# Gabriel Software LLC
# Type 1 SOC 2
# 2018

# REPORT ON GABRIEL SOFTWARE LLC'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

## Pursuant to Reporting on Service Organization Controls 2 (SOC 2)<br>Type 1 examination performed under AT-C 105 and AT-C 205

**July 31, 2018**

# Table of Contents

# SECTION 1

# INDEPENDENT SERVICE AUDITOR’S REPORT

# INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT GABRIEL SOFTWARE LLC RELEVANT TO SECURITY AND AVAILABILITY

To Gabriel Software LLC:

We have examined the attached description titled "Description of Gabriel Software LLC's SaaS Services System as of July 31, 2018" (the description) and the suitability of the design of controls to meet the criteria for the Security and Availability principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), as of July 31, 2018. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Gabriel Software LLC's ('Gabriel Software' or 'the Company') controls are suitably designed, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Gabriel Software uses Microsoft Corporation ("subservice organization") for cloud hosting services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed. The description presents Gabriel Software's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, and suitably designed at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

Gabriel Software has provided the attached assertion titled "Management of Gabriel Software LLC's Assertion Regarding Its SaaS Services System as of July 31, 2018," which is based on the criteria identified in management's assertion. Gabriel Software is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Gabriel Software's assertion and on the suitability of the design of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed to meet the applicable trust services criteria as of July 31, 2018.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. Because of their nature and inherent limitations, controls at a service organization may not prevent, or detect and correct, all errors or omissions to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the description criteria identified in Gabriel Software's assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented as of July 31, 2018, and
b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively as of July 31, 2018, and user entities applied the complementary user-entity controls contemplated in the design of Gabriel Software's controls as of July 31, 2018 and the subservice organization applied, as of July 31, 2018, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system.

This report is intended solely for the information and use of Gabriel Software; user entities of Gabriel Software's SaaS Services System as of July 31, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, or other parties.
- Internal control and its limitations.
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN ASSURANCE

August 10, 2018
Tampa, Florida

# SECTION 2

# MANAGEMENT OF GABRIEL SOFTWARE LLC’S ASSERTION REGARDING ITS SYSTEM AS OF JULY 31, 2018

**Management of Gabriel Software LLC’s Assertion Regarding Its System as of July 31, 2018**

August 10, 2018

We have prepared the attached description titled "Description of Gabriel Software LLC’s SaaS Services System as of July 31, 2018" (the description), based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization’s system in paragraphs 1.34-.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the SaaS Services System, particularly system controls intended to meet the criteria for the Security and Availability principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. the description fairly presents the SaaS Services System as of July 31, 2018, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided.

(2) The components of the system used to provide the services, which are the following:

- *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- *Software*. The application programs and IT systems software that supports application programs (operating systems, middleware, and utilities).
- *People*. The personnel involved in governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- *Processes*. The automated and manual procedures.
- *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

(3) The boundaries or aspects of the system covered by the description.

(4) How the system captures and addresses significant events and conditions.

(5) The process used to prepare and deliver reports and other information to user entities or other parties.

(6) If information is provided to, or received from other parties, how such information is provided or received; the role of the other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization’s system.

(8) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons therefore.

(9) Other aspects of the service organization’s control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(10) Relevant details of changes to the service organization’s system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization’s system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.

Armand Brunelle
CEO
Gabriel Software LLC

# SECTION 3

# DESCRIPTION OF GABRIEL SOFTWARE LLC'S SYSTEM AS OF JULY 31, 2018

# OVERVIEW OF OPERATIONS

## Company Background

Gabriel Software was founded in 2016 as a cloud-based Church Management Software company that delivers functionality for Parishes and Diocese around the World. Gabriel enables their clients to communicate with their Parishioners and members; leveraging current communication methods including e-mail and texting.

Gabriel's mission is simple - serve the Church. The company accomplishes this mission each day by providing clients with cloud-based software to help clients engage their parishioners.

