Credit Union Web Solutions Services System

SOC 3 Report

January 1, 2025 to December 31, 2025

Table of Contents

Section I – Assertion of CUSG's Management

Assertion of CUSG's Management

We are responsible for designing, implementing, operating, and maintaining effective controls within CU Solutions Group, Incorporated's ("CUSG") Credit Union Web Solutions Services System throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that CUSG's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (With Revised Points of Focus – 2022)* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that CUSG's service commitments and system requirements were achieved based on the applicable trust services criteria. CUSG's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CUSG, to achieve CUSG's principal service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of CUSG's controls. The description does not disclose the actual controls at the subservice organizations.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CUSG, to achieve CUSG's principal service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of the service organization's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that CUSG's service commitments and system requirements were achieved based on the applicable trust services criteria.

Timmy Bohlman, Chief Technology Officer
May 19, 2026

Section II – Independent Service Auditor's Report

BARNES DENNIG
Accounting • Tax • Business Insight

OHIO OFFICE
150 E. 4th Street
Cincinnati, OH 45202
Main: 513.241.8313
Fax: 513.241.8303

Independent Service Auditor's Report on a SOC 3 Examination

To: CU Solutions Group

Scope

We have examined CU Solutions Group, Incorporated's ("CUSG" or "Service Organization") accompanying assertion titled "Assertion of CUSG's Management" (assertion) that the controls within CUSG's Credit Union Web Solutions Services system were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that CUSG's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Processing Integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (With Revised Points of Focus – 2022)* in AICPA, Trust Services Criteria.

The description of the boundaries of the system indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CUSG, to achieve CUSG's principal service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of CUSG's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CUSG, to achieve CUSG's principal service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of CUSG's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

CUSG is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that CUSG's service commitments and system requirements were achieved. CUSG has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, CUSG is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards

established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the Service Organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve CUSG's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve CUSG's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AIPCA. We applied the statements on quality control standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within CUSG's Credit Union Web Solutions Services system were effective throughout the period January 1, 2025 to December 31, 2025 if complementary subservice and user entity controls contemplated in the design of the Service Organization's controls operated effectively, to provide reasonable assurance that CUSG's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Barnes Dennig & Co., Ltd.
May 19, 2026

Section III – Description of the Boundaries of the Credit Union Web Solutions Services System

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The examination covers both CUSG internal technology and CUSG dedicated Web Hosting systems security, availability, processing integrity and confidentiality controls. The systems are comprised of the following components:

- Software
- Data
- Infrastructure
- People
- Procedures

These five components comprising the Credit Union Web Solutions Services System are described below:

SOFTWARE

CUSG Web developers are proficient in producing sophisticated and modern web products using technologies such as XML, JSON, JavaScript, jQuery, AJAX, PHP, Linux, MariaDB, Vue, Bootstrap, and Microsoft Tools. CUSG develops web-based applications for presentation of customer web sites and customer data where applicable.

DATA

When CUSG systems process client data, CUSG serves as a data processor service provider. CUSG considers its Credit Union clients to be data controllers.

Client data received and/or maintained by CUSG is safeguarded and protected, regardless of the type of data, at all times. This protection includes:

- Restricting access to only designated database personnel
- Maintaining the data on secure servers located in a secured server room at NTT

Any data that the customer has not requested CUSG to retain is electronically deleted and e-shredded after its intended use.

Specific data and data types stored in the CUSG applications are client driven and controlled. Clients maintain direct control over the data itself and administer user credentials and access privileges. While the client may choose to include nearly any kind of data the table below describes some typical cases.

CUSG Application	Data Types
Content Management System (CMS)	Client driven and controlled, content can be client administered by user credentials and privileges. Rate and product descriptions, ties to home banking, and lending origination systems, and member services communications.
Performance Pro 4	Client driven and controlled, content is client administered by user credentials and privileges. Baseline content is provided by CUSG including competencies and goals. Factors are pre-weighted. These elements are client modifiable. Client can also

CUSG Application	Data Types
	add additional data points per user in Performance Pro. (It is possible to add sensitive information, but CUSG highly recommends against this practice.) Email addresses, first and last names, company affiliation.
The Learning Center	Client driven and controlled, content can be client administered by user credentials and privileges. Based on various client administered user rights individuals have access to curated self-paced learning content. Email addresses, first and last names, company affiliation.

