logicbroker®
connecting your eCommerce ecosystem

Logicbroker Security and Operational Controls

Logicbroker | 1000 Bridgeport Ave Shelton, CT 06484 | 203.929.7633 | 203.513.8326 | http://www.logicbroker.com

1. Logicbroker represents that it follows industry best practices as a means to prevent any compromise of its information systems, computer networks or data files ("Computer Systems") by unauthorized users, viruses or malicious computer programs ("malicious functionalities") which could in turn be propagated via computer networks, e-mail, magnetic media or other means to Client.

2. Logicbroker shall apply appropriate internal information security practices, including, but not limited to, using appropriate firewall and antivirus software; maintaining said countermeasures, operating systems and other applications with up-to-date virus definitions and security patches; installing and operating security mechanisms in the manner in which they were intended sufficient to ensure Client will not be impacted nor its operations disrupted; and permitting only authorized users to computer systems applications.

3. Logicbroker agrees to adhere to industry "best practices" security standards as it pertains to the technology environment hosting and controlling access to data provided by Client and utilized by both Client and Logicbroker. Logicbroker further agrees to exercise reasonable due diligence to ensure that any and all of Logicbroker 's agents, business partners, contractors and subcontractors maintain compliance with the same industry "best practices" security standards.

4. If Client is provided access to Logicbroker systems, Client will secure access to any passwords provided by Logicbroker to ensure that only authorized users have access to Logicbroker systems. Client will follow Logicbroker's policies and rules with regard to its electronic systems. Client shall promptly notify Logicbroker of any changes in the status of its authorized users (e.g. termination of employment or change of access level). All authorized users must be named users (e.g. no generic passwords or shared accounts). Client will ensure that only those of its personnel who are authorized to access the databases and applications on Logicbroker's systems will do so and only in a manner that is consistent with Client's permitted use of such Logicbroker systems. Client will notify Logicbroker promptly upon becoming aware of any unauthorized access, disclosure or use of such passwords. The parties shall work together in order to mitigate to the extent practicable any harmful effect resulting from such unauthorized access, disclosure or use of such passwords.

5. Logicbroker shall transmit, transfer, and deliver all data via an encrypted or similarly secure transport methodology and in a format to be mutually agreed upon by both parties. If the data is to be shared back and forth, Logicbroker shall ensure that its systems are able to receive data from Client in a mutually agreed upon format. Logicbroker shall promptly notify Client upon becoming aware of any unauthorized access, disclosure or use of such passwords and any security breaches of the connected systems. The parties shall work together in order to mitigate, to the extent practicable, any harmful effect resulting from such unauthorized access, disclosure or use of such passwords.

6. Logicbroker shall use up to date anti-virus tools to remove known malicious functionalities from any email messages or data transmitted to Client; prevent the transmission of attacks on Client via the network connections between Client and Logicbroker; and prevent unauthorized access to Client via Logicbroker's networks and access codes.

7. Each Party will use commercially reasonable measures to screen any software provided or made available by it to the other Party hereunder for the purpose of avoiding the introduction of any "**virus**" or other computer software routine or hardware components which are designed (i) to permit access or use by third parties to the software of the other Party not authorized by this Agreement, (ii) to disable or damage hardware or damage, erase or delay access to software or data of the other Party or (iii) to perform any other similar actions. If a virus is found to have been introduced into Client's systems or the systems used to provide the Services as a result of a breach of the foregoing covenant, Logicbroker will use commercially reasonable efforts, at no additional charge, to reasonably assist Client (within the scope of the Services) (A) in eradicating the virus and reversing its effects and (B) to the extent the virus causes a loss of data or operational efficiency as a result of a breach of the foregoing covenant, in mitigating and reversing such losses.

8. Logicbroker in accordance with its standard security policies and procedures shall perform and share with Client a summary of the most recent results of any third party security assessment or SSAE 16 assessment of the Logicbroker technology environment, including any Third Party hosting environment.

