**Overview**

Establishing a secure and resilient network is mission-critical for the Germany branch. This document outlines the key security strategies, technologies, and operational practices required to protect digital assets, ensure compliance (especially GDPR), and prevent data breaches or operational disruption.

**1. Security Objectives**

* Enforce strong perimeter and internal network security.
* Secure data transmission and remote access.
* Prevent unauthorized access to internal systems.
* Monitor, detect, and respond to security incidents proactively.
* Comply with European cybersecurity and privacy regulations.

**2. Perimeter Security**

**Firewall Deployment**

* Deploy an enterprise-grade **stateful firewall** (e.g., FortiGate, pfSense, or Cisco Meraki).
* Key configurations:
  + Port filtering and access control lists (ACLs).
  + Geo-IP blocking (limit exposure to only needed regions).
  + VPN enforcement for remote access.
  + Intrusion Prevention System (IPS) module enabled.

**DDoS Mitigation (Optional)**

* Some ISPs offer basic DDoS protection—confirm availability.
* Cloud-based mitigation services (e.g., Cloudflare Gateway) if high risk.

**3. Network Segmentation**

Use **VLANs** to isolate traffic and limit lateral movement:

* **Admin VLAN** – Full access to all systems.
* **Staff VLAN** – Limited access to production systems.
* **Guest VLAN** – Internet-only, no internal resource access.
* **IoT/Device VLAN** – For printers, phones, etc., strictly isolated.

Apply **Inter-VLAN routing rules** via Layer 3 switch or firewall.

**4. Endpoint Security**

**Workstation & Device Protection**

* Mandatory **EDR/Antivirus** on all laptops/desktops (e.g., CrowdStrike, Bitdefender, Sophos).
* **Full-disk encryption** (BitLocker/FileVault).
* Auto-lock and session timeouts enabled.
* Disable USB ports unless required and justified.

**Mobile Device Management (MDM)**

* Required if mobile phones/tablets access company data (e.g., Microsoft Intune, Jamf).

**5. Identity & Access Control**

**Authentication Standards**

* Use **SSO with MFA** (e.g., Microsoft Entra ID, Okta).
* Passwords: Minimum 12 characters + rotation policies.
* Disable default device logins (especially for network equipment).

**Role-Based Access Control (RBAC)**

* Define and enforce access levels for every department or role.
* Remove access immediately upon employee offboarding.

**6. Remote Access Security**

**VPN Access**

* Required for all remote access, with two-factor authentication.
* Prefer **IPSec** or **SSL VPN** tunnels using enterprise-grade clients.

**Cloud Access Policies**

* Limit admin panels and dashboards to known IPs where possible.
* Use **conditional access rules** for critical SaaS tools.

**7. Monitoring & Logging**

**Tools & Practices**

* Enable **Syslog** on all critical network hardware.
* Aggregate logs into a **central logging server** or **SIEM** (e.g., Wazuh, Splunk).
* Set up alerts for:
  + Failed login attempts
  + Suspicious traffic
  + Network configuration changes

**Regular Security Audits**

* Conduct internal vulnerability scans quarterly.
* Perform penetration testing yearly (or more often if budget allows).

**8. Physical Security**

* Lock server racks and network closets.
* Use surveillance cameras at entry points.
* Secure switch closets with access logs and keycard systems.

**9. Compliance (GDPR + Local)**

* Maintain **records of data processing activities** involving personal data.
* Store logs for **up to 6 months**, encrypted and access-controlled.
* Ensure **data transfers outside the EU** are legally covered (e.g., SCCs).

**10. Employee Awareness**

* Conduct **security awareness training** quarterly.
* Simulate phishing attacks to improve staff vigilance.
* Include security policies in onboarding documentation.

**Conclusion**

Security isn’t just a feature—it’s a foundation. This framework provides multi-layered protection for the Germany branch, balancing usability with strict access control and visibility. Following this plan will reduce attack surfaces, safeguard sensitive data, and ensure compliance with European standards.

For custom firewall rules or security onboarding templates, contact the IT Security Lead or submit a security request ticket.