SECTION 3 – Description of the System

Overview of Operations

**Company Background**

*[company’s name]* provides *[type of services]*.  *[company’s name]* operates in *[Country and State]* and employs approximately *[#]* employees.

**Overview of Products and Services**

The *[product’s name*] is designed to *[product’s function].  [Company’s name]* currently offers the below application and features which are covered by this report:

* [Application / feature name and description]
* [Application / feature name and description]
* [Application / feature name and description]

**Principle Service Commitments and System Requirements**

*[Company’s name*] designs its processes and procedures related to the *[product name]* to meet its objectives for its *[product name]* services.  Those objectives are based on the service commitments that *[Company’s name]* makes to user entities, the laws and regulations that govern the provision of the *[product name]* services, and the financial, operational, and compliance requirements that *[Company’s name]* has established for the services.  The *[product name]* services of *[Company’s name]* are subject to the relevant regulatory and industry information and data security requirements in which *[Company’s name]* operates. The principal *security, availability, and confidentiality* commitments are standardized, and include, but are not limited to, the following:

Security: *[Describe Security commitments]*

Availability: *[Describe Security commitments] (if in scope)*

Confidentiality: *[Describe Security commitments] (if in scope)*

Processing Integrity: *[Describe Security commitments] (if in scope)*

Privacy: *[Describe Security commitments] (if in scope)*

*[Company’s name]* establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements.

Such requirements are communicated in *[Company’s name]’s system policies and procedures, and contracts with customers]*.  Information security policies define an organization-wide approach to how systems and data are protected.  These policies include ones 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, trained, and managed.  In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the *[product name].*

**Components of the System**

*System Architecture*

*[INSERT IMAGE OF NETWORK DIAGRAM]*

*Infrastructure*

The production information systems are hosted on *[cloud service provider].  [cloud service provider]* is responsible for the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer and storage) and *[company’s name]* is responsible for securing the application platform deployed in *[cloud service provider]* (i.e. customer data, applications, identity access management, operating system and network virtual firewall configuration, network traffic, server-side encryption). Production servers and client-facing applications are logically and physically secured from *[company’s name]*’s internal corporate information systems.

*Software*

*[company’s name]* has selected several vendors to provide important aspects of the application hosting framework used to support a robust cloud infrastructure for *[company’s name]* applications.

These providers are organized to provide the platform necessary to securely and reliably provide access to users, manageability by system administrators, and seamless upgradeability.  The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

|  |  |
| --- | --- |
| **Software** | |
| **Production Application** | **Business Function Description** |
| *[system]* | *[system purpose]* |
| *[system]* | *[system purpose]* |
| *[system]* | *[system purpose]* |

*People*

*[company’s name]* staff organized into the following functional areas:

* Corporate executive management– responsible for *[overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives]*
* Operations - responsible for *developing and supporting the [company]’s services.*
* IT services - responsible for *[managing, monitoring and supporting user entities' information and systems from unauthorized access and use while maintaining integrity and availability]*
* Product Department - responsible for *[tbd]*
* HR Department - responsible for *[tbd]*
* IT Help Desk Department - responsible fo*r [tbd]*
* *others*

*Data*

Data, as defined by  *[company’s name]* constitutes the following:

* *[list data, i.e - input artifacts, transaction reports, PII, etc..]*
* *[list data]*

**Customer Responsibilities**

*[Describe your customer’s responsibilities] An example:*

*Administrator-level user access privileges granted to customers and to their respective environment(s) are initially provided via e-mail using uniquely generated passwords that follow the Example Cloud Service Organization standard for secure passwords (at least 8 characters, lower and uppercase letters, one number, and one symbol).*

*The password is paired with the customer’s account information to establish accountability for user actions in the Example Service Organization’s system. In addition, although recommended, at the customer’s discretion, the uniquely generated initial password associated with the customer’s user ID must be changed upon initial login.*

*Because Dedicated and Virtual customers have system administrator-level privileged access to most configurations and have the ability to perform logical security administration functions for their respective environments, any customer-initiated changes or modifications to servers, services (including anti-virus definitions), or logical access entitlements are exclusively the responsibility of these customers. Hypervisors are not used on dedicated servers unless enabled.*

