential services supply chain. To help SME's achieve NIS2 compliance, here are some key best practices tailored to their resources and capacity:

- **1. Conduct a Risk Assessment:** Identify key assets, potential threats, and vulnerabilities. Prioritize risks based on likelihood and potential impact, using methodologies like ISO/IEC 27005 or ENISA guidance.
- **2. Implement a Cybersecurity Governance Framework:** Adopt a simplified version of existing frameworks (ISO/IEC 27001, NIST CSF) to establish roles, responsibilities, and policies around cybersecurity.
- **3. Train Staff on Cybersecurity Awareness:** Regularly educate employees on phishing attacks, social engineering, password management, and safe online practices.
- **4. Ensure Strong Access Control and Authentication:** Enforce multi-factor authentication (MFA) across key systems. Limit user privileges through a least-privilege model to reduce insider threats.
- **5. Develop an Incident Response Plan:** Create an incident response plan that outlines procedures for detecting, reporting, and responding to cybersecurity incidents. Test the plan through tabletop exercises to identify gaps and weaknesses.
- **6. Practice Regular Patching and Vulnerability Management:** Implement automated patch management processes to ensure systems and software are updated regularly. Use vulnerability scanning tools to identify security weaknesses.
- **7. Plan for Business Continuity and Disaster Recovery (BC/DR):** Develop BC/DR plans that cover key systems and data recovery after a security incident. Regularly test backup processes to ensure that critical data can be restored efficiently.
- **8. Monitor and Log Network Activity:** Implement network monitoring tools to detect unusual activity. Keep logs to facilitate incident detection and compliance with reporting requirements under NIS2.