Controls and Compliance Checklist

Yes	No	Control	Explanation
	X	Least Privilege.	In the current state of the company all employees have access to PII and SPII.
	X	Disaster recovery plans.	Business continuity not guaranteed in case of disaster without plans for disaster recovery.
	X	Password policies.	Minimal requirements for employee passwords, which in turn means an easier time for a threat actor to access data.
	X	Separation of duties.	Separation of duties is crucial in minimizing the risk fraud and permission to critical data.
X		Firewall.	A firewall is already implemented.
	X	Intrusion detection system (IDS).	IDS is required to recognize threat actor intrusion.
	X	Backups.	Backups of critical data is important for business continuity.
X		Antivirus software.	Antivirus software is already in place.
	X	Manual monitoring maintenance, and intervention for legacy systems.	Systems are monitored and maintained but there is no schedule nor are there procedures that are well defined, this increases the risk of a intrusion.
	X	Encryption.	No encryption is used, this would greatly increase security of PII and SPII.

	X	Password management system.	No password management system is in place, Including it would improve the whole department work flow if an issue with a password would arise.
X		Locks(offices, storefront, warehouse).	Locks in this case are sufficient.
X		Close-circuit television (CCTV) surveillance.	CCTV is installed and maintained.
X		Fire detection/prevention (fire alarm, sprinkler system, etc).	The company has a fire detection and prevention system.

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Explanation
	X	Only authorized users have access to customer's credit card information.	The company's internal data is available to all the employees.
	X	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	Credit card information stored in the company's internal data has no encryption and can be accessed by all the employees.
	X	Implement data encryption procedures to better secure credit card transactions touchpoints and data.	The company doesn't have an encryption process.
	X	Adopt secure password management policies.	Zero to none password policies and no password management system in established in the company.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
	X	User access policies are established.	Least Privilege and Separation of duties are not established.
	X	Sensitive data (PII/SPII) is confidential/private.	PII/SPII information lack encryption.
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated.	Data integrity is established.
	X	Data is available to individuals authorized to access it.	The policies of Least Privilege need to be applied and give employees access to data only vital to their work.