Logistix Solutions Security Whitepaper

Introduction

As a software provider, Logistix Solutions fully understands the security implications of using enterprise level software and incorporating highly sensitive strategic data. Our software delivery platform, architecture and on-premise model are designed to deliver better security than cloud-based and many traditional solutions. We make security a priority to protect our own software and data solutions and well as our customers' data. Because Logix runs on our customers' own computers and networks, organizations can directly benefit from their own internal security protocols and the knowledge that they are always in control of their own data and software application.

Security drives our organizational structure, training and support processes. It shapes the technology we employ in-house. It's central to our everyday operations and customer interactions, including how we address customer concerns. It's prioritized in the way we handle customer data. And it's the cornerstone of our account controls, our compliance and the certifications we offer our customers.

This paper outlines Logistix Solutions' approach to security and compliance for our suite of Logix software and internal data. This whitepaper focuses on security including details on organizational and technical safeguards regarding how Logistix Solutions protects our software and your data.

Logistix Solutions' security culture

Logistix Solutions has created a focused security culture for all employees and third-party consultants. The influence of this culture is apparent during the training and onboarding process, and as part of every stage of development, support and customer interaction.

Background checks

Before they join our team, Logistix Solutions determines an individual's or organizations' previous employment, credentials, performance and available track record. and performs internal and external reference checks. Background checks are conducted to the extent permissible by law and availability of information.

Security enforcement

All Logistix Solutions employees and consultants undergo security training as part of the on-boarding process and receive ongoing security updates. New employees and consultants agree to our Non-Disclosure Agreement, which highlights our commitment to keep customer information safe and secure. For instance, topics like secure coding practices, product design and mitigation techniques and more are part of the training process.

Collaboration with the security research community and software development providers

Logistix Solutions has long enjoyed a working relationship with the software development community, and we greatly value their help identifying potential vulnerabilities in their own products' potential to impact our Logix software and data. Logistix Solutions receives bulletins and notices from our partners and diligently updates its software and development platforms to better secure against on-going threats and malware.

Operational security

Far from being an afterthought or the focus of occasional initiatives, security is an integral part of our operations.

Vulnerability management

Logistix Solutions administrates a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and audits. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and tracked until it can be verified that the issues have been remediated. Logistix Solutions also maintains relationships and interfaces with its development partners, such as Microsoft and Google, to track reported issues in services and tools.

Malware and virus prevention

An effective malware or virus attack can lead to software and data compromise. Logistix Solutions takes these threats very seriously and uses a variety of methods to prevent, detect and eradicate malware. Logistix Solutions development computers are fully protected against malware and virus intrusion and limit any interaction other than as necessary to support product development. Logistix Solutions' malware strategy begins with infection prevention by using manual and automated scanners to scour its software and data dynamically or on a daily basis.

Before publishing any Logistix Solutions software or data for download on our secure website, malware and virus scanning software is used to identify any occurrence of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners.

Logistix Solutions makes use of multiple antivirus engines in its email, cloud, servers and workstations to help identify malware that may be missed by antivirus signatures.

Website

Logistix Solutions' security monitoring program is focused on information gathered from its website services provider, employee actions on systems and outside knowledge of

vulnerabilities. Website traffic reports, security alerts, bulletins and active account management enable us to actively determine when an unknown threat may exist and escalates to a review of our security protocols, published software and any supporting data.

Incident management

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation.

Technology with security at its core

Logistix Solutions runs on a website technology platform that is conceived, designed and built to operate securely. Our website and application software which is available for download is protected using the latest SSL security protocols and Code Signing Certification to ensure the original application code and any supporting data has not been tampered with and originates from Logistix Solutions LLC.

Seal of trust

An SSL certificate includes a seal of trust graphic confirming Logistix Solutions' website is secure and our visitors' information is protected. Without this trusted SSL certificate, Google Chrome will tag a site as Not Secure. SSL security may also provide warranty and other guarantees which may be available and can be reviewed in detail upon request.

Securing data

Data is vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, all of our customers' data is always directly in control and resident on our customers' own computers. Any data transmitted to Logistix Solutions is voluntarily provided by our customers under the pertinent Non-Disclosure Agreement and protected by Logistix Solutions' own encryption and password protection so that only our users and Logistix Solutions can access or read the data. Any data transmitted to Logistix Solutions by the customer for support or other purposes in other forms, such as in Excel, is at the customer's own volition and according to their security protocols.

Support Service availability

Support services are available generally via email by contacting the business center at bc@logistixsolutions.com with a general response time of 24 hours or often less.

Independent third-party certifications

Logistix Solutions' Logix application is protected via third-party Code Signing certification provided by Sectigo.

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow.

Preventing Tampering and Compromised Software

Enterprise Code Signing certificates enable developers to digitally sign applications, drivers and software programs so that end users can verify that a third party has not altered or compromised the code they receive. To verify the code is safe and trusted, these digital certificates include the software developer's signature, the company name and timestamping.

All Logistix Solutions applications are Code Signed using Sectigo CSL's to ensure that the application and imbedded data are authentic and have not been compromised.

Data usage

Our philosophy

Logistix Solutions customers own their data, not Logistix Solutions. The data that customers put into our systems is theirs, and we do not scan it, access it nor use it without our customers' authorization (typically for support services). Logistix Solutions will not process data for any purpose other than to fulfill our support obligations. Furthermore, if customers request that we delete their data after having been provided such data, we commit to deleting it from our systems immediately or within an agreed upon time frame allowing for effective support services. Finally, we provide tools that make it easy for customers to transmit their data if they choose.

Third-party consultants

Logistix Solutions directly conducts virtually all support activities to provide our services. However, Logistix Solutions may engage some third-party consultants or suppliers to provide services related to its applications, including customer and technical support. Prior to onboarding third-party suppliers, Logistix Solutions conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Logistix Solutions has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

Conclusion

The protection of your data and corporate intelligence is a primary design consideration for all of Logistix Solutions' customer approach, products and operations. Our design and operational protocols enable Logistix Solutions to address vulnerabilities quickly or prevent them entirely.

We believe that Logistix Solutions can offer a level of protection that very few other software providers or private enterprise IT teams can match. Because protecting data and corporate intelligence is core to Logistix Solutions' business, we can make security a priority and make assurances that others cannot. Logistix Solutions strong contractual commitments make sure you maintain control over your data and our applications and how the data it is processed including any results from our application(s) and suggested solutions and computations.

For these reasons and more, organizations across the globe trust Logistix Solutions with their most valuable asset: their information. Logistix Solutions will continue to invest in our platform to allow you to benefit from our services in a secure and transparent manner.