Infrastructure security

CONTROL	STATUS
Encryption key access restricted The company restricts privileged access to encryption keys to authorized users with a business need.	✓
Unique account authentication enforced The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	✓
Production application access restricted System access restricted to authorized access only	✓
Production database access restricted The company restricts privileged access to databases to authorized users with a business need.	✓
Production OS access restricted The company restricts privileged access to the operating system to authorized users with a business need.	✓
Production network access restricted The company restricts privileged access to the production network to authorized users with a business need.	✓
Unique network system authentication enforced The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	✓
Remote access encrypted enforced The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	✓
Log management utilized The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	✓
Network segmentation implemented The company's network is segmented to prevent unauthorized access to customer data.	✓

1 to 10 of 14 results

Organizational security

CONTROL	STATUS
Asset disposal procedures utilized The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	✓
Production inventory maintained The company maintains a formal inventory of production system assets.	✓
Portable media encrypted The company encrypts portable and removable media devices when used.	✓
Anti-malware technology utilized The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	✓
Performance evaluations conducted The company managers are required to complete performance evaluations for direct reports at least annually.	✓
MDM system utilized The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	✓

Product security

CONTROL	STATUS
Data encryption utilized The company's datastores housing sensitive customer data are encrypted at rest.	✓
Control self-assessments conducted The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	✓

Internal security procedures

CONTROL	STATUS
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.	✓
Continuity and disaster recovery plans tested The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	✓
Cybersecurity insurance maintained The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	✓
Whistleblower policy established The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	✓
Board oversight briefings conducted The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	✓
Board charter documented The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	✓
Board expertise developed The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	✓
System changes externally communicated The company notifies customers of critical system changes that may affect their processing.	✓
Organization structure documented The company maintains an organizational chart that describes the organizational structure and reporting lines.	✓
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.	✓

1 to 10 of 22 results

Data and privacy

CONTROL	STATUS
Data retention procedures established The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	✓
Customer data deleted upon leaving The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	✓
Data classification policy established The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	✓
Production data segmented The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	✓