Internal Security Procedures

CONTROL	STATUS
Vulnerabilities scanned and remediated Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	✓
Continuity and disaster recovery plans tested The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	✓
Incident response plan tested The company tests their incident response plan at least annually.	✓
Access requests required The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	✓
Backup processes established The company's data backup policy documents requirements for backup and recovery of customer data.	✓
Vendor management program established The company has a vendor management program in place. Components of this program include: ▪ critical third-party vendor inventory; ▪ vendor's security and privacy requirements; and ▪ review of critical third-party vendors at least annually.	✓
Incident response policies established The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	✓
Configuration management system established The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	✓
Management roles and responsibilities defined The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	✓
Service description communicated The company provides a description of its products and services to internal and external users.	✓
Security policies established and reviewed The company's information security policies and procedures are documented and reviewed at least	✓
Support system available The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. annually.	✓
Roles and responsibilities specified Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	✓

Data center access reviewed
The company reviews access to the data centers at least annually.

Physical access processes established
The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorisation from control owners.

Third-party agreements established
The company has written agreements in place with vendors and related third-parties.
These agreements include confidentiality and privacy commitments applicable to that entity.

Incident management procedures followed
The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

Development lifecycle established
The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

Cybersecurity insurance maintained
The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.

Continuity and Disaster Recovery plans established
The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.