Gabriel trademarked the term Parishioner Relationship Management® to define the vision of how the Church can engage parishioners and how the company's software can support activities.

## Description of Services Provided

Gabriel provides cloud-based diocese and parish management software. Features include:

**Membership Management -** complete census features to track

- Families and individuals
- Committees
- Occupation/workplace
- Sacraments
- Self-service membership portal

**Religious Education -** manage a parish religious education program

- Grade/levels
- Classroom lists and attendance
- Online registration and payment
- Auto promotion and sacrament creation

**Fundraising -** track all aspects of offertory and fundraising including

- Contribution tracking by fund
- Pledge tracking by fund
- Capital campaign management
- Reporting and analytic tools
- Online contribution platform

**Ministry Scheduling -** Liturgical ministry scheduling

- Service week scheduling
- Family scheduling
- Members manage own schedules on membership portal

**Reporting and Analysis**

- Statistical data capture
- Attendance at mass/services
- Can be used for analysis in conjunction with fundraising data
- Sacramental register
- Official Catholic directory

**Utilities -** these utilities are available across all functions

- E-mail
- Mail merge and mailing labels
- Lists and real-time reporting
- Multi-parish administration
- Diocese Module

*Infrastructure*

Primary infrastructure used to provide Gabriel Software's SaaS Services system includes the following:

| **Primary Infrastructure** | |
|---|---|
| **Hardware** | **Purpose** |
| Microsoft Azure Cloud Service | Application hosting |

*Software*

Primary software used to provide Gabriel Software's SaaS Services system includes the following:

| **Primary Software** | |
|---|---|
| **Software** | **Purpose** |
| Microsoft Azure SQL Server | Database Management System |
| VisualStudio.com | Change Management and software version control |
| Office365 | Productivity Software |

*People*

The Gabriel Software staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Development team - responsible for delivering a responsive system that fully complies with the functional specification
- Quality assurance team - verifies that the system complies with the functional specification through functional testing procedures
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

*Processes*

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Gabriel Software policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Gabriel Software team member.

*Physical Security*

Gabriel application is hosted in the Microsoft Azure cloud. The data center located in the office facility controls only the Local Area Network to facilitate internet connectivity and printing within the office.

*Logical Access*

Gabriel Software uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In situations in which incompatible responsibilities cannot be segregated, Gabriel Software implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the Gabriel Software network using an Office 365 Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customer employees access the Gabriel Parish Management system through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Gabriel Software's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Upon hire, employees are assigned to a position. Two days prior to the employees' start date, employee user IDs are identified along with their role based access requirements and are provided to the System Administrator for creation in the Office 365 active directory.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO. As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

The System Administrator is notified of employees that are terminated and will initiate the suspension of their user IDs and delete all access roles from IDs belonging to them.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by the System Administrator and distributed to the managers via an e-mail. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the system administrator for processing.

### *Computer Operations - Backups*

Gabriel utilizes Microsoft SQL Azure database replication. Databases are replicated between two Microsoft datacenters every 15 minutes. The company's Disaster Recovery Plan outlines the procedure for activating the replicated database in the event of a datacenter disaster.

### *Computer Operations - Availability*

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Gabriel Software monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Gabriel Software evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space
- Disk storage
- Network bandwidth

Gabriel Software has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Gabriel Software system owners review proposed operating system patches to determine whether the patches are applied. Customers and Gabriel Software systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Gabriel Software staff validate that all patches have been installed and if applicable that reboots have been completed.

### *Change Control*

Gabriel Software maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Gabriel Software has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Gabriel Software system owners review proposed operating system patches to determine whether the patches are applied. Customers and Gabriel Software systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Gabriel Software staff validate that all patches have been installed and if applicable that reboots have been completed.

