Security Statement

Last Updated: 3/28/2023

Introduction

EMS LINQ, LLC. ("LINQ" or the "Company") is committed to protecting the data that it receives, stores, and processes on behalf of customers that use the Company's Software-as-a-Service solutions ("Customer Data").

This Security Statement outlines LINQ's approach to security, and focuses on the administrative, physical, and technical controls that the Company has implemented to protect the Company's SaaS solutions and the Customer Data that LINQ handles in connection with those solutions.

Security Organization and Program

Security is a key priority at LINQ. The Company's security program is managed by LINQ's Chief Information Security Officer (CISO), who meets with executive management regularly to discuss security-related issues and coordinate company-wide security initiatives.

LINQ maintains a comprehensive set of information security policies and procedures that govern the handling of Customer Data, including its receipt, access, storage, transmission, distribution, and deletion. These policies and procedures are approved by Senior Management and are reviewed and updated regularly to address evolving standards and requirements. These policies and procedures include:

- Organizational Security
- Physical and Environmental Security
- Communications and Connectivity
- Change Control
- Data Integrity

- Incident Response
- Privacy
- Backup and Offsite Storage

LINQ personnel involved in LINQ's security program are encouraged to maintain an active role in relevant cybersecurity information sharing forums, special interest groups, and professional associations to stay up to date on new and emerging cybersecurity risks that may impact the Company or its operations.

Security Controls Infrastructure and Physical Security

LINQ's SaaS Solutions are built on enterprise-grade commercial cloud infrastructure operated by third-party providers such as Rackspace, AWS, Azure, and Google. These providers comply with leading security standards and frameworks, including ISO/IEC 27001, SSAE 18 SOC 2, and PCI-DSS. They apply physical security controls at their data centers that include biometric and badge-based access controls, 24/7 monitoring by video and security personnel, intrusion detection systems, and controls to mitigate the risk of fires, power loss, climate, and temperature variabilities.

LINQ also applies physical security controls in its own offices and other LINQ-controlled facilities where customer data is processed. Those controls include:

- Badge-based access controls and audit trails;
- Mandatory visitor escorts;
- Video monitoring of all entrance and exit points;
- Intrusion detection alarms at egress and ingress points;
- Clean desk and clear screen policies;
- Documented procedures for the addition and removal of information assets to and from facilities; and
- Periodic testing of physical security controls.

Data Security

Data Classification

LINQ has implemented a data classification policy that classifies data according to sensitivity and applies corresponding access control, handling rules, and retention rules.

Data Segregation

LINQ's solutions are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides effective logical data

separation for different customers using customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for development and production.

Data Access Controls

LINQ has implemented policies, procedures, and technical controls to ensure that access to Customer Data is managed on a "need to know basis," that LINQ personnel appropriately protect their access, and that information is accessed securely.

LINQ assigns user access privileges based on the principle of least privilege according to a user's role and business need. Documented request and approval processes must be followed to gain access to assets that are not within a user's assigned to a role. Additional controls are assigned for privileged access rights such as administrators of applications. LINQ conducts quarterly manual reviews of user accounts and security groups to ensure access privileges remain correctly assigned.

LINQ personnel are assigned unique user IDs which must be used to access information assets, and LINQ has implemented a password policy to ensure employees set strong passwords and protect them appropriate. Rules for sharing and inputting passwords are enforced to avoid unauthorized use and disclosure.

Data Encryption

LINQ encrypts databases housing sensitive Customer Data at rest using industry-standard encryption protocols.

Data Retention and Disposal

LINQ has implemented documented data retention and disposal procedures to ensure the secure retention and disposal of Customer Data and associated media in accordance with applicable regulations and LINQ's contractual agreements with Customers.

Network Security

LINQ has implemented several measures designed to ensure the security of the Company's networks and to protect Customer Data in transmission.

LINQ's Cloud Services team has implemented procedural and technical standards for the deployment of network devices that include baseline configurations for network devices, network architecture, and approved protocols and ports. The LINQ networking team regularly monitors network devices for compliance with technical standards and potential malicious activities.

Remote access to production systems by LINQ personnel is restricted to authorized employees over an encrypted virtual private network (VPN) connection, protected with Multi-Factor Authentication (MFA).