INFRASTRUCTURE

Internet Connectivity

Internet connectivity in the NTT hosted environment is currently multiple GIG-E, OC192, and OC48 from multiple Tier 1 providers, with the capacity to upgrade bandwidth as required. The Tier 1 internet providers guarantee 99.9% uptime, which CUSG passes through to its customers through the NTT network.

Network Security

CUSG network security includes:

- Email Security Services - Email is hosted with Microsoft 365 services. Email security including filtering spam, viruses, phishing, denial of service attacks ("DoS"), harvesting, and other attacks are handled through Microsoft online services.

- Encryption - sensitive customer data is stored using BitLocker encryption provided by Microsoft 365. Keys are centrally administered by Microsoft for encrypted data.

CUSG network security at the NTT Hosting facility uses the following technologies to secure customer data and information passed across the Internet:

- Multi-tenant Juniper firewalls with a virtual firewall instance running AppSecure inspection.
- Multi-tenant cloud-based Palo Alto implementation with standard profile for Denial of Service ("DoS") and Distributed Denial of Service ("DDoS") protection with DoS/DDoS scrubbing services.
- Multi-tenant Cisco Nexus Ethernet switches with VLAN separation between customers.
- Multi-tenant central logging/reporting for basic operating system ("OS"), database, network, etc. (SEIMSs).
- Secure administrative environment.
- Dedicated VPN virtual appliance(s).
- Two Factor Authentication for VPN access.
- NTT host level anti-virus solutions.
- IPA identity management for assigned users with shell access to systems.
- Pure Storage arrays in the private network with logically segmented mounts for secure data storage and real-time replication to a secondary data center.

- Email Security Services - filters spam, viruses, phishing, DoS, harvest attacks, and other attacks.
- SSL Encryption and Authentication - Web applications utilize SSL encryption and authentication, as well as automatic timeout logoff.
- Encryption - areas of the hosted solution where sensitive customer data is stored uses Pure Storage with AES 256 encryption, OpenSSL encryption, and PGP encryption to store the aforementioned data.
- Access - Root access to systems is limited to approved staff identified by the CTO, and access is limited to super user do ("sudo") rights, which allow users to execute certain commands that the super user normally performs.

System Back-ups

As noted above, CUSG maintains data on secure servers at NTT and therefore relies on NTT for system backup procedures. Additionally, CUSG has an IT disaster recovery plan that is reviewed and updated annually.

Access to Facility

CUSG does not maintain a physical location and therefore does not have a facility to access. CUSG relies on the physical access controls in place at NTT. CUSG obtains and reviews the NTT SOC 2 type II report annually noting that controls related to physical access appear reasonable and sufficient. See listing of complementary subservice organization controls in which CUSG places reliance on NTT SOC report in Section IV.

PEOPLE

CUSG Technology Solutions is supported by the following key functional staff:

Chief Technology Officer – The CTO oversees all operations of the Technology Solutions area, and monitors security and change controls. The CTO is responsible for the NTT hosting environment. The CTO ensures that all policies and procedures are in place, and audits all operations of the Technology Solutions area, reporting results to the Security Team.

Chief Information Security Officer – The CISO Supports the control environment by establishing accountability, clearly communicating security responsibilities, and overseeing risk assessment and monitoring activities in alignment with management's objectives.
Director of Information Technology – The DIT is responsible for the overall infrastructure of corporate office technology, internal technology planning, implementation, and oversight. The DIT manages the internal IT team.

Manager of Software Development – The Manager of Software Development ("MSD") assists the CTO in the daily operations of the NTT hosting environment.

Senior Application Developer – Senior Application Developers ("SAD") assist the CTO and the MSD in the daily operations of the NTT hosting environment.

Application Developers – Application Developers perform application programming changes to the CUSG Web Hosting environment.

Web Developers – Web Developers are responsible for daily support of CUSG Web Hosting customers. They perform basic changes to customer hosted files, email support, and general troubleshooting. They perform change control activities around updates they perform for customers.