*Data Communications*

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted by A-LIGN to measure the security posture of a target system or environment. A-LIGN uses an accepted industry standard penetration testing methodology. A-LIGN approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, A-LIGN attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by A-LIGN as well on a quarterly basis in accordance with Gabriel Software policy. A-LIGN uses industry standard scanning technologies and a formal methodology specified by Gabriel Software. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Gabriel Software system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

*Data*

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. Customer data is captured which is utilized by Gabriel Software in delivering its SaaS services system. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems

**Boundaries of the System**

The scope of this report includes the SaaS services system performed in the Attleboro, Massachusetts facilities.

This report does not include the Cloud Hosting services provided by Microsoft at the US East facilities.

**Significant Events and Conditions**

Gabriel Software has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Gabriel system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

### Preparation and Delivery of Reports and Data

Gabriel Software utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

### Subservice Organizations

The Cloud Hosting services provided by Microsoft Azure are monitored by management; however, they have not been included in the scope of this review. The following criteria and controls are expected to be implemented by Microsoft Azure.

| Subservice Organization Controls | | |
|---|---|---|
| **Principle** | **Criteria** | **Applicable Controls** |
| Security | 5.5 | Physical access to the facilities housing the production systems is restricted to authorized personnel |
| Security | 5.5 | Logical and physical access to production infrastructure is restricted to authorized personnel |
| Security / Availability | 5.5 / 1.2 | Systems and data are protected against unauthorized physical access and environmental threats |
| Availability | 1.2 | Security measures are in place to protect the environmental security of the facilities housing the production servers |

### Criteria Not Applicable to the System

All Common, and Availability criteria were applicable to the Gabriel Software SaaS services system.

### Significant Changes in the Last 12 Months

No significant changes have occurred to the services provided to user entities since the organization last review or in the 12 months preceding the end of the review period.

## 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 Gabriel Software's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Gabriel Software'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, as well as by example.

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual

- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

### Commitment to Competence

Gabriel Software's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

### Management's Philosophy and Operating Style

Gabriel Software's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

### Organizational Structure and Assignment of Authority and Responsibility

Gabriel Software's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes 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.

Gabriel Software's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It 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 communicated to employees and updated as needed.

### Human Resources Policies and Practices

Gabriel Software'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 its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Gabriel Software's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

## RISK ASSESSMENT

Gabriel Software’s risk assessment process identifies and manages risks that could potentially affect Gabriel Software’s ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Gabriel Software 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 has identified risks resulting from the nature of the services provided by Gabriel Software, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Gabriel Software has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm’s internal controls. The approach is intended to align the entity’s strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Gabriel Software attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

## TRUST SERVICES PRINCIPLES AND CRITERIA

### In-Scope Trust Services Principles

| Common Criteria (to all Security and Availability Principles) |
|---|
| The security principle refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information. |

| Availability |
|---|
| The availability principle refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance. |

### Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Gabriel Software's SaaS Services system; as well as the nature of the components of the system result in risks that the criteria will not be met. Gabriel Software addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Gabriel Software's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

