

Figure 1{{INSERT LOGO}}

Corporate Security Assurance Report

{{INSERT Company name}}

{{INSERT DATE}}

2020

*Important Notice from Tugboat Logic Inc.*

Intended audience for this document

**DISCLAIMER: This document is provided as a sample template for the benefit of authorized users of Tugboat Logic. Tugboat Logic makes no representations or warranties as to the commercial applicability or fitness for purpose of this document or its use by any authorized or unauthorized user. Tugboat Logic makes no representation regarding the accuracy or any content contained in this document, its use by an authorized user or any final work product that utilized this template. Reliance upon and use of this document is solely the risk of the publisher and recipient of this document. Please remember to delete this instructions page before sending to clients.**

This document serves as a template for you to proactively provide to your customers or sales prospects in order for them to get an overall understanding of your information security program. This document should be only provided under a non-disclosure agreement.

Purpose of this document

The purpose of this document is to provide enough detail about your company and product offering to enable a customer/sales prospect to:

1. Make an initial assessment of the level of overall technical and business risk in adopting your solution in their network environment
2. Provide enough detail on your product and company that would be normally addressed by a vendor security questionnaire
3. Gain enough confidence in your company and security posture that they are willing to move forward and purchase your solution

User guidance for this document

1. There are three types of content in this document to make it easier to use. Words in red font are instructions that you can delete later. Words in greyed out font are sample text you can delete later. Words in yellow highlight are custom fields for you to complete. An effort has been made to provide generic language wherever possible to reduce the amount of content you need to supply.
2. Provide enough detail in the products section and technical details section of this document to be clear on how your solution works, what forms of data you collect and process, and data flows in and out of your product or service.
3. Provide custom diagrams whenever possible for product and/or solution architecture details. Some diagrams are included in this template as examples of best practices; however, they should be customized to your specific solution.
4. Do not include any customer information in this document, unless you have explicit written consent to do so.
5. Do not provide any sensitive or proprietary information in this document that is covered by any patent filings or is confidentially held by the company on behalf of third parties.
6. Provide enough commercial details regarding your business that is relevant for a recipient to make a business risk assessment about your company or product.
7. Be truthful and complete in your completion of this document.
8. Keep a record of any security commitments made to the customer and ensure those commitments are delivered. You can use the **Tugboat Logic Virtual CISO Platform** as a convenient repository to store security documents that are sent to clients.

Table of Contents

1.0 Solution Overview 3

2.0 Product Overview 3

3.0 Solution Technical Information 5

4.0 Data Privacy and the Company Platform 8

5.0 Information Security Program Overview 11

6.0 Risk Mitigation, Compliance, Certification Readiness 13

7.0 Customer Support Service Level Agreement 14

8.0 Corporate Overview, Financials and Insurance 16

9.0 Exhibits 17

1.0 Solution Overview

*Instructions: Include brief value proposition statement on your company solution including what you provide, who it is for, how you are unlike other solutions, and how you are unique.*

{{Insert Company Name}} is the leader in {{insert what your product does}} for the {{insert who it is for/which market/buyer}}. Unlike traditional {{insert competitive products}}, only {{insert Company Name}} provides a {{insert unique capability that only you can claim}}.

Sample Text:

*Tugboat Logic is the virtual CISO platform for the enterprise. Unlike traditional GRC platforms designed for large enterprises, only Tugboat Logic provides an automated framework to demystify the process of setting up a security program. With Tugboat Logic, enterprises can quickly get secure and prove it to customers.*

2.0 Product Overview

2.1 Solution Architecture

*Instructions: Include brief description of your solution and how it is delivered. For example, is it an appliance or a SaaS application, what are the inputs and outputs of the system, etc.?*

The {{insert Solution Name}} is a {{insert platform deployment method (e.g. mobile app, SaaS app, on-premise appliance, software) }} that {{insert how it works here – inputs and outputs, APIs, integrations on-premise, etc.}}.