PROCEDURES

CUSG has documented policies and procedures that support the management, operations, monitoring and controls over CUSG IT and NTT hosting environments. Specific examples of relevant policies and procedures include, but are not limited to, the following:

- Technology and Security Policies
- Technology Solutions Policies
- Risk Assessment
- Incident Response Policy
- Change Management Policy & Procedures

OTHER ASPECTS OF CUSG'S CONTROLS

CONTROL ENVIRONMENT

Organization and Management

CUSG's control environment is the responsibility of its Executive Management as they oversee the management of their respective departments. They ensure that each department's control activities, policies, standards, and procedures reflect positively on the organizational missions and customer service.

Management Philosophy and Operating Style

CUSG's mission is to provide web-based technology solutions for organizations nationwide. CUSG will deliver operational excellence in all divisions of the company and meet or exceed our commitments to the many constituencies we serve. Executive Management has an open door to customers and employees at all times and their direct contact information is openly communicated to ensure immediate escalation occurs. This enables Executive Management to participate in organizational controls. An operational emphasis is placed on timely and accurate responses and customer service is emphasized with a commitment to exceeding customers' expectations and building a team environment that includes employees, vendors, customers, and contractors.

Assignment of Authority and Responsibility

CUSG's Executive Management includes the Chief Executive Officer ("CEO"), Chief Operating Officers ("COO"), Chief Financial Officer ("CFO"), and its Board of Directors. They have ultimate responsibility for all activities within CUSG, including the internal controls which are executed by the CTO. This includes the assignment of authority and responsibility for operation activities, and establishment of reporting relationships and authorization protocols.

Organizational Structure

Management has a clearly defined organizational chart and staff job descriptions to ensure the functions and reporting relationships are understood.

Training

CUSG provides training on its hi-tech equipment and computer applications primarily via on-the-job-training ("OJT"). New production employees are hired with the basic skill sets necessary for their respective job assignments. Additional training is normally accomplished via OJT. When new equipment or applications are introduced into the company, either an instructor for the new equipment conducts training locally or, in some cases personnel are sent to the vendor's location to receive technical training. Additional training and certifications are provided to employees through online training.

Hiring Practices and Human Resource Policies

CUSG hires skilled staff with the necessary qualifications to perform the required duties. Criminal background checks are performed prior to hiring. To ensure that the necessary skill sets are maintained, budget is allocated annually to provide training for staff. Written performance evaluations are performed annually to provide employees with an evaluation of their performance and to provide performance improvement feedback.

Each new employee is put through a formal orientation. The orientation process carefully reviews the Personnel Policy Manual, offers an organizational overview, and discusses a range of procedures and job requirements. Detailed policies pertaining to customer information security are reviewed closely during orientation. It is clearly communicated that a breach in these policies may result in disciplinary action, including suspension or termination of employment. The Personnel Policy Manual is reviewed and updated periodically throughout the year as needed by the Executive Management team.

CUSG is an equal opportunity employer and makes employment decisions based on merit. Company policy prohibits unlawful discrimination based on genetic characteristics, race, color, creed, gender, gender identity, marital status, age, national origin or ancestry, physical or mental disability, medical condition, veteran status, sexual orientation or any other consideration made unlawful by federal, state, or local laws.

CUSG is committed to complying with all applicable laws providing equal employment opportunities. This commitment applies to all persons involved in the operations of CUSG and prohibits unlawful discrimination by any employee of CUSG, including management and co-workers.

Integrity and Ethics

The organization and management of CUSG establishes a control environment within which employees must function. It is a framework for all aspects of internal control. The control environment includes a commitment to the highest ethical standards that will never compromise the truth or the company's values. Employees demonstrate professionalism through responsibility, accountability, and reliability in all interactions with customers and each other. These values have been established as performance review criteria and are used for employee evaluation.

Confidentiality Agreement

All employees are required to review and sign a confidentiality agreement on their first day of employment. The agreement, which is part of the new employee orientation packet, contains clear guidelines of the employees' role in protecting customer information. Management reviews the confidentiality guidelines with staff regularly.

Code of Ethics

CUSG's business conduct is governed by a standard of ethics to provide guidance to departments about the way the company intends to conduct business. Responsibilities covered are avoiding misrepresentation, gifts, personal conduct, compliance, service standards, equitable practices, confidentiality, conflicts of interest, marketing, and financial reporting. These are regularly communicated to all CUSG employees.

