Help Desk Security Audit Checklist

Use this help desk security audit checklist to evaluate whether your customer support platform has the essential protections required to safeguard sensitive customer data and maintain compliance.

Authentication and login security

☐ Multi-factor authentication (MFA) is enabled for all support agents

☐ Single sign-on (SSO) is integrated with your identity provider

☐ Automatic session timeouts are configured for inactive users

☐ Password policies enforce strong and unique credentials

Access control and permissions

☐ Role-based access control (RBAC) is configured for all support roles

☐ Ticket visibility is restricted by team or department

☐ Only administrators can export or delete large volumes of data

☐ Login access is restricted to approved IP addresses or VPN networks

Data protection and encryption

☐ All customer data is encrypted at rest using modern encryption standards

☐ Data in transit is protected using TLS encryption

☐ Sensitive information (credit cards, passwords, tokens) is automatically redacted in tickets

☐ Data retention policies define how long support data is stored

Compliance and vendor verification

☐ Vendor provides SOC 2 Type II or ISO 27001 certification

☐ HIPAA or PCI DSS compliance is verified if required by your industry

☐ A signed Data Processing Agreement (DPA) is available

☐ Privacy policies clearly explain how customer data is handled

Monitoring, logging, and alerts

☐ Audit logs track all user actions within the help desk system

☐ Alerts are triggered for suspicious activity or large data exports

☐ Activity logs record ticket access, edits, exports, and deletions

☐ Security teams regularly review logs for unusual behavior

Infrastructure and disaster recovery

☐ Daily automated backups are enabled

☐ Backup data is stored securely in a separate location

☐ Vendor performs regular penetration testing

☐ Platform uptime guarantees and SLAs are clearly defined