Sample Text:

*The Tugboat Logic Virtual CISO Platform is a SaaS solution that includes a web-based user interface for tracking all of your InfoSec program requirements. Customers have the ability to create their own InfoSec program from Tugboat’s predefined database of policies and controls, as well as upload and respond to security questionnaires automatically using Tugboat’s machine-learning-based Auto-Answer engine. Outputs include InfoSec Policy Document, completed security questionnaires and vendor security assessments.*

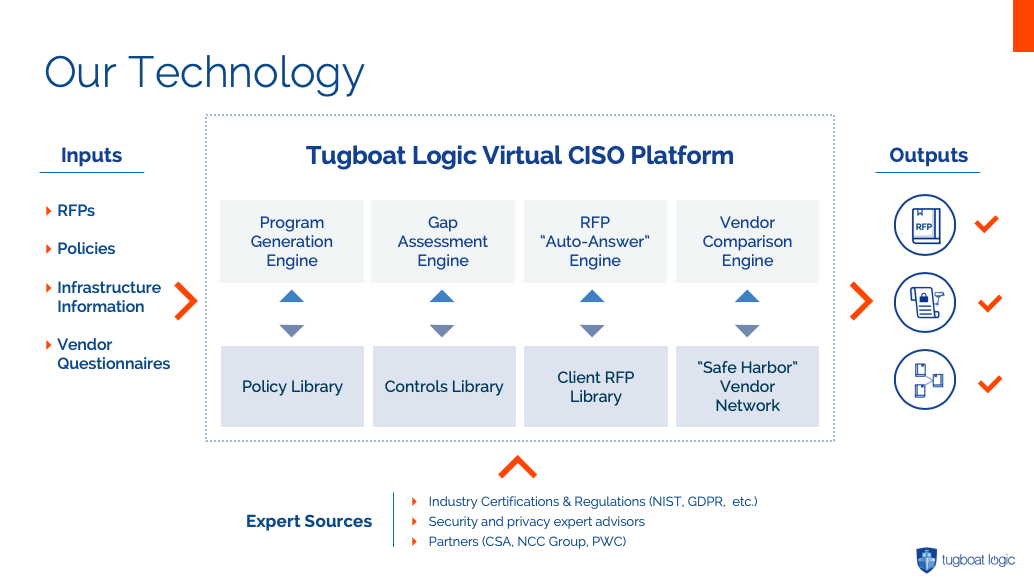


Figure 2 {{Insert {Company Solution Name}}

*Instructions: Create a Visio diagram of your solution architecture showing what data is input and output. Sample above for reference.*

2.1. Customer Data Collected by Product

*Instructions: Explain in this section what your product/solution requires in terms of customer data in order to function properly to explain at high level why you need it (e.g. “stores requirements around the InfoSec program of the customer, as well as imports third-party security questionnaires”). Then fill out table beneath on specific items you collect and how you secure it (e.g. encrypt it, anonymize it, both).*

The {{Company solution}} provides a system that {{insert what type of data your product needs in order to do its core function}}. Below are the types of data fields collected by the products that are categorized as either personally identifiable information or (PII) and personal data:

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Field** | **Category** | **Required by Product** | **Security Method** |
| Full name | PII | Yes | Anonymize |
| Home address | PII | No | N/A |
| Email address | PII | Yes | Encrypted |
| Social Security number | PII |  |  |
| Passport number | PII |  |  |
| Driver’s license number | PII |  |  |
| Credit card number | PII | Optional | Anonymize |
| Date of birth | PII |  |  |
| Telephone number | PII |  |  |
| Log in details | Personal Data |  |  |
| Device ID | Personal Data |  |  |
| IP Addresses | Personal Data |  |  |
| Cookies | Personal Data |  |  |

3.0 Solution Technical Information

**Instructions:**

3.1 Architecture Overview

*Instructions: Explain the technical overview of your product/solution, including delivery platform (mobile app, SaaS solution, on-premise appliance or software), and how client data is stored, moved and secured within this environment.*

*{{Insert Company Product Name}} is a {{Insert platform delivery method details}}. The {{Insert product name}} is built on a {{Insert application architecture type}} architecture. Client data locations and data flows are outlined in the diagram below along with the security measures in place to protect this data.*