## Control Activities Specified by the Service Organization

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC1.0** | **Common Criteria Related to Organization and Management** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC1.1 | The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability. | A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.<br>Reporting relationships and organizational structures are reviewed annually by management.<br>Roles and responsibilities are defined in written job descriptions and communicated to personnel.<br>Management reviews job descriptions annually and makes updates, if necessary. |
| CC1.2 | Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability. | A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel.<br>Roles and responsibilities are defined in written job descriptions and communicated to personnel.<br>Management reviews job descriptions annually and makes updates, if necessary. |
| CC1.3 | The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities. | Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.<br>The experience and training of candidates for employment of transfer are evaluated before they assess the responsibilities of their position.<br>Employee evaluations are performed for employees on an annual basis.<br>Employees are required to complete information security training upon hire as a part of training compliance.<br>Employees are required to complete information security training on an annual basis and is tracked and monitored as a part of training compliance. |
| CC1.4 | The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability. | An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.<br>Personnel are required to sign and accept the employee handbook and code of conduct upon hire. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| CC1.0 | Common Criteria Related to Organization and Management | |
| Control Point | Criteria | Control Activity Specified by the Service Organization |
| | | Personnel are required to complete a background check provided by a third-party vendor upon hire. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC2.0** | **Common Criteria Related to Communications** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC2.1 | Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation. | System descriptions are communicated to authorized external users via service level agreement (SLA) that delineate the boundaries of the system and describe relevant system components.<br>A description of the system delineating the boundaries of the system is posted on a secure network drive and is available to personnel.<br>A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.<br>Reporting relationships and organizational structures are reviewed annually by management.<br>Roles and responsibilities are defined in written job descriptions and communicated to personnel.<br>Customer responsibilities are outlined and communicated through the service level agreement. |
| CC2.2 | The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities. | Security and availability commitments are communicated to external users via defined SLA.<br>A description of the system delineating the boundaries of the system is posted on a secure network drive and is available to personnel.<br>Employees are required to complete information security training upon hire as a part of training compliance.<br>Employees are required to complete information security training on an annual basis and is tracked and monitored as a part of training compliance.<br>Personnel are required to sign and accept the employee handbook and code of conduct upon hire. |
| CC2.3 | The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties. | A description of the system delineating the boundaries of the system is posted on a secure network drive and is available to personnel.<br>Roles and responsibilities are defined in written job descriptions and communicated to personnel.<br>Management reviews job descriptions annually and makes updates, if necessary.<br>Personnel are required to attend annual security training. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC2.0** | **Common Criteria Related to Communications** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| | | Customer responsibilities are outlined and communicated through the service level agreement. |
| CC2.4 | Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities. | Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.<br>Employees are required to complete information security training upon hire as a part of training compliance.<br>Employees are required to complete information security training on an annual basis and is tracked and monitored as a part of training compliance. |
| CC2.5 | Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel. | Employees are required to complete information security training upon hire as a part of training compliance.<br>Employees are required to complete information security training on an annual basis and is tracked and monitored as a part of training compliance.<br>Documented incident response and information security policies and procedures are in place to guide personnel in the event of an incident.<br>Defined SLAs are in place and communicated to authorized external users. The SLAs include communication procedures for reporting security and availability related failure, incidents, and concerns to personnel. |
| CC2.6 | System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner. | Application changes are authorized, tested, and approved by management prior to implementation.<br>Infrastructure changes are authorized and approved by management prior to implementation.<br>Changes are communicated to internal users via automatic updates from the version control software.<br>Upcoming changes are communicated to external users via weekly release notes. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC3.0** | **Common Criteria Related to Risk Management and Design and Implementation of Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC3.1 | The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes. | A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.<br>Documented policies and procedures are in place to guide personnel when performing the risk assessment process.<br>A formal risk assessment is performed on an annual basis to identify threats that could impair systems security and availability commitments and requirements.<br>Identified risks are rated using a risk evaluation process and rating are reviewed by management.<br>Management develops risk mitigation strategies to address risks identified during the risk assessment process. |
| CC3.2 | The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary. | Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.<br>Business continuity and disaster recovery plans are developed and updated on an annual basis.<br>Business continuity and disaster recovery plans are tested on an annual basis. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC4.0** | **Common Criteria Related to Monitoring Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC4.1 | The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner. | Logical access reviews are performed on a semi-annual basis.<br>Backup restoration tests are performed on a semi-annual basis.<br>Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.<br>The monitoring software is configured to alert administrators when thresholds have been exceeded. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC5.0** | **Common Criteria Related to Logical and Physical Access Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC5.1 | Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability. | Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.<br>Logical and physical access to systems is granted to an employee as a component of the hiring process.<br>Logical and physical access to systems is revoked as a component of the termination process.<br>Logical access reviews are performed on a semi-annual basis.<br>An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.<br>The IDS is configured to notify personnel upon intrusion detection. |
| | **Connectivity Console - Azure** | |
| | | Connectivity console user access is restricted via role based security privileges defined within the access control system.<br>Connectivity console administrative access is restricted to user accounts accessible by the following personnel:<br>• CEO<br>• CTO<br>• Product Development<br>Connectivity console users are authenticated via individually-assigned user accounts and passwords. The connectivity console is configured to enforce password requirements that include:<br>• Password history<br>• Maximum password age<br>• Minimum password length<br>• Complexity<br>The connectivity console is configured to log user login events and user activity. |
| | **Network - Office 365** | |
| | | Network user access is restricted via role based security privileges defined within the access control system. |

