VENDOR
SECURITY AUDIT

VENDOR BUSINESS CONTINUITY / DISASTER RECOVERY

	SATISFACTORY	N / A	UNSATISFACTORY
Vendor has a **business continuity plan.**	☐	☐	☐
Vendor incorporates **Denial-of-Service** & other cyber-attacks as part of their business continuity plan.	☐	☐	☐
Vendor has an updated **disaster recovery plan.**	☐	☐	☐

VENDOR ORGANIZATIONAL SECURITY

	SATISFACTORY	N / A	UNSATISFACTORY
Employees of vendor complete **routine cybersecurity training.**	☐	☐	☐
Vendor has a formal **change control process** for IT.	☐	☐	☐
Vendor is able to provide a **company security rating.**	☐	☐	☐
Vendor is able to provide a **history of data breaches** (if any). Vendor	☐	☐	☐
has an **adequate password policy.**	☐	☐	☐

VENDOR GENERAL SECURITY

	SATISFACTORY	N / A	UNSATISFACTORY
Vendor installs **antivirus software** on systems & endpoints.	☐	☐	☐
Vendor **routinely patches** systems.	☐	☐	☐
Vendor **tests patches** prior to implementation.	☐	☐	☐
Vendor invests in **data protection & security controls.**	☐	☐	☐
Vendor **restricts physical access** to core processing systems. Vendor	☐	☐	☐
has a process for **secure disposal** of equipment.	☐	☐	☐
Employees have **unique login ID's** when accessing data.	☐	☐	☐

techtron

www.techtron.co.za

info@techtron.co.za

VENDOR
SECURITY AUDIT

VENDOR NETWORK SECURITY

	SATISFACTORY	N / A	UNSATISFACTORY
Vendor protects network boundaries using **firewalls.**	☐	☐	☐
Vendor regularly performs **network vulnerability scans.**	☐	☐	☐
Vendor uses an **IDS** or **IPS** on their network.	☐	☐	☐
Vendor's remote users are required to use **VPNs** when accessing vendor's systems.	☐	☐	☐
Vendor protects **wireless networks** (if applicable).	☐	☐	☐

VENDOR SYSTEM SECURITY

	SATISFACTORY	N / A	UNSATISFACTORY
Vendor has verified **backup & recovery process.**	☐	☐	☐
Vendor uses **access control** (Ex: RBAC).	☐	☐	☐
Vendor uses an **IDS** or **IPS** on their network.	☐	☐	☐
Vendor restricts systems that contain **sensitive data** to only authorized users.	☐	☐	☐
Vendor securely collects, stores, or transmits **PII** (if applicable).	☐	☐	☐
Vendor has **mitigations in place** for web application exploits such as **SQL Injection & XSS scripting attacks** (if applicable).	☐	☐	☐

VENDOR INCIDENT RESPONSE

	SATISFACTORY	N / A	UNSATISFACTORY
Vendor has an **incident response team.**	☐	☐	☐
Vendor **continuously monitors security controls** to protect cybersecurity incidents.	☐	☐	☐
Vendor has a process to **remediate newly found risks.**	☐	☐	☐

techtron

info@techtron.co.za

www.techtron.co.za

VENDOR
SECURITY AUDIT

VENDOR AUDITING / REPORTING / REGULATIONS

	SATISFACTORY	N / A	UNSATISFACTORY
▸ Vendor has had an **IT audit** in the past 12 months.	☐	☐	☐
▸ Vendor has had a **penetration test** in the past 12 months. Vendor is	☐	☐	☐
▸ able to provide **penetration test results.**	☐	☐	☐
▸ Vendor is able to provide an **IT system outline.**	☐	☐	☐
▸ Vendor complies with any **necessary governmental regulations** (if applicable).	☐	☐	☐
▸ Vendor has **industry standard certifications** (if applicable).	☐	☐	☐
▸ Vendor monitors their vendors' **risk & standing.**	☐	☐	☐

COMMENTS