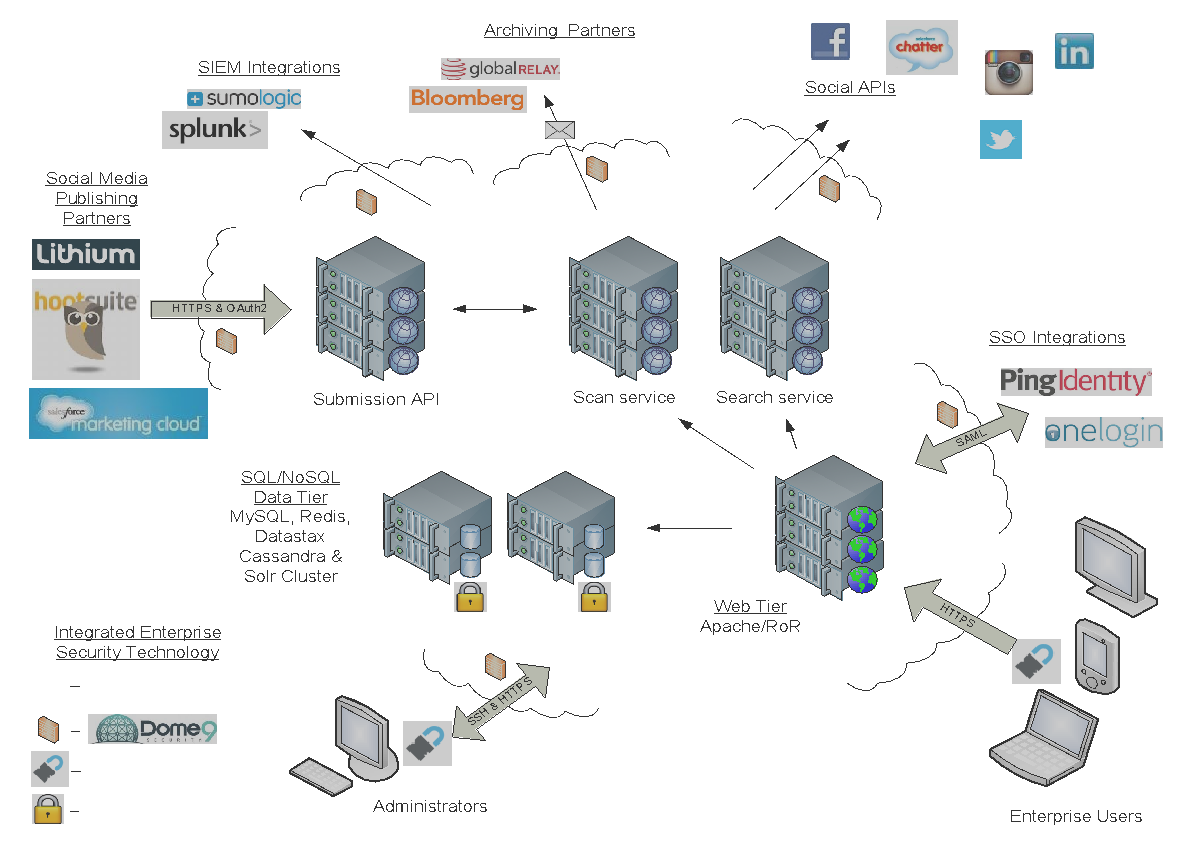
Sample Text:

*Tugboat Logic is a SaaS-based delivery platform hosted in Amazon Web Services. All customers receive their own tenant of the Tugboat Logic Virtual CISO Platform. The Tugboat Logic Virtual CISO platform is a multi-tenant client-server application where all customers receive their own instance. Tenants are logically separated to prevent unauthorized access to client data. Client data locations and data flows are outlined in the diagram below along with the security measures in place to protect this data.*

3.2 Technical Architecture Diagrams

*Instructions: Provide a diagram that illustrates the function of your product, user interaction workflow and data flows into and out of your systems or application. This is most easily achieved by two diagrams – one that has a high-level “systems view” of the security products used to protect the network and client data, and a block diagram that shows the “virtual design” of the application modules where client data resides and moves, and how it is protected.*

**System-Level Security Architecture Diagram**  
  
The following diagram identifies the system architecture of the solution, and what security solutions are employed to protect the network and client data.



