TUGBOAT LOGIC

ATTESTATION REPORT

Tugboat Logic Inc.

July 19, 2021

TABLE OF CONTENTS

433 Airport Blvd, Suite 304
Burlingame, CA 94010 USA
www.tugboatlogic.com

July 19, 2021

About Tugboat Logic's Attestation Report

We are pleased to confirm that Tugboat Logic Inc. has implemented an Information Security Program and a set of Security Controls that are automatically monitored in real time, by Tugboat Logic's Security Assurance platform. Detailed information of the program, controls implemented, and their status is described in Appendix A.

Tugboat Logic's Security Assurance Platform is a cloud-based security and compliance solution that helps organizations establish, maintain and automatically monitor their Information Security Program and share it with external stakeholders. The information contained in this report has been automatically generated from the platform as of July 19, 2021. This report can be obtained on demand at any point in time and captures the data directly from Tugboat Logic Inc.'s Information Security Program as it is represented in the platform.

The combination of the results described in Appendix A, together with Tugboat Logic Inc.'s assertion and the self assessment questionnaire completed by Tugboat Logic Inc. in Appendix B, has been designed to provide the reader with relevant and useful information to evaluate Tugboat Logic Inc.'s security posture and to obtain the necessary confidence and comfort over the effectiveness and operation of their security controls.

The control assessment evaluation is based on a combination of automated evidence collection and verification as well as manual input from Tugboat Logic Inc.. The validity and scope of the data collected in this report are confirmed in Tugboat Logic Inc.'s assertion and the self assessment completed in Appendix B.

July 19, 2021

Tugboat Logic Inc.’s assertion on the Information Security Program

We assert that the information included in this Attestation Report is accurate and that the requirements of our Information Security Program have been met and are operating as of the date of this letter. Our Information Security Program consists of a set of policies and controls that have been designed to protect information and systems from events that could negatively impact our security commitments and to mitigate, monitor and respond to unexpected security events.

We confirm, to the best of our knowledge and belief:

1. We have considered all significant information we believe is relevant to the Assertion.
2. We have input valid data related to our Information Security Program in the Tugboat Logic Platform and configured the automated evidence collection tasks appropriately to collect data relevant to the program and have been fairly represented in Appendix A.
3. The controls identified in Appendix A have been designed and implemented to mitigate significant information security risks in the organization.

Yours truly,

Tugboat Logic Inc.
Get Secure. Build Trust. Sell More.
Tugboat Logic Inc.

APPENDIX A

INFORMATION SECURITY PROGRAM DETAILS AND STATUS

Information in this section is extracted directly from Tugboat Logic's Security Assurance Platform.

Control Name	Control Description	Is the control implemented?	Is the control operating?
TBL1 - Information Security Policies	The organization has formalized and approved the following Infosec policies, which are communicated to and acknowledged by employees and contractors: - Information Security - Access Control - Server Security - Workstation Security - Incident Management - Business Continuity and Disaster Recovery - Network Security - Change Management - Vendor Management - Privacy	Yes	Yes
TBL2 - Access Management	The organization uses Tugboatlogic's automated Onboarding/Offboarding solution to manage user access requests, changes and revocations. User access rights are reviewed on a quarterly basis.	Yes	Yes

TBL3 - User Identification and Authentication	Unique user IDs and strong passwords are required to gain access to information assets (database, servers) and applications. Multi-factor authentication (MFA) is enforced for user accounts with access to the organization's production platform.	Yes	Yes
TBL4 - Workstation Antivirus	The organization has anti-virus software installed and enabled on all workstations.	Yes	Yes
TBL5 - Vendor Management	The organization utilizes Tugboat Logic's vendor management module to evaluate vendors annually. Corrective actions are taken as required based on the results of the assessments.	Yes	Yes
TBL6 - Encryption of Cloud Data at Rest	The organization encrypts sensitive data at rest (stored and backup) in its cloud hosting data stores.	Yes	Yes
TBL7 - Security Awareness Training	The organization uses Tugboat Logic's awareness training module to conduct annual information security awareness training for all employees.	Yes	Yes

