bechtle

Network & Compliance

Network Security Baseline Checklist

This checklist outlines baseline network security and compliance controls that are relevant for every organization. Not every control will be implemented in the same way, but each area should be addressed based on risk, size, and regulatory requirements.

Network Foundation

- □ Network assets (devices, users, access points) are identified and documented
- □ Authentication is centralized and protected (e.g. MFA where applicable)
- □ Network segmentation is applied or considered (e.g. production, guest, admin, OT)
- □ Critical network traffic is protected through encryption
- □ Network devices are maintained through regular patching and firmware updates
- □ Wireless access is secured using current security standards

Identity & Access Control

- □ Access rights follow the principle of least privilege
- □ Privileged access is separated from standard user access
- □ Joiner / mover / leaver processes are defined and enforced
- □ Access decisions consider risk factors (location, device, behavior)
- □ Roles and access rights are reviewed periodically

Monitoring & Detection

- □ Network activity is monitored for security events
- □ Alerts exist for suspicious behavior and access attempts
- □ Logs are collected and retained for investigation purposes
- □ Configuration and log data are backed up securely
- □ Vulnerability scanning or security testing is performed periodically

Compliance & Risk Management

- □ Data sensitivity and criticality are defined
- □ Security risks are assessed and documented
- □ An incident response process exists and is reviewed regularly
- □ Third-party and supplier risks are considered
- □ Evidence can be produced to support audits or compliance reviews

This checklist outlines baseline network security and compliance controls that are relevant for every organization. Not every control will be implemented in the same way, but each area should be addressed based on risk, size, and regulatory requirements.

Backup & Recovery

- □ Backup processes exist for critical systems and configurations
- □ Restore procedures are tested periodically
- □ Backups are protected against loss and tampering
- □ Recovery objectives (RTO/RPO) are defined
- □ Business continuity requirements are linked to network dependencies

Endpoint & Device Security

- □ Endpoints and connected devices are protected and monitored
- □ Device trust or compliance is evaluated before granting access
- □ Lost or compromised devices can be contained or wiped
- □ Non-compliant or unknown devices are restricted

Policies & Awareness

- □ Security policies are defined and kept up to date
- □ Employees receive security awareness training
- □ Clear procedures exist for reporting security incidents
- □ Privileged users receive additional security guidance
- □ Rules for personal or unmanaged devices are defined

Take the Next Step.

Establishing a strong network security and compliance baseline does not start with complex frameworks, but with understanding where you stand today. This checklist helps you review essential focus areas, gain initial insight into your current environment, and identify topics that may require further attention.

At Bechtle, we support organizations in translating these insights into practical next steps, whether that involves deeper assessment, targeted improvements, or ongoing support.

Use this checklist as a starting point and explore the supporting assets in this campaign to learn how organizations can strengthen network stability, reduce risk, and address compliance expectations in a practical and confident way.

Network & Security Brochure

Through its network and security services, Bechtle helps organizations reduce complexity, strengthen protection, and maintain a reliable IT foundation that supports both operational and regulatory requirements.

This brochure gives an overview of all the services offered.

Whitepaper Building a Compliant IT Foundation

This whitepaper explains what compliance means in practice and how it connects to IT foundations such as security, continuity, and governance. It provides context on regulatory expectations and helps organizations understand how to approach compliance in a structured way.

E-BOOK
bechtle
The five most common security threats to your organization.
And what you can do about it.

E-Book The Five Most Common Security Threats

This e-book provides context on common security threats that impact organizations today. It helps readers understand why these threats matter and how they relate to everyday security and risk management decisions.