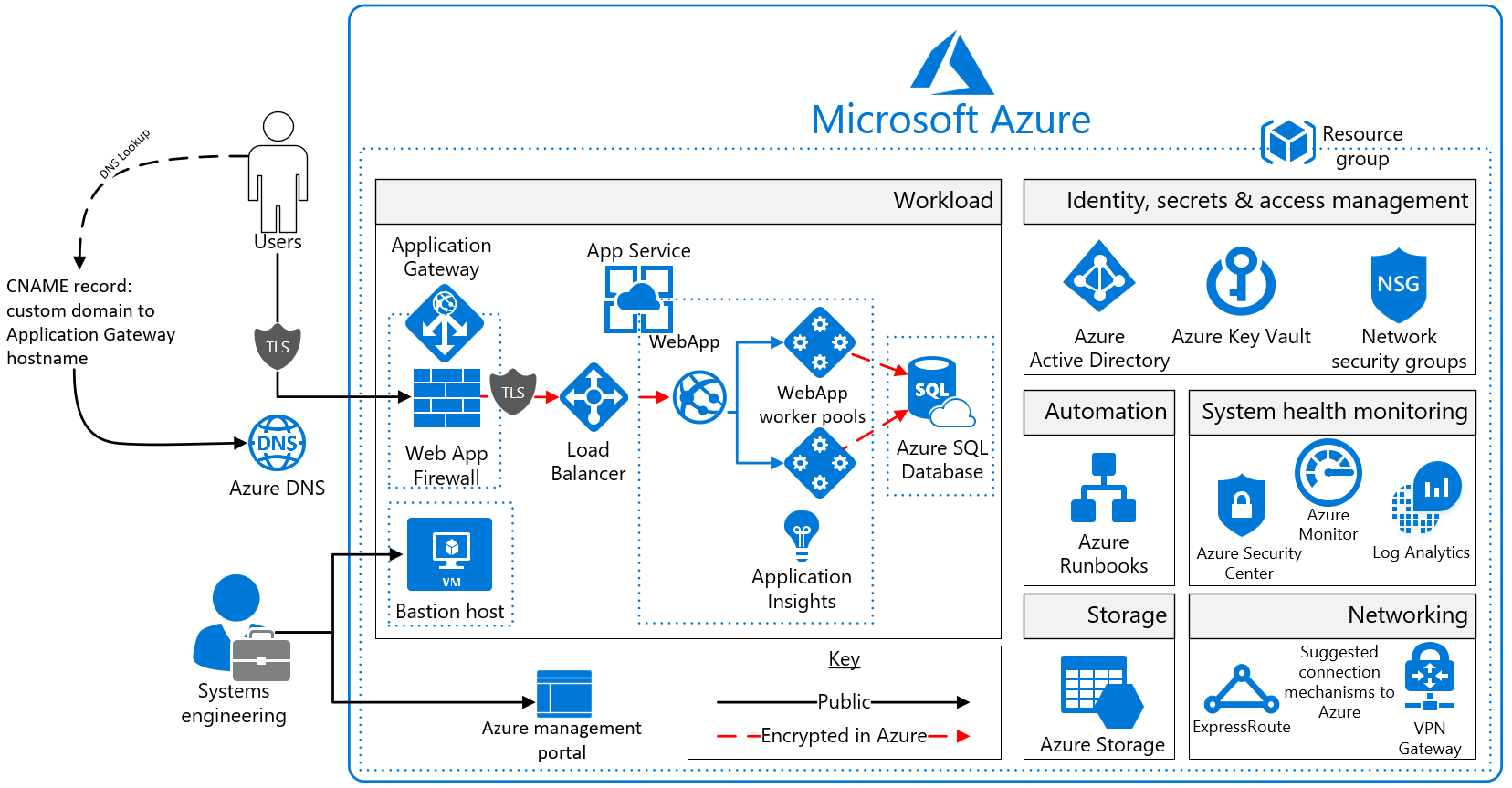
**SAMPLE**

Figure 3 Security Architecture - System View

**Virtual Security Architecture Diagram**

The following diagram identifies the virtual design of the solution, including all places where customer data resides, all data flows and how it is secured by {{insert Company Name}}.

Optional Sample Text: The web tier and backend services are segmented into their own VLAN so as to limit only traffic to only TLS encrypted links over a single port. There are two data layers which are each segmented into their own VLAN to limit access to only those service that require them. The data ingestion/egress layer by default does not have any incoming ports open and provides a way for the platform to reach to the outside to ingest data available from the customer or 3rd-party APIs. If the customs would like to push data to the ingress service, this can be configured on a case-by-case basis. The training service (creation of AI models) is also separated into its own VLAN to ensure no external access.



**SAMPLE**

Figure 4 Virtual Security Architecture

3.3 Third Party Integrations (APIs)

The Company has incorporated into its solution architecture the following third-party solutions that form part of its overall Information Security Program.

|  |  |
| --- | --- |
| **Technology** | **Description** |
| Firewall/Internet Gateway | Company uses the {{insert firewall product name or generic name}} to grant access to systems. |
| Access Control | Company manages operational access to systems with SSH keys tied to directory permissions. |
| Encryption - Data at Rest | Company encrypts all customer data at rest with 256-bit AES encryption in the following databases {{insert databases where customer data resides here}}. |
| Encryption - Data in Motion | Company uses encrypted connections between applications and databases to ensure the security and integrity of data on the wire. |
| Intrusion Detection/Prevention | Company implements the {{insert IPS/IDS product name or generic name}} intrusion detection system to detect and remediate unauthorized access on critical systems. |
| SIEM/ Logging Solutions | Company uses {{insert SIEM or logging solution}} to log all network security events. |
| Other Security Products |  |

