NIS 2 INFORMATION SECURITY CHECKLIST

INCIDENT HANDLING POLICY

Establish an incident handling policy laying down the roles, responsibilities, and procedures. This includes:

- ✓ Incident categorization system
- ✓ Effective communication plans for escalation and reporting
- ✓ Assignment of roles to competent employees
- ✓ Documents such as incident response manuals, escalation charts, and contact lists
- ✓ Interfaces with business continuity management
- ✓ Test, review, and update policy regularly and after significant incidents or changes

Event Reporting

- ✓ Establish a simple mechanism for reporting suspicious events
- ✓ Communicate reporting mechanism to network
- ✓ Provide regular training on using the report mechanism

Monitoring and Logging

- ✓ Implement procedures and tools to monitor and log network activities
- ✓ Automate monitoring where feasible to minimize false alerts
- ✓ Maintain, document, and review logs including network traffic, user changes, access events, and system performance
- ✓ Review logs for trends and set appropriate alarm thresholds
- ✓ Backup logs centrally and protect against unauthorized access
- ✓ Ensure synchronized time sources for log correlation and redundancy
- ✓ Regularly update procedures and asset lists

NIS 2 INFORMATION SECURITY CHECKLIST

INCIDENT HANDLING POLICY

Event Assessment and Clarification

- ✓ Assess suspicious events based on predefined criteria
- ✓ Prioritize incidents for containment and eradication
- ✓ Review logs for event assessment and correlation
- ✓ Reassess events with new information
- ✓ Quarterly review for recurring incidents

Incident Response

- ✓ Respond promptly using documented procedures
- ✓ Include stages for incident containment, eradication, and recovery
- ✓ Establish communication plans with CSIRTs, authorities, and stakeholders
- ✓ Log response activities and preserve evidence
- ✓ Test procedures at planned intervals

Post-Incident Reviews

- ✓ Conduct reviews to identify incident root causes and lessons learned
- ✓ Improve network security, risk treatment, and incident handling based on reviews
- ✓ Review after significant incidents at planned intervals

This checklist can be used as a guideline to start implementing a NIS2 compliant information security policy. Reach out to Centripetal to see how we can help your organization improve the security posture of your network and information systems.

CENTRIPETAL