*Example Cloud Service Organization requires that a customer’s ability to gain logical access be performed from behind a dedicated firewall and on a customized encrypted network session in order to implement a hypervisor.3 It is the customer’s responsibility to maintain hypervisors where installed and this process is excluded from the scope of this report. Since customers are assigned physical data center keys that provide them with physical access to the racks on which their dedicated servers reside, customer-initiated server maintenance activities performed by customers are excluded from the scope of this report.*

**Process and Procedures**

*Security Management*

*[company’s name*] has a dedicated Information Security team responsible for management of information security throughout the organization. The information security team is responsible for developing, maintaining and enforcing *[company’s name]* information security policies. The information security policy is reviewed annually.

Security Policies

The following security policies and related processes are in place for the *[product name]*.

* *Risk Management Policy*
* *Vendor Management Policy*
* *Asset Management Policy*
* *Access Control Policy*
* *Authentication and Password Policy*
* *Encryption Policy*
* *Data Classification Policy*
* *Audit Logging Policy*
* *Physical Security Policy*
* *Acceptable Use Policy*
* *Information Security Policy*
* *Human Resources Policy*
* *Data Retention and Disposal Policy*
* *Security Incident Management Policy*
* *Vulnerability Management Policy*
* *Change Management Policy*
* *Business Continuity Policy*
* *Backup Policy*
* *Internal Audit Policy*
* *Compliance Program Management Policy*

During the annual security training, management ensures communication of the latest security policies.

*Access Management*

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. A formal process has been established for managing user accounts and controlling access to *[company’s name]* resources. Administrative access privileges are assigned to only those users requiring access to fulfill their job responsibilities and are restricted to authorized personnel. To help ensure access privileges are appropriate, the Information Security team completes an audit of the production environment accounts on a *quarterly* basis.  Accounts identified as inappropriate are investigated and resolved.

Firewall systems are in place to protect the production network and are utilized to restrict access and filter unauthorized traffic. A next-generation antivirus solution is in place and installed on the company owned laptops and *[type of servers*] servers.  Encryption is also utilized on web servers for web communication sessions*.[company’s name]* stores data in an encrypted format where access to the cryptographic keys is restricted to authorized personnel.

*Data Backup and Disaster Recovery*

*[company’s name]* uses data replication and systems are backed up on a regular basis with established schedules and frequencies.  Backups are monitored and alerts are generated in the event of an unsuccessful execution.  Failure alerts are escalated, investigated and resolved. Asset disposal procedures are in place to guide personnel in disposing of technology equipment when they reach the end of their life.

Disaster recovery is performed in real time. *[company’s name]* performs data restore tests of the replicated data on a periodic basis to ensure that systems can be recovered in the event of a failure.

*Change Management*

*[company’s name*] has a formal change management in place to ensure that all changes to the product and system are introduced in a controlled and coordinated manner. The formal process requires identification and recording of significant changes in a ticketing system. Proposed changes are evaluated and the *Information Security team* meets regularly to review and approve changes to the production environment.

Changes are developed and tested in a separate development or test environment before implementation. A version control software is utilized to control changes and access to modify source code contained in the version control software is restricted to those with a business need.  Confidential information is not used during system design, development, testing, implementation, and change processes. Developers do not have access to the production environment without an authorized business need.

*[company’s name]* uses an automated deployment tool to control changes to production.

*Incident Response*

Security incidents and other IT-related problems are reported to the *technical operations* team. Incident response and escalation policies and procedures are in place to guide the helpdesk team in managing unexpected incidents impacting the business.  Management utilizes a ticketing system for tracking and resolving any identified incidents with customers.  *Engineering/technical operations team* complete incident postmortem reports upon system outages that include the incident and impact analysis, resolutions, lessons learned, and action items.  Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process.

*System Monitoring*

The *engineering/technical operations team* used a variety of monitoring systems to identify and detect possible security threats and incidents. These 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.  These alerts and notifications are reviewed by the engineering/technical operations team using a security incident and event monitoring tool.

