Date: Wed, Feb 7, 2024
To: IT Management, Axiom Apparel
From: Shafee Ahmed, Security Analyst

After a thorough review of our current security measures and compliance with PCI DSS, GDPR, and SOC standards, I've identified several critical areas that require immediate attention as outlined by the following checklists, and explained further in my suggested action items.

Controls assessment checklist

Yes	No	Control
□	☑	Least Privilege
□	☑	Disaster recovery plans
□	☑	Password policies
□	☑	Separation of duties
☑	□	Firewall
□	☑	Intrusion detection system (IDS)
□	☑	Backups
☑	□	Antivirus software
□	☑	Manual monitoring, maintenance, and intervention for legacy systems
□	☑	Encryption
□	☑	Password management system
☑	□	Locks (offices, storefront, warehouse)
☑	□	Closed-circuit television (CCTV) surveillance
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
☐	☑	Only authorized users have access to customers' credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☑	☐	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☑	☐	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☑	☐	E.U. customers' data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☑	☐	Ensure data is properly classified and inventoried.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☑	☐	Data is available to individuals authorized to access it.

Recommendations

1. Implement strict access controls. Develop a user access policy that ensures only authorized users can access sensitive customer data, such as PII (Personally Identifiable Information) and SPII (Sensitive Personal Information). This can be achieved by enforcing the principle of least privilege and the separation of duties.

2. Encrypt all sensitive data, whether at rest or in transit, especially customers' financial and personal data. Encryption adds a layer of confidentiality and mitigates the risk of data breaches.

3. Deploy an Intrusion Detection System (IDS). An IDS will enhance our security posture by assisting in the monitoring and analysis of network traffic.

4. Secure password management. Our current password policy is the bare minimum and does not meet regulatory standards. We should revise our policy to include stronger complexity requirements, such as a minimum of eight characters, at least one special symbol, and at least one number.

5. Establish a disaster recovery plan. Implement a disaster recovery strategy, including regular backups to the cloud, to ensure business continuity and availability in the event of a disaster.

I look forward to discussing these recommendations at our next teamwide security meeting. I am at your disposal should there be any questions or concerns I can help clarify in this document.