9. Logicbroker SLA and Azure Hosting Umbrella. Logicbroker is a cloud-based solution with redundant production services, such as automatic failovers. Monitoring offers full visibility to procurement data via automated reporting on a scheduled basis on the transactional level. Additionally, there is real-time reporting on any system issue. Server performance, health, and wellness are monitored internally by Logicbroker and externally by Microsoft.

    a) Logicbroker will provide a dedicated resource for Client who will be available during the hours of 8AM-6PM EST. Outside of those hours, Logicbroker provides 24/7/365 rotating on call support, along with a support email group.
    b) If there is a mission critical action item, Logicbroker will provide feedback within 4 hours. Normal updates will be provided during 8AM-6PM EST or by on call support outside of those hours.
    c) Logicbroker will provide a web based user interface for Client to be able to run reports to view business critical KPI in real time. In addition, reports can be automatically delivered via email on daily/weekly/monthly configurations to suit the needs of Client.
    d) Logicbroker utilizes Azure services which run 24/7 to monitor the health and performance of the servers. There is also internal reporting on the data that runs every 6 hours and sends a full report of any abnormalities or exceptions to the Operations Team. There is a dedicated resource monitoring the system 24/7 to respond to any issues that are reported, or escalate if needed to Level 2 support.

e) Based on the mappings and integrations, there are often mandatory fields identified (i.e. a tracking number on a shipment notice). If the data is missing, the document is failed and the client is emailed/notified to address the situation in order for the shipment to be reprocessed. These checks are configurable and apply to all documents (i.e. missing PO number on an order, missing total on an invoice). A distribution list is set up that includes all interested parties for Client (primary contact and internal support team) which is used when notifying via email. All issues are tracked until resolved.
f) Within the user interface provided, Client will be able to view documents in flight in real-time with additional KPI reporting. For example, Client would be able to run a report to view how many purchase orders have been sent that have not been acknowledged over a configurable period of time
g) Within the user interface provided, Client will be able to view the data being processed at designated statuses to monitor workflows per trading partner to make sure their SLA is being maintained.

10. Logicbroker shall also perform and share with Client a web application assessment of any and all web applications utilized by Client to enter, transmit and/or store Client data.

11. In accordance with all applicable U.S. and international privacy laws, Logicbroker agrees to safeguard confidential, protected individually identifiable personal information (health, financial identity) which is received, transmitted, managed, processed, etc. and to require any subcontractors, or agents to meet these same standards.

12. Logicbroker agrees to regularly audit and monitor information systems processing Client's business activities to ensure the protection of Client's information. Monitoring includes, but is not limited to, potential breaches or hacking activity and access to devices.

13. If Logicbroker becomes aware of or determines that Logicbroker 's technology or equipment is adversely affected by a security breach, or is causing or is threatening to cause a security breach, incident or other violation of the Logicbroker 's or Client's network or security standards, Logicbroker agrees to immediately notify a member of Client's Technology Management team.

14. Logicbroker's SLA capabilities include timely deliverable documents to meet SLA requirements, a user interface for Client for exception management, and reports Client can view in real-time or have delivered to specific team members/email distribution groups. Logicbroker has partnered with Microsoft to utilize Microsoft Azure for hosting product infrastructure. Azure references 99.95% availability SLA, 24/7 tech support, and around-the-clock service health monitoring that companies such as Skype, Office 365 and Xbox utilize as well. Throughput and capacity are monitored by the Logicbroker production services unit. Server health and performance are monitored through Microsoft Azure and are easily expanded based upon client's current and future requirements. The Logicbroker cloud

architecture enables large volume throughput and asynchronous communication without the need for hardware or infrastructure on the client side. Quarterly releases are delivered without cost to clients and follow a three step implementation approach to keep production online. For Azure, security upgrades or system patches are required to update, and if servers will be down for a designated period of time, Logicbroker will hold orders in a queue to continue processes for Client and will deliver all documents held in queue once service is returned online. Backup and recovery is handled by Microsoft Azure. Azure SQL has 30 full days of restore points. New VM's can be implemented quickly by a production services team. Azure highlights include, but are not limited to:

a) 24 hour monitored physical security. Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.
b) Monitoring and logging. Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers.
c) Patching. Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.
d) Antivirus/Antimalware protection. Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.
e) Intrusion detection and DDoS. Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.
f) Zero standing privileges. Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems that store customer data is strictly controlled via lock box processes.
g) Isolation. Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users. Virtual Machines do not receive inbound traffic from the Internet unless customers configure them to do so.
h) Azure Virtual Networks. Customers can choose to assign multiple deployments to an isolated Virtual Network and allow those deployments to communicate with each other through private IP addresses.
i) Encrypted communications. Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.
j) Private connection. Customers can use ExpressRoute to establish a private connection to Azure datacenters, keeping their traffic off the Internet.