TBL8 - Workstation Disk Encryption and Passwords	Disk encryption and system passwords are enabled across all organization workstations.	Yes	Yes
TBL9 - System Performance and Capacity Monitoring	The IT team in the organization continuously monitors system capacity and performance in its cloud environment(s) to identify anomalies that could compromise the systems' availability.	Yes	Yes
TBL10 - System Event Logging	Logging is enabled to monitor activities in the organization's cloud environment(s). Automated alerts are configured to notify IT management, and issues identified are resolved in a timely manner in line with the incident management process.	Yes	Yes
TBL11 - Firewall Rules	The organization's IT management performs an annual review of firewall rules.	Yes	Yes

TBL12 - Asset Inventory	A list of all data within the organization is maintained, including the data owner, classification and where it is stored. The asset listing is reviewed and updated by management on an as-needed basis.	Yes	Yes
TBL13 - Encryption of Data in Transit	Encryption technologies are used to protect communication and transmission of data over public networks.	Yes	Yes
TBL14 - Incident Notification and Resolution	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process.	Yes	Yes
TBL15 - Change Management Process	A defined change management process guides changes to the applications and supporting infrastructure. IT management reviews the process document on an annual basis, and it is updated as needed.	Yes	Yes

TBL16 - Patch Management	The organization maintains a patch management process to confirm the timely remediation of operating system vulnerabilities. In addition, production systems are scanned to test for patch compliance on a quarterly basis.	Yes	Yes
TBL17 - Vulnerability Assessment or Penetration Testing	A vulnerability assessment or penetration test is conducted on an annual basis to identify security exploits. All identified issues are classified according to the risk analyzed and remediated in a timely manner.	Yes	Yes
TBL18 - Administrative/Privileged Access	Access to a generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.	Yes	Yes
TBL19 - Data Backup and Monitoring	Back-ups are performed with the organization's defined frequency using an automated system, replicated to a separate location, and monitored for failure.	Yes	Yes

TBL20 - Privacy Statement and Terms of Business	The organization has a privacy policy on its website that defines privacy obligations in accordance with local laws and regulations. In addition, formal agreements with customers that acknowledge its compliance with security, confidentiality, and privacy commitments are maintained. Management reviews the privacy statement and terms of business on an annual basis.	Yes	Yes

APPENDIX B

TUGBOAT LOGIC INC. SELF ASSESSMENT QUESTIONNAIRE

Information in this section is provided by Tugboat Logic Inc.

Company Background

Tugboat Logic is the Security Assurance Platform for the enterprise. We provide a cloud-based, security and compliance automation system that is designed to help you build and manage your entire InfoSec program that’s as unique as you are. Automatically define security policies, respond to RFPs and provide proof of compliance so you can gain confidence with customers and win more deals. Tugboat Logic provides an automated framework to demystify the process of setting up a security program and then leveraging that program to respond to vendor assessments and audit, or manage third party risk. Further, with Tugboat Logic enterprises can quickly prove compliance, pass third party audits and certifications and adherence to privacy standards with robust evidence collection, reporting and data export capabilities.

Description of products in scope for this assessment

The Tugboat Logic Security Assurance 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, generate their own security policies or use our predefined set of security policies, demonstrate compliance against the InfoSec program by automatically collecting evidence and get ready to do get audited or certified by a third party with our audit readiness module. The solution also enables admins to upload and respond to security questionnaires automatically using Tugboat’s machine-learning-based Auto-Answer recommendation engine. Outputs include an InfoSec Policy Document, Security Assurance Report, completed security questionnaires and Vendor Security Assessments.

List of vendors/sub-processors used to provide services in scope

- Amazon Web Services (AWS)

Are your organization's information security policies approved, published, reviewed annually and communicated?

Yes, Tugboat Logic platform is used to manage an organization's information security policies review, approve and publish the policies in your infosec program. The policies are reviewed and approved by management at least annually and accessible to all the organization's employees through the Tugboat Logic platform.

Does your organization have an implemented solution for managing user access requests, changes and revocations? Are reviews performed for access rights to systems, applications and network devices?

Yes, Tugboat Logic's automated Onboarding/Offboarding solution is utilized to manage user access requests, changes and termination. User access rights are reviewed on a quarterly basis.

How are organization's workstations protected from malware infection?

