<COMPANY>'S DESCRIPTION OF ITS SOFTWARE APPLICATION

SECURE CYBER GATES

DOCUMENT CONTROL PAGE

Document ID	SCG/SDTEM/120/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Overview of Operations

Description of Services Provided
[About Company]
[Services Provided]

Principal Service Commitments and System Requirements

<COMPANY> designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that <COMPANY> makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that <COMPANY> has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- The fundamental design of <COMPANY>'s software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- <COMPANY> implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.

- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between <COMPANY> and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in <COMPANY> 's system policies and procedures, system design documentation, and contracts with customers. 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. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System used to provide services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures

Infrastructure

The <COMPANY> is hosted in Amazon Web Services (AWS) in their AP-South-1 region. <COMPANY>'s software application uses a virtual and secure network environment on top of AWS infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. <COMPANY> software application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through an AWS Internet Gateway, over to a virtual private cloud that:

- Houses the entire application runtime
- Protects the application runtime from any external networks

The internal networks of AWS are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through. Further, all VPC network flow logs, DNS logs, and other AWS console events are continuously monitored by AWS Guard duty to spot malicious activity and unauthorized behavior. Specifically, AWS Guard Duty uses machine learning, anomaly detection, and integrated threat intelligence to identify potential threats

Software

<COMPANY> is responsible for managing the development and operation of the <Product or service name> including infrastructure components such as servers, databases, and storage systems. The in-scope <COMPANY> infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	Business Function / Description	OS DB	Physical Location
<COMPANY> Main Web App			
AWS IAM	Identity and access management console for AWS resources.	AWS Proprietary	AWS
AWS Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.	AWS Proprietary	AWS

Amazon Simple Storage Services (S3)	Provides an interface used to store and retrieve business unit data. S3 APIs provide bucket- and object-level access and version control. S3 is controlled through the AWS IAM interface.	AWS Proprietary	AWS
GStuite	Identity/Email provider for all <COMPANY> employees	GStuite Proprietary	GCP(Gmail)

Supporting Tools	
System / Application	**Business Function / Description**
AWS Elastic Beanstalk	Service for deploying and scaling web applications and services
AWS CloudTrail	Security event logging for AWS resources
AWS CloudWatch	Security and operational monitoring and event logging for AWS resources
AWS GuardDuty	Threat detection service that continuously monitors for malicious activity and unauthorized behavior for AWS resources
Slack / G Suite	Office communication services

Network Architecture Diagram

[Insert Network Diagram/System Flow]

People

<COMPANY>'s staff have been organized into various functions like Sales, Support, Engineering, Product Management etc. The personnel have also been assigned the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, vulnerabilities, and adding controls to mitigate this risk. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Data

Data, as defined by <COMPANY>, constitutes the following:

- Transaction data

- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Output reports are available and include data and files systematically generated from the system. The availability of these reports is limited by job function. Reports delivered externally are only sent using a secure method—encrypted email, secure FTP, or secure websites to customer users.

All data that is managed, processed and stored as a part of the <COMPANY> software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value and criticality to achieving the objectives of the organization.

All customer data is categorized as confidential. Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer Confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	• Customer system and operating data • Customer PII • Anything subject to a confidentiality agreement with a customer

Company Confidential	Information that originated or is owned internally, or was entrusted to <COMPANY> by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• <COMPANY>'s PII • Unpublished financial information • Documents and processes explicitly marked as confidential • Unpublished goals, forecasts, and initiatives marked as confidential • Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Press releases • Public website

Customer data is retained per agreements with customers and disposed of upon request by customers. A confirmation is sent back to the customer to notify them that the disposal is complete

Procedures and Policies

Formal policies and procedures have been established to support the <COMPANY> software application. These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor management
- Physical security
- Risk management
- Password
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management
- Human Resource Management

All policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

<COMPANY> also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the <COMPANY> software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of <COMPANY> 's description of the system. This section provides information about the five interrelated components of internal control at <COMPANY>, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of <COMPANY>'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of <COMPANY>'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

<COMPANY> and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of business conduct" communicates the organization's values and behavioral standards to staff members
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management and

Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.

- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

<COMPANY>'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Senior Management Oversight
<COMPANY>'s control awareness is significantly influenced by its senior management. Attributes that define "tone at the top" include senior management's experience of its members, their involvement and scrutiny of operational activities, and their interaction with independent assessments of the company's operations and information security posture.

Management Philosophy and Operating Style

<COMPANY>'s management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information. <COMPANY>'s control environment reflects the philosophy of management. <COMPANY>'s information security function, composed of senior management and the Information Security Officer, meets

frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities <COMPANY> has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high severity security incidents annually.
- Senior management meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap.

Organizational Structure and Assignment of Authority and Responsibility

<COMPANY>'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and updated as required.

Human Resources

<COMPANY>'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top quality personnel who ensure the service organization operates at maximum efficiency.

Specific control activities that the service organization has implemented in this area are described below:

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's
- policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

Risk Assessment

<COMPANY> regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to the applicable trust services criteria set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

<COMPANY>'s risk assessment process identifies significant risks inherent in products and services as they oversee their areas of responsibility. <COMPANY> identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the <COMPANY>

software application, and management has implemented various measures designed to manage these risks.