| **COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES** | | |
|---|---|---|
| **CC5.0** | **Common Criteria Related to Logical and Physical Access Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| | | Network administrative access is restricted to user accounts accessible by the following authorized personnel:<br>• CEO<br>• CTO<br>• Product Development<br>• Marketing<br>Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include:<br>• Password age (minimum & maximum)<br>• Password length<br>• Complexity<br>The network is configured to log user login events and user activity. |
| | **Database** | |
| | | Database user access is restricted via role based security privileges defined within the access control system.<br>Database administrative access is restricted to user accounts accessible by the following personnel:<br>• CEO<br>• CTO<br>• Product Development<br>Database users are authenticated via individually-assigned user accounts and passwords. Databases are configured to enforce password requirements that include:<br>• Password history<br>• Maximum password age<br>• Minimum password length<br>• Complexity<br>The database is configured to log user login events and user activity. |
| | **Application - GabrielSoft** | |
| | | Application user access is restricted via role based security privileges defined within the access control system. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC5.0** | **Common Criteria Related to Logical and Physical Access Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| | | Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include:<br>• Minimum Length<br>• Special character<br>• Uppercase character<br>• Lowercase character<br>Application account lockout policies are in place that include:<br>• Account lockout duration<br>• Account lockout threshold<br>• Account lockout counter reset<br>The application is configured to log user login events and user activity.<br>Privileged access to sensitive resources is restricted to defined user roles. |
| CC5.2 | New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.<br>Logical and physical access to systems is granted to an employee as a component of the hiring process.<br>Logical and physical access to systems is revoked as a component of the termination process.<br>Logical access reviews are performed on a semi-annual basis.<br>Account sharing is prohibited unless a variance from policy is granted by the chief technology officer. |
| CC5.3 | Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability. | Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.<br>Logical and physical access to systems is granted to an employee as a component of the hiring process.<br>Logical and physical access to systems is revoked as a component of the termination process.<br>Logical access reviews are performed on a semi-annual basis. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC5.0** | **Common Criteria Related to Logical and Physical Access Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| | | An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.<br>The IDS is configured to notify personnel upon intrusion detection. |
| | **Connectivity Console - Azure** | |
| | | Connectivity console user access is restricted via role based security privileges defined within the access control system.<br>Connectivity console administrative access is restricted to user accounts accessible by the following personnel:<br>• CEO<br>• CTO<br>• Product Development<br>Connectivity console users are authenticated via individually-assigned user accounts and passwords. The connectivity console is configured to enforce password requirements that include:<br>• Password history<br>• Maximum password age<br>• Minimum password length<br>• Complexity<br>The connectivity console is configured to log user login events and user activity. |
| | **Network - Office 365** | |
| | | Network user access is restricted via role based security privileges defined within the access control system.<br>Network administrative access is restricted to user accounts accessible by the following authorized personnel:<br>• CEO<br>• CTO<br>• Product Development<br>• Marketing<br>Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include:<br>• Password age (minimum & maximum)<br>• Password length<br>• Complexity |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC5.0** | **Common Criteria Related to Logical and Physical Access Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| | | The network is configured to log user login events and user activity. |
| | **Database** | |
| | | Database user access is restricted via role based security privileges defined within the access control system.<br>Database administrative access is restricted to user accounts accessible by the following personnel:<br>• CEO<br>• CTO<br>• Product Development<br>Database users are authenticated via individually-assigned user accounts and passwords. Databases are configured to enforce password requirements that include:<br>• Password history<br>• Maximum password age<br>• Minimum password length<br>• Complexity<br>The database is configured to log user login events and user activity. |
| | **Application - GabrielSoft** | |
| | | Application user access is restricted via role based security privileges defined within the access control system.<br>Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include:<br>• Minimum Length<br>• Special character<br>• Uppercase character<br>• Lowercase character<br>Application account lockout policies are in place that include:<br>• Account lockout duration<br>• Account lockout threshold<br>• Account lockout counter reset<br>The application is configured to log user login events and user activity.<br>Users can only access the system remotely through the use of secure sockets layer (SSL), or other encrypted communication system. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC5.0** | **Common Criteria Related to Logical and Physical Access Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC5.4 | Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability. | Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.<br>Logical and physical access to systems is granted to an employee as a component of the hiring process.<br>Logical and physical access to systems is revoked as a component of the termination process.<br>Logical access reviews are performed on a semi-annual basis. |
