LeaseAccelerator
Lease Lifecycle Automation

Security and Business Continuity Policy

Overview

This policy describes the security and business continuity measures that LAS applies generally to the Subscription Services. Any capitalized terms used but not defined in this policy have the meaning ascribed to such term in the Subscription Agreement. References to "LAS", "we," "our" and "us" in this policy mean the LeaseAccelerator entity that is a party to the Agreement with you. References to "you" and any derivatives thereof in this policy mean the Customer entity that is a party to the Agreement with LAS. This policy may be amended by us from time to time and any such changes will be posted at the LAS Legal web page.

Security measures

1. **User Security Measures.** LAS maintains an information and physical security program that implements the following controls to restrict access to the systems used by LAS to provide the Subscription Services and on which we store your data:

    a. Entry into the Subscription Services is username and password-controlled or via Single-Sign-On (SSO) if the SSO option was purchased by you.

    b. On the login screen, the password is encrypted using RSA 128-bit public key/private key encryption from the user's browser – independent of the https session – before being submitted over the Internet.

    c. The Subscription Services use https for session activity, including login.

    d. User access to features is restricted through role-based permissions. Configuration of role-based permissions is controlled by LAS senior-level engineering staff. LAS privileged user accounts are limited to specific personnel within the LAS Technology Services Team. Approvals for access are made by their supervisor and approved by our Account Management Team. LAS performs privileged user quarterly access reviews. LAS promptly revokes employee access to VPN, soft-token, and account(s) upon notification from our VP of Talent Development (HR).

    e. Sensitive information and operations that a user is not authorized to access are physically omitted from the web page prior to delivery to the user's browser.

    f. Manually-constructed URLs are blocked by a combination of session ID controls and a request-by-request tracking ID.

    g. The Subscription Services incorporate technology specifically designed to protect against cross-site request forgery (CSRF) attempts.

    h. Form data is submitted using POST mechanisms.

    i. Your data is stored in a separate set of tablespaces and logically separated from the data of other LAS customers.

    j. Passwords are stored in encrypted form; no passwords are stored in plaintext.

    k. Plaintext passwords are not written to any log.

l. LAS staff has no mechanism for “figuring out” user passwords; if a user forgets their password, LAS staff can reset their password to a known control password in order to allow the user to re-enter the system.

m. The servers for the Subscription Services are physically hosted in facilities that have obtained industry-recognized security certifications such as, but not limited to, ISO 27001, SOC 1, SOC 2, and PCI.

n. Copies of your data are limited to those reasonably necessary for us to provide the Subscription Services and the business continuity and backup measures we implement as described further below.

2. **Encryption During Transmission; Storage.** Your data is encrypted during transmission between the Subscription Services and any third party, including your users, and while being stored in any back-up media.

3. **TLS Encryption.** Following your request to us, LAS will reasonably cooperate with you to establish Transport Layer Security (TLS) encryption between you and LAS for email communications.

4. **Access Reports**. LAS provides you the ability to run reports listing all users with access to your data, including the date of last access, scope of access, and authorization level for each user.

5. **Log Information.** LAS retains system log and transaction log information for no less than one (1) year for logical systems and no less than 90 days for physical security. LAS reviews these logs daily and addresses any discovered abnormalities promptly following detection.

6. **Security Awareness Training**. LAS employees who have access to your data will undergo security training on an annual basis.

7. **Background Checks**. If a LAS employee has (a) access to your production data or your network or systems or (b) unescorted access to your facilities, LAS assigns employees, to the extent permitted by applicable law, on which LAS has conducted a criminal convictions search within five (5) years of first having such access. The criminal convictions search typically covers the preceding seven (7) year period. Subject to applicable law, LAS will not assign any such employee who has been convicted of, or plead guilty to, a felony of any type or a misdemeanor involving theft, fraud, embezzlement, or money laundering or which is otherwise related to dishonesty or a breach of trust.

Penetration tests and vulnerability scans

1. Upon your written request and at your expense and subject to the requirements of this paragraph, LAS may permit you (or your third party designee who is reasonably acceptable to us and not a competitor of LAS) to perform penetration testing and/or vulnerability scanning to test the security of the Subscription Services (“**Testing**”). In the event LAS grants its consent to such testing or scanning, you agree to all of the following:

    a. To comply with LAS’s requirements for engaging in such testing and scanning;
    b. To not disrupt, degrade, or otherwise harm in any manner the Subscription Services or its host’s services or cause a violation of LAS obligations to any third party, including those requirements in LAS’s then current Penetration Testing Policy;

c. Not to: (i) test (i.e., submission of traffic) against any other servers other than the LAS-identified host servers; (ii) engage in denial of service attacks, including distributed denial of service attacks, against any servers or network equipment; (iii) attempt server reboots; nor (iv) install bots, viruses, trojans, "rootkits" or other executables that may harm the LAS Subscription Services or systems or other customers of LAS;
d. Share the results of the Testing with LAS;
e. To require your third party designee to comply with all of the foregoing; and
f. Indemnify LAS for any and all damages caused by the Testing.

2. Any consent granted by LAS is limited to a single Testing event, which will occur at a time mutually agreed by you and LAS, and does not apply to any future Testing. LAS reserves the right to revoke its consent at any time and to terminate or suspend any Testing, and you agree to comply with the foregoing and immediately discontinue or suspend, as applicable, any Testing.

3. If the Testing results in negative findings that have, or could reasonably be expected to have, an adverse impact on the Subscription Services, LAS will review those findings with you, and if LAS is able to confirm the findings, LAS will use reasonable efforts to remediate such findings as soon as reasonably practicable.

SOC audits

1. LAS audits the security of its computing environment and systems used to provide the Subscription Services no less frequently than on an annual basis and according to industry-recognized security standards such as required for a Service Organization Control 1 ("SOC1") audit and a Service Organization Control 2 ("SOC2") audit (collectively, an "LAS Audit"). The LAS Audit produces one or more reports, including a SOC1, Type 2 report and a SOC2, Type 2 report (an "Audit Report"). Promptly following your written request, LAS will make available for your review a summary of each Audit Report for the then-current Contract Year. At LAS's sole election, the summary may be made available to you at our designated facility or via an online sharing portal.

2. LAS will review the results of an Audit Report and use reasonable efforts to remediate, as soon as reasonably practicable, (a) any errors identified in a LAS Audit that could reasonably be expected to have an adverse impact on the Subscription Services and (b) any material control deficiencies identified in the LAS Audit. If requested by you in writing, LAS will provide you with a written statement indicating how LAS remediated the findings.

Business continuity

1. **Business Continuity Plan.** LAS maintains business continuity and disaster recovery plans (collectively, a "**Business Continuity Plan**") designed for LAS to continue performance of the Subscription Services during your Subscription Term. Promptly following the occurrence of an event that triggers the implementation of our Business Continuity Plan (but not to exceed two (2) Business Days after LAS becomes aware of such event), LAS will notify you in writing, at your address listed on your Order Form, regarding the event. LAS tests its Business Continuity Plan no less than annually. Upon your request, LAS will provide you with a copy of LAS' most recently completed SOC 1 attestation.

2. **System Back-Up; Lost/Damaged Data**. LAS performs back-ups of its systems and production data on a daily basis. LAS will use reasonable efforts to restore, at its own expense and from the most recent backup, any of your production data that is lost or damaged by LAS. To the extent that any such loss or damage is attributable to causes beyond the reasonable control of LAS, you may request assistance from LAS with respect to restoration of production data, which assistance may be provided at an additional cost to you.