3.4 Open Source Components

The Company utilizes the following open-source packages in its solution.

|  |  |
| --- | --- |
| **Package – Version** | **License** |
| E.g. Tensorflow | Apache-2.0 |
| Egg. Django | BSD |
| Egg. Python | Apache-2.0 |
| Egg. Nifi | Apache 2.0 |
|  |  |
|  |  |

4.0 Data Privacy and the Company Platform

4.1 Company Business Intent and User Data

The {{insert product solution name}} helps companies {{insert core mission of your solution}}. Our solution gathers the following types of customer data:

*Instructions: One of the core tenants around data security is what client data you need to store, and why you need it. In this section, please elaborate on your intent for collecting user data. This is especially important if doing business in regions regulated by GDPR.*

* {{insert types of customer data you collect in this list}}

{{Insert company name}} sole business intent collecting the sensitive data above is to help the client:

* {{insert reason(s) WHY you collect this data – it serves which function}}

{{Insert company name}} only collects data on a “need to have basis”, and does not monetize or seek any gain from harvesting or processing any of the client data listed above. In addition, Tugboat Logic will delete any stored customer data upon request by the client.

Sample Text:   
The Tugboat Logic Virtual CISO Platform helps companies manage all aspects of their InfoSec program by automating processes and providing expert security guidance. Our solution gathers the following types of customer data:

* InfoSec policies and controls that the customer has defined in the Tugboat Logic system
* Implementation notes the client has entered into the Tugboat Logic system
* Security events and incidents the client has entered into the Tugboat Logic system
* Customer security questionnaires that are uploaded into the Auto-Answer RFP system
* Vendor security questionnaires the client uploads into the Vendor Management system
* Employee and admin names and email addresses

Tugboat Logic’s sole business intent collecting the sensitive data above is to help the client:

* Create an Information Security policy of record
* Define and track a set of security controls and prove they have been implemented
* Respond automatically to questions in a security questionnaire
* Assess and audit the security posture of their third-party vendors
* Conduct employee cyber security awareness training
* In general, our primary goals in collecting information are to provide and improve our products and services, to provide quality customer service, to contact companies whose representative has indicated an interest in receiving information about Tugboat Logic products and to enable users to effectively navigate the web site.

Tugboat Logic only collects client data on a “need to have” basis, and does not monetize or seek any gain from harvesting or processing any of the client data listed above. In addition, if you wish to cancel your account or request that we no longer use your information to provide you services contact us at privacy@tugboatlogic.com.

4.2 User Consent and Data Privacy

*Instructions: If your solution collects consumer data, this section is good to explain how you obtain consent via a Data Privacy policy.*

For all data provided to the {{Insert Company Solution name}}, an explicit authorization is given by the user for {{Insert Company name}} to use the data or to access third party applications on behalf of an authorized user only for the purpose of the proper function of the {{Insert Company name}} system.   
  
End users have rights to access their personal data under their local data privacy laws and are able to correct, amend or delete that information under certain conditions. If an end user would like to exercise their right of access, if they would like to change their personal data, or if they no longer desire our service, they may access, correct, update or delete it by emailing our Customer Support at {{insert email address here such as: privacy@company.com}}. We will respond to their request to access within a reasonable timeframe. In certain circumstances we may be required by law to retain their personal information, or may need to retain their personal information in order to continue providing a service. {{Insert Company name’s}} complete privacy policy is viewable at {{Insert URL for your privacy policy. If you need help with a sample privacy policy see sample text below.}}

Sample text: For all data provided to the Tugboat Logic system, an explicit authorization is given by the user for Tugboat Logic to use the data or to access third party applications on behalf of an authorized user only for the purpose of the proper function of the Tugboat Logic system.   
  
End users have rights to access their personal data under their local data privacy laws and are able to correct, amend or delete that information under certain conditions. If an end user would like to exercise their right of access, if they would like to change their personal data, or if they no longer desire our service, they may access, correct, update or delete it by emailing our Customer Support at privacy@tugboatlogic.com. We will respond to your request to access within a reasonable timeframe. In certain circumstances we may be required by law to retain their personal information, or may need to retain their personal information in order to continue providing a service. Tugboat Logic’s complete privacy policy is viewable at <https://tugboatlogic.com/privacy-policy>.

