NetSecure Connect - Internal Security Audit

Company Profile: NetSecure Connect

NetSecure Connect is a mid-sized Internet Service Provider (ISP) based in Karachi, Pakistan. It provides broadband and fiber-optic internet services to residential and small business customers. The company has a main office, a customer support center, and several local data centers.

Key Services: Internet access, VoIP, smart-home router integration, network equipment leasing.
IT Infrastructure includes: central billing systems, CRM, DNS servers, NOC, customer portal, and support tools.

Scope, Goals, and Risk Assessment

Audit Scope

This internal audit aims to assess NetSecure Connect's IT and cybersecurity posture, identify current weaknesses, and provide recommendations to achieve compliance and improve resilience.

Goals

- Assess current controls and compliance status
- Identify non-compliance with PCI DSS and GDPR-like standards
- Recommend improvements to protect customer data and IT systems

Risk Assessment Summary

- Legacy CRM system with vulnerabilities
- No encryption for locally stored customer data
- No breach response policy or MFA for employees
- Limited internal network segmentation
- Weak physical access control in some data centers

Controls Assessment Checklist

Control	Yes / No
Least Privilege	No
Disaster Recovery Plans	No
Password Policies	Yes
Separation of Duties	No
Firewall	Yes
Intrusion Detection System (IDS)	No
Backups	Yes
Antivirus Software	Yes
Manual monitoring for legacy systems	No
Encryption	No
Password Management System	No
Locks (offices, storefront, warehouse)	Yes
Closed-circuit television (CCTV)	Yes
Fire detection/prevention systems	Yes

Compliance Checklist

PCI DSS

Best Practice	Yes / No
Only authorized users have access to customers' credit card information.	No
Credit card information is securely stored, processed, and transmitted.	No
Data encryption used at credit card transaction points.	No

Secure password management policies in place.	No

GDPR

Best Practice	Yes / No
E.U. customer data is kept private and secure.	No
There is a 72-hour breach notification policy.	No
Data classification and inventory exists.	No
Privacy policies are enforced and documented.	No

SOC 1 & SOC 2

Best Practice	Yes / No
User access policies are established.	No
Sensitive data is kept confidential.	No
Data integrity is maintained and verified.	No
Data access is limited to authorized personnel.	No

Recommendations for IT Manager

1. Implement least privilege access control and MFA for all employees.
2. Establish a breach response plan and data classification system.
3. Encrypt all sensitive customer and payment data.
4. Replace or isolate legacy systems with known vulnerabilities.
5. Implement intrusion detection and enhance network segmentation.
6. Ensure compliance with PCI DSS and GDPR to support international expansion.
7. Conduct regular audits and employee security training.