Commitment to Excellence

Excellence should reflect the knowledge and skills required to accomplish tasks that define an individual's job. Through consideration of CUSG's objectives and the strategies and plans for achievement of these objectives, management specifies the competence levels required for particular jobs and translates those levels into requisite knowledge and skills. CUSG management has analyzed and defined the tasks and knowledge requirements that comprise the positions within the organization. They consider such factors to the extent to which individuals must exercise judgment and the extent of related supervision when making hiring decisions. CUSG communicates this to personnel through the interview and performance review processes.

RISK ASSESSMENT/MANAGEMENT

CUSG has a risk assessment process that manages the risks that could affect its ability to provide reliable customer processing. Management is continuously developing its controls and is proactive with its risk assessment.

INFORMATION AND COMMUNICATION

Departmental management meetings are held where department reports and productivity statistics are communicated, issues are discussed and acted upon accordingly, and policies and procedures are defined. CUSG utilizes various methods of communication to ensure employees understand their individual roles and company controls.

MONITORING

CUSG's Management Team is involved with the day-to-day operations of the business and close supervision of Technology Solutions employees. CUSG contracts with outside consultants to perform security reviews of their systems.

CUSG uses a subservice organization to provide data center hosting and another subservice organization for file sharing and collaboration. Management requests and reviews a SOC 2 Type II examination report for each subservice organization to monitor the effectiveness of the applicable controls, with notable focus on logical security, availability (power and data connectivity), physical security and environmental controls. Network, server, and application availability and security is monitored on a 24x7 basis. Through its daily operational activities, CUSG's management monitors the services performed by the subservice organizations to ensure that operations and controls expected to be implemented at the subservice organizations are functioning effectively. CUSG's Technology Solutions staff perform periodic visits of the data center to monitor compliance with the service level agreement. Management stays abreast of changes planned at the hosting facility and relays any issues or concerns to subservice organization management.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOC)

CUSG's controls related to the credit union web solutions services system cover only a portion of overall internal control for each user entity of CUSG. It is not feasible for the Trust Services Criteria related to the credit union web solutions services system to be achieved solely by CUSG. Therefore, each user entity's internal control must be evaluated in conjunction with CUSG's controls and the related tests and results described in Section IV of this document, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations and identified below, along with the related trust services principles criteria.

Complementary Subservice Organization Control	Related Criteria	Responsible Subservices
(CSOC 1) Subservice organizations are responsible for providing adequate physical access control, monitoring, and surveillance cameras.	CC6.4	NTT and Microsoft
(CSOC 2) Subservice organizations are responsible for providing logical access control to the technical environment to adequately protect CUSG's information assets.	CC6.1 CC6.2 CC6.3 CC6.7 CC7.1	All subservice organizations
(CSOC 3) Subservice organizations are responsible for providing power conditioning, redundancy, and backup, as well as environmental control and monitoring systems.	A1.2	NTT and Microsoft
(CSOC 4) Subservice organizations are responsible for validating and background check of prospective employees before access to the physical data center environment.	CC1.4 CC1.5	NTT and Microsoft
(CSOC 5) Subservice organizations are responsible for completing regular security reviews, assessments, and audits to validate proper security controls operation and effectiveness.	CC6.8	NTT and Microsoft
(CSOC 6) Subservice organizations are responsible for maintaining incident and breach management procedures to detect, contain, remediate, and notify CUSG of any events.	CC2.3 CC7.3 CC7.4	All subservice organizations
(CSOC 7) Subservice organizations are responsible for performing incremental application-based backups every 4 hours with onsite and offsite storage, maintaining image-based backups onsite for 30 days, and retaining offsite backups. Backup data is retained and destroyed in accordance with defined retention requirements.	CC6.5 C1.2 A1.2	NTT

COMPLEMENTARY USER ENTITY (CUSTOMER) CONTROLS

CUSG's service delivery models are designed with the assumption that certain controls would be implemented by customer organizations. It is not feasible for all the controls related to the credit union web solutions services to be completely achieved by CUSG. Therefore, each customer's internal control structure must be evaluated in conjunction with CUSG's controls, considering the related complementary user entity controls identified below. Executive Management makes control recommendations to customer organizations and provides the means to implement these controls in many instances. CUSG also provides best practice guidance to customers regarding control elements outside the sphere of CUSG's responsibility. In order for a customer to rely on the controls reported in this document, each customer must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively. The following list describes certain complementary user entity controls that customers must consider to achieve the principles and criteria identified in this document. The user entity controls presented below, along with a reference to the trust services criteria, should not be regarded as a comprehensive list of all controls that customers should employ.