4.3 Regulated or Private Data Incidents Within Company

*Instructions: If your solution collects personally identifiable (PII) such as credit card or social security number, indicate how said data is handled (encrypted, anonymized, both). A good best practice is to encrypt all PII data at rest, and anonymize it somehow by either adding “XXX” hashes to part of it (e.g.* [*XXX@gmail.com*](mailto:XXX@gmail.com)*, or XXX-XX-1234) or doing a unique hash (Patrick@gmail.com turns into* [*aZytRqf@gmail.com*](mailto:aZytRqf@gmail.com)*) so you cannot see the data in clear text in log files and elsewhere.*

Sample text: The {{Insert Company Solution name}} will only take action on personally identifiable (PII) or structured data (credit card numbers, social security numbers, passport numbers) for compliance or other security policy reasons. The access to such data is limited to only those internal users or teams that are required by law or corporate governance to see incidents containing PII. The {{Insert Company Solution name}} allows role-based provisioning and incident notifications to be restricted to specific users or teams.

All PII and private user data that may be captured within a compliance or security incident is encrypted at rest within the {{Insert Company name}} database infrastructure. All structured data such as {{define what structured data you collect such as SSN #s, etc.}} are masked with “XXX” hashes automatically by the system so they are illegible when displayed within the audit log.

Sample text: The Tugboat Logic Virtual CISO Platform will only take action on personally identifiable (PII) or structured data (credit card numbers, social security numbers, passport numbers) for compliance or other security policy reasons. The access to such data is limited to only those internal users or teams that are required by law or corporate governance to see incidents containing PII. Tugboat Logic allows role-based provisioning and incident notifications to be restricted to specific users or teams.

All PII and private user data that may be captured within a compliance or security incident is encrypted at rest within the Tugboat Logic database infrastructure. All structured data such as email address or phone numbers are masked with “XXX” hashes automatically by the system so they are illegible when displayed within the audit log.

4.4 Company and Data Platforms

*Instructions: In this section, disclose if you are sharing data with third-party partners in any way, such as via API etc.*

{{Insert Company Name}} is an authorized development partner with {{Insert all authorized 3rd party vendor names}}. As an authorized partner, {{Insert Company Name}} utilizes only authorized data interfaces (APIs) provided by these partners with authenticated connections. {{Insert Company Name}} is contractually bound to uphold the terms of use for each supported data platform. {{Insert Company Name}} also commits to each of its development partners that it will uphold specific codes of conduct and safeguard end user data with the same duty of care and diligence as the network itself.

{{Insert Company Name}} does not sell, distribute, license or otherwise export or make available any customer data made available to it as a result of normal and authorized use of its software by {{Insert Company Name}} administrators or authorized third party software vendors that require data sharing in order to enable interoperable functionality and services.

Sample text: Tugboat Logic is an authorized development partner with Atlassian and Salesforce.com. As an authorized partner, Tugboat Logic utilizes only authorized data interfaces (APIs) provided by these partners with authenticated connections. Tugboat Logic is contractually bound to uphold the terms of use for each supported data platform. Tugboat Logic also commits to each of its development partners that it will uphold specific codes of conduct and safeguard end user data with the same duty of care and diligence as the network itself.

Tugboat Logic does not sell, distribute, license or otherwise export or make available any customer data made available to it as a result of normal and authorized use of its software by Tugboat Logic administrators or authorized third party software vendors that require data sharing in order to enable interoperable functionality and services.

5.0 Information Security Program Overview

5.1 Background

This Information Security Policy is based upon the International Standard ISEC/ISO 270001 the Code of Practice for Information Security Management and ISEC/ISO 270002.

5.2 Requirements for policy

{{Insert Company Name}} has an obligation to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS) to all staff, employees and partners. The objective of this requirement is to ensure that users of *IT/IS* facilities do not unintentionally place themselves, or the Organization, at risk of prosecution or disciplinary action, by carrying out computer related activities that contravene current policy or legislative restrictions. Information within the Organization is intended to be openly accessible and available to all members of the organization for sharing and processing. Certain information (sensitive information) has to be processed, handled and managed securely and with accountability.

This policy outlines the control requirements for all information contained within the Organization network and IT systems.