*Vulnerability Assessments and Penetration Tests*

Vulnerability assessments of the *production network and the web application* are performed on a *periodic basis* to identify potential security vulnerabilities.  In addition, penetration testing is performed *annually* by a third-party vendor in order to find and address any security weaknesses.  Information security personnel retain the penetration testing reports, monitor the results of the assessment within the report, and work to create remediation plans to remedy any potential vulnerabilities, where applicable.

*Data Management*

The *[company’s name]* application platform is used to collect and process customer data and transfer information and content that is confidential and proprietary.  Customer data may include personally identifiable information (PII) of individuals subject to the privacy laws and regulations in jurisdictions in which the customers operate.

The following table describes the information used and supported by the system.

|  |  |
| --- | --- |
| **Data Used and Supported by the System** | |
| **Data Description** | **Classification** |
| Customer data is defined as data that *[company’s name]* customers would consider themselves owners of, and would regard as their own confidential data. Typically, this data has either been sent to *[company’s name]’s* for storing or processing, or has been created as a result of using *[company’s name]’*s products. | Customer Confidential |
| Company Restricted data is internal to the company, and it is used to operate its business. Very few people in *[company’s name]* have access to Company Restricted data. | Company Restricted |
| Company Confidential data is data internal to the *[company’s name]* that is used to operate the business. Many people in the company have access to this data. | Company Confidential |
| Public information may be disclosed to any entity or person within or outside of the company. The data may be available through a public website, and does not have confidentiality requirements. | Public |

SubserviceOrganizations

The *[type of services]* Platform services provided by *[service provider’s name]* were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at *[service provider’s name]*, alone or in combination with controls at *[company’s name],* and the types of controls expected to be implemented at *[service provider’s name],* to achieve *[company’s name]*, service commitments and system requirements based on the applicable trust services criteria.

|  |  |
| --- | --- |
| **Control Activity Expected to be Implemented by** *[service provider’s name],* | **Applicable Trust Services Criteria** |
| *[service provider’s name]* is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the *[company’s name]* applications reside. | CC6.1- CC6.3 CC6.5, CC6.6, CC7.2 |
| *[service provider’s name]* is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | CC6.4 - CC6.5  CC7.2 |
| *[service provider’s name]* is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where *[company’s name]* systems reside. | CC6.7 |
| *[service provider’s name]* is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the *[company’s name]* applications reside. | CC7.1 |

Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

***Security*** *- Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the information or systems and affect the entity's ability to meet its objectives.*

*The following categories are out of scope for the purposes of this report as they do not fit with [company’s name] business:*

***Availability*** *- Information and systems are available for operation and use to meet the entity’s objectives.*

***Confidentiality*** *- Information designated as confidential is protected to meet the entity’s objectives.*

***Processing Integrity*** *- System processing is complete, valid, accurate, timely, and authorized to meet the entity’s objectives.*

***Privacy*** *- Personal information is collected, used, retained, disclosed, and disposed of to meet the entity’s objectives.*

**Relevant Aspects of Internal Control**

This section provides information about the five interrelated components of internal control at *[company’s name]’.*

Control Environment

*[company’s name]*’s control environment reflects the philosophy of senior management concerning the importance of security of *[product’s name].* The components of the control environment factors include the integrity and ethical values, management’s commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by *executive management/the board of directors* and operations management.

*[company’s name]*’s board of directors meets quarterly to discuss and oversee the security activities of *[company’s name]*. The importance of security is emphasized within *[company’s name]* through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, *[company’s name]* has taken into consideration the relevance of controls to meet the relevant trust criteria.

Risk Assessment

*[company’s name]’*s regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria Key members of the *{i.e internal audit department, executive management and operational teams}* meet on *an annual basis* to identify and review risks to the system.  These risks are documented in a risk register.

Management considers risks that can arise from both external and internal factors including, but not limited to technological development, customer needs, competition, regulations, economic changes, fraud opportunities, changes in employees, changes in management, policies and processes.

Management assesses security risks on an ongoing basis. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessment and conducting a formal annual risk assessment. The risk assessment requires risk analysis which includes the identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed.