- Customers must control the amount, kind, and access to sensitive information which may be entered into the CUSG provided software in order to preserve security and confidentiality.
- Customers should carefully review any reports that are made available by CUSG. (Criteria CC 8.1 & PI 1.1)
- Customers are responsible for the backup of all data files, report files and program files resident on their systems used to communicate with CUSG. Appropriate backup procedures should be in place to safeguard such backups from intentional or unintentional changes, damage or theft. (Criteria A 1.2)
- Customers are responsible for ensuring that they have contingency plans that are adequate and that complement CUSG plans to form a means for handling processing disruptions. Each customer organization should have its own contingency plans to recover from a processing disruption at its own site(s). (Criteria A 1.3)

USER ENTITY RESPONSIBILITIES

Specific activities user entities must perform to fully benefit from the services.

- Customers are responsible for the security of their own networks. While the security measures surrounding CUSG provide security for its hosting platform, file sharing and collaboration, these measures do not ensure the security of the customers' networks.
- Customers should perform periodic vulnerability scanning and penetration testing of their internal network and internet-facing hosts to identify weaknesses in network security. This should be done as part of an overall information security risk assessment and program. Appropriate steps should be taken to mitigate risks discovered during the risk assessment.
- Firewall(s) that protect the customer's internal network from the internet and any implemented demilitarized zone ("DMZ").
- Periodic internal and external testing of the overall information security program.
- Establishing a DMZ for publicly accessible systems (i.e. email servers, file transfer servers, web servers, etc.).
- Use of network address translation in conjunction with internal, private IP addresses.

- Use of secure network protocols when using unsecured network connections.
- Ensuring that operating systems are security-hardened per vendor specifications.
- Ensuring that vendor software security updates are applied in a timely manner.
- Use of current anti-virus software with up-to-date virus definitions.
- Limited and controlled use of remote network access connections, such as VPN's and dial-up.
- Limited and controlled use of remote-control utilities.
- Use of strong passwords that are eight or more characters in length, are comprised of alphabetic, symbol, and numeric characters; are not allowed to be common names/words that can be easily guessed; are changed on a regular basis; and are not allowed to be re-used more than every 12 months.

CHANGES TO THE SYSTEM DURING THE PERIOD

A new Chief Information Security Officer joined the CUSG team in March of 2025. The Event Manager was discontinued as a separate product. There were no other significant changes that are likely to affect report users' understanding of how the Credit Union Web Solutions Services System is used to provide the services during the period from January 1, 2025 through December 31, 2025.

INCIDENTS

CUSG identified no system incidents during the testing period that were the result of controls that were not suitably designed or operating effectively or that resulted in a significant failure in the achievement of one or more service commitments or system requirements.

Section IV – Principal Service Commitments and System Requirements

CUSG designs its processes and procedures to meet its objectives to provide websites, consulting, custom solutions, and e-business services to Credit Union organizations. Those objectives are based on the service commitments that CUSG makes to user entities, laws and regulations that govern the provision for the collection of Customer Data and the financial, operational, and compliance requirements that CUSG has established for the services.

Security and confidentiality commitments to user entities are documented and communicated in Master Service Agreements (MSA's) and other customer agreements. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. These commitments are standardized and include, but are not limited to, the following:

Security:

CUSG agrees to take reasonable steps to protect Client's Web sites from unauthorized intrusions. These steps include employing technologies such as firewalls, IP filtering devices, Intrusion detection systems, usage logs and other system monitoring, and security-hardened software and hardware. Clients will be notified within a commercially reasonable time regarding unauthorized intrusion and steps taken in response to it.

Confidentiality:

CUSG maintains the confidentiality of all confidential or proprietary information acquired from clients and does not publish or disclose such information in any manner to any other person. CUSG has built the control environment to comply with applicable privacy laws, rules, and regulations.

Availability:

CUSG uses redundant systems, backups, and disaster preparedness to ensure client access to CUSG services across hosting platforms is maintained and monitored optimally. Appropriate mechanisms, procedures, and testing in place offer high-availability services.

Processing Integrity:

CUSG ensures the consistency and integrity of data processed for its clients through active monitoring, change control processes, data classification, and strong development activities within the CUSG hosting environment.