5.3 Policy structure

This document forms the {{Insert Company Name}} Information Security Policy. Its purpose is to provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the Organization. Supporting Policies and guidance documents containing detailed Information Security requirements are established in support of this policy and can be found in the content of this document and supporting documents in Exhibits attached to this document. Dependent upon the subject matter, supporting policies and guidance will either apply across the Organization or to more specific management, employees, departments or individuals within the Organization.

5.4 Purpose and scope

All processing of data and collection of information will be processed in accordance with {{Insert jurisdiction name}} law.

This policy defines how the organization will secure electronic information, which is found within:-

* {{Insert Company Name}} IS/IT infrastructure.
* Key Business System data and information.
* Security of information held in electronic form on any organization computer.

And is processed or used by:

* Organization Staff and employees who have access to or administer the organization network or IT systems.
* External users, agents and guest users authorized to use organization network or IT Systems.
* Individuals who process key data and information within Key Business Systems.

5.5 Objectives

Information Security controls are designed to protect members of the Organization and {{Insert Company Name}} reputation through the preservation of:

* *Confidentiality* - knowing that *key data and information* can be accessed only by those authorized to do so;
* *Integrity* - knowing that *key data and information* is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
* *Availability* - knowing that the *key data and information* can always be accessed.

The Organization is committed to protecting its customers, users, employees and Key Business Systems. Controls will therefore be deployed that mitigate the risk of vulnerabilities being exploited which adversely affect the efficient operation of the organization.

5.6 Applicability

{{Insert Company Name}}’s Information Security Program applies to all users of the organization network and IT Services and includes:

* All full-time, part-time and temporary staff employed by, or working for or on behalf of the organization;
* Employees working at the organization;
* Third party contractors and consultants working for or on behalf of the organization;
* All other individuals and partners who have been granted access to {{Insert Company Name}}’s network or IT Services.

Managers are ultimately responsible for ensuring that adherence to this policy is observed within their respective department and for overseeing compliance by employees under their direction, control or supervision. Each employee is responsible for their own actions and must ensure all actions relating to using the organization network and IT Services adheres to the principles and requirements of this policy.

5.7 Data Protection Officer

The designated Data Protection Officer (DPO) for {{Insert Company Name}} is:

{{Employee Name}}

{{Employee Title}}

{{Employee email address}}

{{Insert Company Name}} ‘s DPO is responsible for monitoring internal compliance, informing management on its data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs), acts as the primary point of contact for data subject access requests (DSAR) and is our point of contact with any relevant supervisory authority (ICO). The DPO’s contact information is provided in all user/public facing communications required by the GDPR for obligations undertaken by the Company.

5.8 Third Party Vendor Assessment

Then Company undertakes periodic reviews of its third party vendors and suppliers to verify that they are in compliance with {{Insert Company Name}}’s policies and controls as stated in the {{Insert Company Name}} Information Security Program.

6.0 Risk Mitigation, Compliance, Certification Readiness

**6.1 Risk Mitigation Policy**

{{Insert Company Name}} mitigates risk to its application infrastructure and service delivery by strictly adhering to industry security principles and regularly measures its adherence to industry benchmarks with regular internal and third-party validation testing. Industry security principles include:

1. All customer and application data that is stored or processed within the system shall be encrypted.
2. All network access ports or connections to the {{Insert Company Name}} System are set to default closed to the Internet and any port access is accessed with data encryption.
3. All servers and internal API processes have multiple redundancies and parallel processes for robust service availability.
4. {{Insert Company Name}} maintains a published information security program containing documented policies, controls and implementation guidance that are reviewed every 12 months.
5. All {{Insert Company Name}} employees are required to review and agree to the Corporate Information Security Program by completing a workflow that includes review and positive acceptance to such policies. {{Insert Company Name}} maintains an auditable log of all employee training.

**6.2 Compliance Overview**

{{Insert Company Name}} has designed its information security program to broadly conform to the principles of ISO27001 to ensure the integrity and security of customer data.

