Compliance Checklist

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	*Explanation*
	X	Only authorized users have access to customers' credit card information.	*Currently, all employees have access to the company's internal data.*
	X	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted and all employees currently have access to internal data, including customers credit card information.*
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company does not currently use encryption to better ensure the confidentiality of customers financial information.*
	X	Adopt secure password management policies.	*Password policies are nominal and no password management system is currently in place.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
	X	E.U. customers' data is kept private/secured.	*The company does not currently use encryption to better ensure the confidentiality of customers financial information.*
X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*There is a plan to notify E.U. customers within 72 hours of a data breach.*

	X	Ensure data is properly classified and inventoried.	*Current assets have been inventoried/listed, but not classified.*
X		Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees, as needed.*

<u>System and Organizations Controls (SOC type 1, SOC type 2)</u>

Yes	**No**	**Best practice**	***Explanation***
	X	User access policies are established.	*Controls of Least Privilege and separation of duties are not currently in place; all employees have access to internally stored data.*
	X	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not currently used to better ensure the confidentiality of PII/SPII.*
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is in place.*
	X	Data is available to individuals authorized to access it.	*While data is available to all employees, authorization needs to be limited to only the individuals who need access to it .*