Along with assessing risks, management has identified and put into effect actions needed to address those risks.  In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently and that the identified risks are mitigated.

Management has documented policies and procedures that guide personnel.  These policies and procedures are communicated to personnel via *the intranet/internal document repository software/team collaboration software.*  Employees are held accountable for complying with these policies.  An acceptable use policy is in place that outlines the consequences for noncompliance.

Necessary actions are taken to reduce the significance or likelihood of the risk occurring and identify the control activities necessary to mitigate the risk.  The risk assessment and mitigation activities also addresses the risks arising from potential business disruptions.

Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.  Management has identified these control activities and documented them in the Control Objectives and Related Control Activities section below.

Vendor Management

Vendors and business partners are also considered during the risk assessment and mitigation activities.  To assist with this process, a vendor management policy is in place and vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data*. [company’s name]* signs non disclosure agreements */service level agreements* of confidentiality and protection with third-parties suppliers and business partners.  Monitoring procedures are in place to ensure continual compliance by vendors and business partners.

Information and Communication Systems

*Internal Communications*

*[company’s name]* has implemented various methods of internal communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated.  These methods include documented policies, training for employees, documented position descriptions*, weekly department meetings, a whistleblower hotline, and the use of e-mail messages to communicate time-sensitive information.*  Employees are encouraged to communicate to their *lead/mentor, supervisor/manager or Senior/Executive* Management.

*External Communications*

*[company’s name]* has also implemented various methods of communications to help ensure that customers *and vendors* understand the role and responsibilities of the Company and to help ensure that significant events are communicated in a timely manner.  External communication methods include website documentation regarding the design and operation of the system and its boundaries, master service agreements, nondisclosure agreements, system alerts or release notes, and escalation procedures.

Monitoring

**Monitoring Activities**

*Ongoing Monitoring*

A procedure has been established for periodic review by executive management of *[company’s name]* compliance systems.  Monitoring tools are used to continuously monitor security events, latency, network performance, and virtual server performance.

*Separate Evaluations*

Management has implemented Kintent, a compliance program to evaluate the performance of specific control activities and processes over time, and confirm that the in-scope controls were consistently applied as designed.

*Internal and External Auditing*

*[company’s name]* has successfully met the requirements of many certifications and regulatory demands, including:

* *Type 1 and Type 2 SOC 2 examinations*
* *Health Insurance Portability and Accountability Act (HIPAA)*

*Subservice Organization Monitoring*

The compliance team reviews *[service provider’s name]* attestation reports on an annual basis to help ensure the design and operating effectiveness of controls at the subservice organization are meeting agreed upon expectations

**Reporting Deficiencies**

Deviations or deficiencies associated with controls with a level High risk assignment are immediately escalated to management for immediate corrective action.  The internal control performance metrics and results of control assessments performed by external parties are provided to the *executive management/board of directors* for review.

*Changes to the System During the Period*

*There were no changes that are likely to affect report users’ understanding of how the System is used to provide the service during the period from January 1, 20XX through December 31, 20XX.*

*System Incidents During the Period*

*There were no identified system incidents that were the result of controls that were not suitably designed or operating effectively or otherwise resulted in a significant failure in the achievement of one or more of the service commitments and system requirements during the period January 1, 20XX to December 31, 20XX.*

Complementary Controls at User Entities

*[company’s name]*’s controls related to the *[product’s name]* system cover only a portion of overall internal control for each user entity. It is not feasible for the criteria related to the system to be achieved solely by *[company’s name]*. Therefore, each user entity’s internal controls should be evaluated in conjunction with Kintent‘s controls described in Section 4 of this report, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The user entity controls presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities are responsible for the following:

|  |  |
| --- | --- |
| **Criteria** | **Complementary User Entity Controls** |
| CC2.1 | *User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by [company’s name] systems and services.* |
| CC6.2 | *Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to [company’s name] application keys and API keys for access to the web service API.* |
| CC6.3 | *Authorized users and their associated access are reviewed periodically.* |
| CC6.6 | *User entities will ensure protective measures are in place for their data as it traverses from user entity to [company’s name].* |
| CC6.6 | *User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to [company’s name].* |