**6.3 Security Certification Readiness**

{{Insert Company Name}} is committed to validating the strength of our InfoSec program by validating it through well-respected third party security certifications. {{Insert Company Name}} has already achieved {{insert completed certification names}}, and has established the following roadmap for adherence to the following additional standards and certifications. Note roadmaps are subject to change. Copies of completed certifications are available to clients upon request.

|  |  |  |
| --- | --- | --- |
| **Standard** | **Description** | **Completion Date** |
| Tugboat Logic Essentials | Baseline InfoSec program certification | {{Completed Date}} |
| SOC-2 Type 1 | Certification to sell to regulated industries | {{Target Date}} |
| SOC-2 Type 2 | Certification to sell to regulated industries | {{Target Date}} |
| ISO-27001 | Certification to sell to regulated industries | {{Target Date}} |
| FedRAMP | Certification to sell to federal government | {{Target Date}} |
| PCI Self-Attested | Certification for handling payment-related PII | {{Target Date}} |
| PCI 3rd Party Audited | Certification for payment processors | {{Target Date}} |
| GDPR Readiness | Regulation for handling European data | {{Target Date}} |

7.0 Customer Support Service Level Agreement

7.1 Service Availability SLA

*Instructions: In this section, define your product availability goals (SLAs) by severity level.*

{{Insert Company Name}} will achieve a Monthly Uptime Percentage of at least {{99,xxx%}} for each calendar month.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Standard** | **Premium** |  |
| **Response times** | **Initial Response** | | **Ongoing Response** |
| **Severity 1** | {xx Hours}} | {{xx Hours}} | {xx Hours/Days}} |
| **Severity 2** | {xx Hours/Days}} | {xx Hours/Days}} | {xx Hours/Days}} |
| **Severity 3** | {xx Hours/Days}} | {xx Hours/Days}} | {{xx Hours/Days}} |
| **Severity 4** | {xx Hours/Days}} | {xx Hours/Days}} | {{xx Hours/Days}} |

**Severity 1**: A problem that severely impacts your use of the software in a production environment (such as loss of production data or in which your production systems are not functioning). The situation halts your business operations and no procedural workaround exists.

**Severity 2**: A problem where the software is functioning but your use in a production environment is severely reduced. The situation is causing a high impact to portions of your business operations and no procedural workaround exists.

**Severity 3:** A problem that involves partial, non-critical loss of use of the software in a production environment or development environment. For production environments, there is a medium-to-low impact on your business, but your business continues to function, including by using a procedural workaround. For development environments, where the situation is causing your project to no longer continue or migrate into production.

**Severity 4**: A general usage question, reporting of a documentation error, or recommendation for a future product enhancement or modification. For production environments, there is low-to-no impact on your business or the performance or functionality of your system. For development environments, there is a medium-to-low impact on your business, but your business continues to function, including by using a procedural workaround.

8.0 Corporate Overview, Financials and Insurance

8.1 Corporate Overview

|  |  |
| --- | --- |
| Incorporation and Governance | Detail |
| Legal Corporate Name | {{Company}} |
| Incorporation Type (LLC, Partnership, C-Corp, Sole Prop) and Jurisdiction | x |
| Incorporation Month/Year | x |
| Public/Private Corporation? | x |
| Number of Employees | x |
| Key Personnel + Contact email |  |
| CEO | {{Name, Email}} |
| CTO | {{Name, Email}} |
| Engineering Primary Contact | {{Name, Email}} |
| Financial Primary Contact | {{Name, Email}} |

8.2 Insurance Coverage

|  |  |  |  |
| --- | --- | --- | --- |
| Insurance Coverage | Coverage | Exclusions | Limits |
| General Liability | x | x | x |
| Director, Errors & Omissions | x | x | x |
| Cyber Risk and Data Breach | x | x | x |
| Business Continuity | x | x | x |
| Employee Liability, Rental Cars | x | x | x |

9.0 Exhibits

*Instructions: In this section, include all relevant documents that are available to the client upon request. Include any that you have available, and feel comfortable sharing. As a general rule, sharing more information early on may earn trust and expedite the security assessment phase of the sales process. Tugboat Logic recommends a minimum of Exhibits 9.1 and 9.2. Since it takes time to get insurance plans worked out, it pays dividends to have Exhibit 9.4 in place before a client requests it.*

*Helpful Advice:*

* *You can download Exhibit 9.2 below automatically from your* ***Tugboat Logic Virtual CISO Platform*** *by going to the “Policies Deck” page, click on “Actions” button, then click on “Download InfoSec Policy Document”.*
* *A sample of Exhibit 9.1 is available in section 4.2 of this document.*
* *A sample of Exhibit 9.3 is available under Policy #TBL-600 in the* ***Tugboat Logic Virtual CISO Platform***

The following additional documents are available to clients upon request, and are subject to the {{insert company name}} non-disclosure agreement.

9.1 Company Privacy Policy

9.2 Company Information Security Policy

9.3 Company Business Continuity Plan

9.4 Company Proof of Insurance

9.5 Company Security Certification Details

9.6 Third-party Vulnerability Assessment Results