| CC5.5 | Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability. | Physical security policies are in place to define the required safeguards to protect the facility containing sensitive information system assets.<br>Refer to the Subservice Organizations section above for additional controls. |
| CC5.6 | Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements. | A firewall is in place to filter unauthorized inbound network traffic from the internet.<br>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.<br>Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.<br>An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.<br>The IDS is configured to notify personnel upon intrusion detection. |
| CC5.7 | The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability. | SSL and other encryption technologies are used for defined points of connectivity.<br>Backup media is stored in an encrypted format.<br>The ability to recall backed up data is restricted to authorized personnel. |
| CC5.8 | Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability. | The ability to migrate changes into the production environment is restricted to authorized and appropriate users. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC5.0** | **Common Criteria Related to Logical and Physical Access Controls** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| | | An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.<br>The IDS is configured to notify personnel upon intrusion detection.<br>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the anti-virus software.<br>The antivirus software is configured to scan workstations on a real-time basis.<br>The antivirus software provider pushes updates to the installed anti-virus software as new updates/signatures are available. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC6.0** | **Common Criteria Related to System Operations** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC6.1 | Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability. | Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.<br>The monitoring software is configured to alert administrators when thresholds have been exceeded.<br>Documented incident response policies and procedures are in place to guide personnel in the event of an incident.<br>Data backup and restore procedures are in place to guide personnel in performing backup activities.<br>An automated backup system is utilized to perform scheduled system backups.<br>Full backups of certain application and database components are performed on a daily basis.<br>IT personnel monitor the success or failure of backups on a weekly basis.<br>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the anti-virus software.<br>The antivirus software is configured to scan workstations on a real-time basis.<br>The antivirus software provider pushes updates to the installed anti-virus software as new updates/signatures are available.<br>A firewall is in place to filter unauthorized inbound network traffic from the internet.<br>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.<br>An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.<br>The IDS is configured to notify personnel upon intrusion detection. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC6.0** | **Common Criteria Related to System Operations** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC6.2 | Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements. | Documented incident response policies and procedures are in place to guide personnel in the event of an incident.<br>A ticket tracking application is utilized to track and respond to incidents.<br>Resolution of events is communicated to users within the corresponding ticket.<br>Change management requests are opened for events that require permanent fixes.<br>Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| **CC7.0** | **Common Criteria Related to Change Management** | |
| **Control Point** | **Criteria** | **Control Activity Specified by the Service Organization** |
| CC7.1 | The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components. | Documented change control policies and procedures are in place to guide personnel in the handling system changes.<br>System changes are authorized, tested, and approved by management prior to implementation. |
| CC7.2 | Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability. | Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.<br>A formal risk assessment is performed on an annual basis to identify threats that could impair systems security and availability commitments and requirements.<br>Identified risks are rated using a risk evaluation process and rating are reviewed by management.<br>Management develops risk mitigation strategies to address risks identified during the risk assessment process. |
| CC7.3 | Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability. | Documented escalation procedures for reporting security incidents are in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints.<br>Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. |
| CC7.4 | Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements. | Documented change control policies and procedures are in place to guide personnel in the handling system changes.<br>System change requests are documented and tracked in a ticketing system.<br>System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.<br>Changes are approved by management prior to implementation.<br>Changes are communicated to internal users via automatic updates from the version control software.<br>Upcoming changes are communicated to external users via weekly release notes. |

| COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES | | |
|---|---|---|
| CC7.0 | Common Criteria Related to Change Management | |
| Control Point | Criteria | Control Activity Specified by the Service Organization |
| | | Development and test environments are physically and logically separated from the production environment.<br>Access to implement changes in the production environment is restricted to authorized IT personnel.<br>File integrity monitoring software is utilized to help detect unauthorized changes within the production environment.<br>Prior code is held in the repository for rollback capability in the event that a system change does not function as designed.<br>The change management process has defined the following roles and assignments:<br>• Authorization of change requests - Change Approval Board<br>• Development - Development Team<br>• Testing - QA Team<br>• Implementation - Production Implementation Team |

| A1.0 | ADDITIONAL CRITERIA FOR AVAILABILITY | |
|---|---|---|
| Control Point | Criteria | Control Activity Specified by the Service Organization |
| A1.1 | Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements. | Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.<br>The monitoring software is configured to alert administrators when thresholds have been exceeded.<br>Future processing demand is forecasted and compared to scheduled capacity on an annual basis. Forecasts are reviewed and approved by management. |
| A1.2 | Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements. | Full backups of certain application and database components are performed on a daily basis.<br>IT personnel monitor the success or failure of backups on a weekly basis.<br>Restore tests are performed on backed up data on a semi-annual basis.<br>Backup media is stored in an encrypted format.<br>The ability to recall backed up data is restricted to authorized personnel.<br>Business continuity and disaster recovery plans are developed and updated on an annual basis.<br>Business continuity and disaster recovery plans are tested on an annual basis.<br>Refer to the Subservice Organizations section above for additional controls. |
| A1.3 | Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements. | Business continuity and disaster recovery plans are developed and updated on an annual basis.<br>Business continuity and disaster recovery plans are tested on an annual basis. |

## MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Gabriel Software’s management performs monitoring activities 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. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

### On-Going Monitoring

Gabriel Software’s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management’s close involvement in Gabriel Software’s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control’s weakness is made based on whether the incident was isolated or requires a change in the company’s procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Gabriel Software’s personnel.

### Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

## INFORMATION AND COMMUNICATION SYSTEMS

Information and communication is an integral component of Gabriel Software’s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity’s operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Gabriel Software, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, town hall meetings are held bi-annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Gabriel Software personnel via e-mail messages.

Specific information systems used to support Gabriel Software’s SaaS Services system are described in the Description of Services section above.

## COMPLEMENTARY USER ENTITY CONTROLS

Gabriel Software's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Principles related to Gabriel Software's services to be solely achieved by Gabriel Software control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Gabriel Software.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Gabriel Software.
2. User entities are responsible for notifying Gabriel Software of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Gabriel Software services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Gabriel Software services.
6. User entities are responsible for providing Gabriel Software with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Gabriel Software of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

# SECTION 4

# INFORMATION PROVIDED BY THE SERVICE AUDITOR

## GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE’s examination of the controls of Gabriel Software was limited to the Trust Services Principles and related criteria and control activities specified by the management of Gabriel Software and did not encompass all aspects of Gabriel Software’s operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities were performed using the following testing methods:

| **TEST** | **DESCRIPTION** |
|---|---|
| Inquiry | The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client’s knowledge of the control and corroborate policy or procedure information. |
| Observation | The service auditor observed application of the control activities by client personnel. |
| Inspection | The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities. |
| Re-performance | The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity’s internal control. |

In determining whether the report meets the user auditor’s objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization’s controls that may affect the processing of the user entity’s transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user entity’s financial statement assertions; and
- Determine whether the service organization’s controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user entity’s financial statements and determine whether they have been implemented.