<COMPANY> believes that effective risk management is based on the following principles:

- Senior management's commitment to the security of <COMPANY> software application
- The involvement, cooperation, and insight of all <COMPANY> staff
- Initiating risk assessments with discovery and identification of risks
- Thorough analysis of identified risks
- Commitment to the strategy and treatment of identified risks
- Communicating all identified risks to the senior management
- Encouraging all <COMPANY> staff to report risks and threat vectors

Scope

The risk assessment and management program applies to all systems and data that are a part of the <COMPANY> software application. The <COMPANY> risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of <COMPANY>'s Information Security Officer and the department or individuals responsible for the area being assessed. All <COMPANY> staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

<COMPANY> uses a number of vendors to meet its business objectives. <COMPANY> understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

<COMPANY> employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, <COMPANY> assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support <COMPANY>'s commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, <COMPANY> management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, <COMPANY> identifies the specific risks that service commitments may not be met, and designs controls necessary to address those risks. <COMPANY>'s management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity and mitigating action.

Control Activities

<COMPANY>'s control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

The <COMPANY> software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

<COMPANY> has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to

perform their function) and controlled by the role of the staff member as well as a role based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems are revoked within three business days.

Administrator access to the production console is restricted to authorized system and security administrators. Powerful service/system accounts and keys are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution. Production infrastructure root level account usage is logged with alerting configured.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assesses the appropriateness of the access and permission levels and make modifications based on the principle of least-privilege, whenever necessary.

Staff members must use complex passwords, wherever possible, for all of their accounts that have access to <COMPANY> customer data. Staff are encouraged to use passwords which have at least 12 characters, randomly generated, alphanumeric and special-character based. Password configuration settings are documented and systematically enforced based on the password complexity requirements configured on each critical system. Access to cloud services or remote access systems requires multi-factor authentication (MFA). Additionally, company owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Physical Access and Environmental Controls

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls of the in-scope system. <COMPANY> reviews the SOC 2 report provided by AWS on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the <COMPANY> software application.

Incident Management

<COMPANY> has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact <COMPANY> via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event

there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the
self-healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of <COMPANY> being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium severity incidents usually cover the large majority of incidents found.
- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.
- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Network Operations Monitoring

Web applications are protected by deploying network firewalls and security groups that inspect traffic flowing to the web application for common attacks. The network is segmented based on the label or classification level of the information stored on the servers. This includes filtering between virtual private cloud (VPC) environments to help ensure only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities. Operations and security functions use a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs.

Incidents and alerts from the security utilities are reviewed by <COMPANY> management. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

<COMPANY> only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

Cryptography

User requests to <COMPANY>'s systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to <COMPANY> web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256 bit.

Change Management

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the <COMPANY> are reviewed, deployed, and managed. The policy covers all changes made to the <COMPANY> software application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information

- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

The ability to implement changes into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Further AWS CloudTrail is configured to track all changes to the production infrastructure.

Customer content and personal information are not used in non-production environments.

Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including for size, data type, and acceptable ranges or formats. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. <COMPANY> uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include encryption on devices for data at rest.

To help prevent malware, the following are implemented within the organization:

- Email attachments entering the organization's email gateway are scanned for viruses; and,
- Anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

Availability

<COMPANY> has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Information and Communication

<COMPANY> maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, <COMPANY> also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Information about the system and services are maintained and made available to users on the company website.

Monitoring Controls

<COMPANY>'s management monitors controls to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Disclosure of Incidents

There were no system incidents as of May 10th 2022 to September 10th 2022, requiring disclosure that either:

Were the result of controls failing; or,

Resulted in a significant impairment to the achievement of system requirements or service commitments to customers.

Complementary User Entity Controls

<COMPANY>'s controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for <COMPANY> customers.

For customers to rely on the information processed through the <COMPANY>'s software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for managing their organization's <COMPANY>'s software application account as well as establishing any customized security solutions or automated processes through the use of setup features
- User entity is responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to the <COMPANY>'s software application periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the <COMPANY>'s software application.
- User entity is responsible for removing terminated employee access to the <COMPANY>'s software application.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the <COMPANY>'s software application.
- User entity is responsible for sending data to <COMPANY>'s software application via a secure connection and/or the data should be encrypted.
- User entity is responsible for notifying <COMPANY>'s software application if they detect or suspect a security incident related to the <COMPANY>.
- User entity is responsible for reviewing email and other forms of communications from <COMPANY>, related to changes that may affect <COMPANY> customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
- User entity is responsible for endpoint protection of workstations used to access the system.
- User entity is responsible for developing their own business continuity and disaster recovery plan

Complementary Subservice Organization Controls

<COMPANY> uses subservice organizations in support of its system. <COMPANY>'s controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the <COMPANY>to be achieved solely by <Software Name>. Therefore, user entity controls must be evaluated in conjunction with <COMPANY>'s controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

<COMPANY> periodically reviews the quality of the outsourced operations by various methods including:

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	AWS	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access to the data center facility is restricted to authorized personnel.	AWS	CC6.4, CC6.5
Environmental protection, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	AWS	CC6.4, A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	AWS	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	AWS	A1.2

A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company’s commitments related to confidentiality.	AWS	C1.1
A defined process is in place to sanitize and destroy hard drives and back up media containing customer data prior to leaving company facilities.	AWS	C1.2

THANK YOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://www.youtube.com/@SECURECYBERGATES
https://securecybergates.com/services
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com