Anti-virus software installed and enabled on all workstations to detect, prevent and take action against malicious software.

Is there a process in place in your organization for all critical vendors with access to data to periodically monitor compliance with security requirements, resolve any reported issues, and conduct an independent review?

Yes, Tugboat Logic's vendor management module is used to perform risk assessments and performance evaluations for vendors annually. Corrective actions are taken as required based on the outcome of the assessments.

Is sensitive data encrypted while at rest within your environment?

Yes, the organization encrypts sensitive data at rest in its cloud hosting environment. The evidence of encryption is managed through Tugboat Logic’s auto collect dashboard.

Does the organization maintain a security awareness training program?

Yes, the organization uses Tugboat Logic's awareness training module to conduct annual information security awareness training for all employees.

Do all workstations in your organization have password and disk encryption enabled for system confidentiality?

Yes, Disk encryption and system passwords are enabled across all organization workstations and evidence for this implementation is managed using Tugboat Logic's auto collect dashboard.

Are monitoring tools deployed and configured in critical segments to detect performance issues that could compromise availability and security?

Yes, our organization’s IT team continuously monitors system capacity and performance in its cloud environment(s) to identify anomalies that could compromise the systems' availability. Evidence for this control implementation is managed with Tugboat Logic's automated cloud service integration.

Are all network and system devices configured so that system errors and security events are logged, and issues identified remediated?

Yes, logging is enabled to monitor activities in the organization's cloud environment(s). Automated alerts are configured to notify IT management, and issues identified are resolved in a timely manner in line with the incident management process. Evidence is managed with Tugboat Logic's automated cloud service integration.

Does your organization's IT management review firewall configurations?

Yes, the organization's IT management performs an annual review of firewall rules.

Does your organization maintain a list of what data is collected, the location, data owner and classification? Is this list updated and reviewed by management?

Yes, a list of all data within the organization is maintained by including details of the data type, data owner, classification and where it is stored. The asset listing is reviewed and updated by management on an as-needed basis.

Is encryption implemented to protect communication and transmission of data over the public network?

Yes, encryption technologies are used to protect the communication and transmission of data over public networks.

Does your organization have a formal process to report, monitor, notify affected parties and resolve incidents?

Yes, all incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process.

Does your organization maintain a formal approved, published, annually reviewed and communicated Change Management policy that defines the change processes to applications and supporting infrastructure?

Yes, our organization has a defined change management process that guides the changes to applications and supporting infrastructure. IT management reviews the process document on an annual basis and it is updated as needed.

Are security patches regularly reviewed and applied to systems as appropriate?

Yes, our organization maintains a patch management process to ensure the timely remediation of operating system vulnerabilities. In addition, production systems are scanned to test for patch compliance on a quarterly basis.

Does your organization perform vulnerability scans/penetration tests of its systems and correct issues identified in a timely manner?

Yes, a vulnerability assessment is conducted at scheduled intervals to identify vulnerabilities/ penetration tests conducted on an annual basis to identify security exploits. All identified issues are classified according to the risk analyzed and remediated in a timely manner.

How does your organization restrict privileged access to applications and infrastructure internally?

Access to administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel, and administrative access is managed using Tugboat Logic's Onboarding and Offboarding module.

How often are backups taken, where are they stored and are they monitored to confirm successful backup?

Yes, an automated system performs backups at the organization's specified frequency, replicates them to an offsite location and monitors backups for failure.

Does your organization maintain an approved and communicated Privacy policy? Are formal agreements that acknowledge the organization's compliance with security, confidentiality, and privacy commitments? Does management review these documentations?

Yes, our organization maintains a documented, approved, published, and communicated Privacy policy on our website that defines privacy obligations in line with local laws and regulations—formal agreements with customers that acknowledge their compliance with security, confidentiality, and privacy commitments. Management reviews the privacy statement and terms of business on an annual basis.

Does your organization have an identification, authentication mechanism and an enforced password policy for internal and external users?

Yes, all users with access information assets and applications have unique IDs and are required to use strong passwords to gain access. Multi-factor authentication (MFA) is enforced for user accounts with access to the organization's production platform.

TUGBOAT LOGIC INC. – BURLINGAME, CA, USA.