Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Explanation
□	☑	Only authorized users have access to customers’ credit card information.	All employees has access to customer's credit card information as no encryption and access control management is in place.
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Sensitive data is not encrypted and is stored locally in the internal database.
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Encryption is not currently used to ensure confidentiality of these sensitive data.
□	☑	Adopt secure password management policies.	Password management is not implemented.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
□	☑	E.U. customers’ data is kept private/secured.	The company does not currently use encryption to better ensure the confidentiality of customers’ financial information.
☑	□	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.

□	☑	Ensure data is properly classified and inventoried.	Current assets have been inventoried/listed, but not classified.
☑	□	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.

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

Yes	No	Best practice	Explanation
□	☑	User access policies are established.	Access controls pertaining to least privilege and separation of duties have not been implemented.
□	☑	Sensitive data (PII/SPII) is confidential/private.	Encryption is not currently used to better ensure the confidentiality of PII/SPII.
☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	The IT department has ensured availability and integrated controls to ensure data integrity.
□	☑	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 to do their jobs.