Customer Users access LINQ solutions through the internet, protected by Transport Layer Security (TLS). This secures network traffic from passive eavesdropping, active tampering, and forgery of messages.

Firewalls are used and configured to prevent unauthorized access to production environment LINQ uses defined Access Control Lists (ACLs) to restrict traffic on routers and firewalls, which are reviewed and approved by network administrators. IP addresses in the ACLs are specific and anonymous connections are not allowed (except ports 443 and port 80 on the web applications). LINQ performs periodic recertification and authorization of firewall rules.

LINQ has implemented an intrusion detection system managed by a third party to provide continuous monitoring of the company's network and early detection and alerting of suspicious activity. Anti-virus and anti-malware software is deployed in environments susceptible to malicious attacks, and installed on all workstations.

Application Security

LINQ has an established software development lifecycle to ensure the security of the applications developed by the Company.

Development Lifecycle

LINQ's Software Development Life Cycle (SDLC) methodology includes version control and release management procedures. System documentation is managed by appropriate access controls. Software vulnerability testing is completed before release and any vulnerability gaps identified are remediated in a timely manner.

Development teams are also required to perform threat modeling exercises that are reviewed and approved by the Cloud Services team. Each team has an SDLC owner who is responsible for ensuring the appropriate completion of the SDLC tasks. The SDLC owner reviews the SDLC tasks and gives the overall sign-off for completion of the SDLC process.

Security in Development and Support Process

LINQ follows the Agile development methodology in which products are deployed following comprehensive requirement gathering, system design, implementation, testing and deployment phases. Security and security testing are implemented throughout the entire software development methodology.

Quality Assurance is involved in the lifecycle and security best practices are a mandated aspect of all development activities. Test areas include volume, stress, security, performance, resource usage, configuration, compatibility, installation, and recovery testing.

The development process includes a review of all embedded third-party components to ensure that security updates are incorporated. Use of open-source software is subject to technical review and approval.

Personnel Security

LINQ emphasizes security as part of its personnel practices, and security is an important part of the Company's workplace culture.

Hiring and Onboarding

Before they join our staff, LINQ conducts criminal background checks on new hires before their start dates.

When they begin employment, all employees are required to acknowledge and agree to LINQ's code of conduct, which includes LINQ's requirements for employees' use of LINQ-controlled data and information systems. New employees are also required to sign a confidentiality agreement that strictly prohibits the unauthorized disclosure of Customer Data and other information to which they are provided access in connection with their employment. Employees who violate these requirements are subject to disciplinary action, up to and including termination of employment.

Training

Upon hire and annually thereafter, all LINQ employees must successfully complete training courses covering basic information security practices. The training courses are designed to assist employees with identifying and responding to social engineering attacks and avoiding inappropriate security practices.

Development and Cloud Operations staff receive further training specific to product development, deployment, and management of secure applications. Additional security training is also provided to employees who handle Customer Data.

Termination

LINQ's Human Resources department manages a formal termination process, which includes notification of LINQ's Corporate IT and Cloud Operations and Facilities departments, the removal of the ex-employee's access privileges, and the return of the employee's information assets and access cards. The exit interview reminds ex-employees of their remaining employment restriction and contractual obligations.

Third Party Security

LINQ has implemented and maintains a vendor and business partner oversight program that is designed to ensure that third parties involved in delivering LINQ's solutions comply with LINQ's security requirements.

That program requires all contracts with vendors or business partners to clearly address (a) the requirement for the vendor or business partner to meet LINQ's information security standards, (b) the ability to perform independent audits of the effectiveness of internal control processes, and (c) the requirement to obtain and provide a third-party attestation report.

Disclosure of any confidential information to a vendor or business partner is provided only as needed and only if the vendor or business partner has implemented appropriate information security and confidentiality controls.

Monitoring and Vulnerability Management

As part of its security program, LINQ pursues various strategies to monitor the security of its information resources and to manage vulnerabilities in its network and solutions.

Annual Risk Assessments

LINQ conducts an annual risk assessment to identify and manage risks that could affect the security of Customer Data or the Company's ability to reliably provide its solutions. The risk assessment process requires management to identify significant risks and to implement measures to address those risks. The Company's risk assessment methodology seeks to identify, measure, and prioritize risks affecting information systems, which in turn informs the continuous improvement of the Company's security strategy.

