Security at Crescendo

Last updated: June 2020

Introduction

At Crescendo, performance, security and data privacy are first-order considerations. Protecting your data is one of our most important responsibilities, and we are committed to being transparent about our practices and helping you understand our approach to security.

Our goal is to take a comprehensive, multi-layered approach to security, ensuring that every element of your data is secure. As new threats emerge, Crescendo is committed to staying diligent in complying with new standards and always striving to improve.

Organizational Security

Crescendo's security program is managed by our Data Protection Officer and Chief Technology Officer, who work together to lead our security personnel and maintain a comprehensive security program that is compliant and constantly evolving with modern industry standards.

As part of our employee onboarding, the focus on security and privacy of information is a key theme. All staff members are required to undergo security training as part of their onboarding, as well as semi-annually. At Crescendo, security is always top of mind.

Protecting Customer Data

Crescendo's security program is designed to prevent unauthorized access to customer data. With risk assessment built into our SDLC, Crescendo strives to catch all vulnerabilities in the design and testing phases. We recognize that this is not always possible, so we have put in place mitigation measures to protect your data at all stages.

Encryption

Each Crescendo customer's data is logically separated from other customers' data. Crescendo's servers are housed in data centers provided and maintained by Amazon Web Services, which employs state-of-the-art physical security to secure the data entrusted to Crescendo.

- **Data at Rest**
  Data at rest in Crescendo's production network is encrypted using industry standard algorithms. All encryption keys are securely stored and access is strictly limited.

- **Data in Transit**
  All client data is encrypted in transit on internal and external networks.

Network Security

Crescendo separates its systems in distinct networks to protect customer data and sensitive data. Production infrastructure is separated from infrastructure used for testing and development.

Network access is restricted to the external web, and mitigations are put in place to prevent against DoS/DDoS attacks. Crescendo also logs network access, audits logs regularly, and has alerts in place for potential intrusions.

Physical Security

Amazon Web Services

Crescendo's services, including data storage, run on Amazon Web Services. The Amazon Web Services platform is designed and built to run on a shared security responsibility model. AWS is responsible for securing the underlying infrastructure that supports our platform, including facilities, network, hardware, and operational software. The infrastructure that Amazon provides is designed and managed in alignment with security best practices and a variety of IT security standards, including SOC 1, 2 and 3, and ISO 27001.

Access Control

Access to systems is restricted by role, and Crescendo adheres to the principles of least privilege wherein staff members are only able to access data that is reasonably required

to fulfill the duties of their role at Crescendo. Production access is reviewed at least quarterly to ensure access roles are always up to date.

Multi-factor authentication is required for remote access to company networks and for all access to systems storing customer data.

Crescendo requires all company accounts and devices to meet minimum password requirements in accordance with our secure password policy. All systems that interact with customer data must meet our password requirements.

Asset Management

All devices issued by Crescendo to Crescendo staff are configured and maintained by Crescendo to comply with our security standards. By default, Crescendo's configuration requires machines to lock when idle, have strong passwords that comply with our password policy, and encrypt data at rest. Devices provided by Crescendo also run anti-virus and anti-malware software.

Mobile devices that are not provided by Crescendo but are used to engage in company business are required to be enrolled in Crescendo's mobile device management system to ensure they meet Crescendo's security standards. These devices are managed by Crescendo and access is revoked immediately upon termination of the relationship with a staff member.

System Monitoring, Logging, and Alerting

Crescendo monitors its systems to maintain an up-to-date view of the state of security and alert responsible personnel to any abnormal or suspicious activity. All production systems are monitored, and access logs are reviewed frequently and stored for a minimum period of 24 months. Production logs are segregated and access is restricted to only the relevant security personnel.

Data Retention and Disposal

Crescendo retains data in accordance with our data classification and retention policy. Customer data is deleted immediately upon request by the end user.

Disaster Recovery and Business Continuity

Crescendo uses services provided by its hosting provider to distribute production operations across multiple physical locations to protect availability of Crescendo services. Crescendo maintains a full backup of production data, to which full backups are saved regularly. Backups are tested at least semi-annually to ensure they can be successfully restored.

Responding to Security Incidents

Crescendo's incident response plan defines procedures for responding to potential security incidents. This plan defines the types of events that are required to be managed by the incident response process, classifies these events by severity, and includes specific instructions on how to alert relevant parties including our customers. Crescendo's incident response plan is tested and updated semi-annually. In the event that an incident is detected, affected customers will be informed within 24 hours via email and/or phone by Crescendo's Customer Success team.

Vendor Management

In some cases, Crescendo leverages third party vendors to provide services and operate efficiently. In the cases where those third parties may interact with or affect the security of customer data, Crescendo takes appropriate measures to review the vendors for risk and establish agreements that require vendors to meet or exceed the security and confidentiality commitments we have in place with our customers and users. Crescendo enforces the requirement for non-disclosure agreements prior to sharing sensitive or restricted information with any third party.

External Validation

Crescendo employs a third party vendor to conduct penetration tests semi-annually. Results of these penetration tests are shared with security personnel and the findings are remediated in a timely manner. Customers may request executive summaries of these reports by contacting their Customer Success Manager.

Conclusion

Our security program covers all aspects of our business that involve access to customer data. This includes our software, the infrastructure that supports our platform, our internal processes, how we hire, onboard and train employees, how we manage customer accounts and data, and how we engage with third party vendors. The security of your data is of critical importance to us. Should you have any questions or concerns about our security program, you may contact us at security@crescendowork.com, or reach out directly to your Customer Success Manager.