Internal and external network vulnerability scans

The Company carries out quarterly internal and external scans to identify vulnerabilities in the company's systems. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed, and identify vulnerabilities. The scanning reports are reviewed by appropriate personnel and remediation efforts are conducted in a timely manner.

External penetration testing

LINQ engages an independent third party to conduct penetration testing of the Company's solutions and external perimeter at least annually. All findings are triaged and are remediated within appropriate timelines.

Incident Response

The Company has established and documented an incident response plan and corresponding procedures to respond to incidents that involve suspected compromise of, or unauthorized access to, Customer Data or other Company information, or Company information systems. The incident response plan is tested annually to assess its effectiveness.

The Company maintains several different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting the Cloud Services team per defined and configured events, thresholds, or metric triggers. Incidents may also be reported by email. Users are made aware of their responsibility to report incidents and that reports will be investigated without any negative consequences for the reporting party.

The Company has designated an incident response team to provide 24/7 event and incident monitoring and response services. The team use established incident classification, escalation, and notification processes for assessing an incident's criticality and severity, and corresponding escalation

to appropriate groups, including privacy, legal, and executive management teams. Incident response team members are trained on the Company's incident response plan and procedures.

Following any high severity incidents, LINQ performs post-mortem reviews to evaluate the lessons learned and identify potential areas of improvement.

Business Continuity/Disaster Recovery

Disaster Recovery Plan

LINQ has adopted and implemented a documented disaster recovery plan (DRP) to guide the recovery of the Company's solutions and other critical services from high-severity outages and other incidents. The DRP includes scope and applicable dependencies for the services, restoration procedures, and communications with appropriate teams. The DRP is reviewed at least annually by a designated user and made available to all applicable users.

Availability and Capacity

The Company continually monitors its network to ensure availability and addresses capacity issues in a timely manner. The process for capacity planning includes an analysis of the capacity based on various parameters. Actions identified from the review are assigned for appropriate resolution. Additionally, the Company projects future capacity requirements.

Backup and Offsite Storage

LINQ has adopted and implemented a documented backup policy and associated procedures for performing backup and restoration of data in a scheduled and timely manner. Controls are established to help safeguard backed up data both onsite and offsite. LINQ also ensures that Customer Data is securely transferred or transported to and from backup locations. LINQ also conducts periodic tests to ensure that data can be safely recovered from backup devices.

Backup Media Destruction

LINQ has adopted and implemented documented procedures for the secure destruction of backup media that includes media destruction by a qualified third party and written confirmation of secure destruction.

Offsite Storage Security

Physical security for the offsite backup storage facility is documented and provided by third-party storage vendors. Access control is enforced at entry points and in storage rooms. Access to the offsite facility is restricted and there is an approval process to obtain access. Backup storage devices (e.g. backup tapes, cloud storage, offsite backups) are encrypted. Secure transportation procedures (e.g. inventory tracking, signed checklists) or media to and from the off-site location are defined.

Audits and Certifications

SOC 2

LINQ has achieved a System and Organization Control 2 (SOC 2) Type 2 report. The LINQ SOC 2 report addresses the trust services criteria relevant to security, availability, and confidentiality. The scope of LINQ's SOC 2 report covers the LINQ Platform of solutions, which includes LINQ State, LINQ ERP, LINQ Nutrition, LINQ Digital, and LINQ Payments.

LINQ's SOC 2 audit is conducted annually by an independent third-party auditor and validates LINQ's logical and physical access controls, system operations management procedures, software development practices, and backup and disaster recovery procedures.

SOC 1

LINQ has achieved a System and Organization Control 1 (SOC 1) Type 2 report. The SOC 1 report addresses the internal controls LINQ has implemented to protect client data, specific internal controls over financial reporting, and data processing integrity.

PCI-DSS

LINQ completes an annual PCI DSS assessment using an approved Qualified Security Assessor (QSA). The auditors reviewed the LINQ Nutrition and LINQ Payments solutions which include validating the infrastructure, development, operations, management, support, and in-scope services.

The PCI DSS designates four levels of compliance based on transaction volume. LINQ Nutrition and LINQ Payments are certified as compliant under PCI DSS version 3.2 at Service Provider Level 1 (the highest volume of transactions, more than 6 million a year).