Cloud Services for Testing Assistant

Security and Privacy White Paper

February 2023

www.lexmark.com

Contents

Security statement

When organizations implement a cloud-based solution, they put their trust in the solution provider to protect their data and deliver a secure platform.

Lexmark takes this trust seriously.

All user data is kept secure. Only required personal data, such as email addresses, names, and student ID numbers, is collected. No financial data is collected or stored.

This document is intended for Lexmark customers and Lexmark partners who are interested in understanding how the information assets are handled within Lexmark Testing Assistant. The document also contains information on how the solution interacts with the information systems of the customer.

User security

Lexmark uses some of the most advanced technology for Internet security commercially available today.

- Users are required to create a unique username and password that must be entered each time they log in. User passwords must meet the complexity requirements.
- All user passwords are encrypted in the database as a nonreversible salted hash.
- Users are warned if they try to set a vulnerable password that a third party already leaked.
- Secure Sockets Layer (SSL) technology is used to protect all data, in motion and at rest, using server authentication and data encryption. User data is safe, secure, and available only to authorized persons.
- Role-based access control method is used to restrict access to authorized users.

Physical security

- Data center certifications:
  - SOC 1 / SSAE 16 / ISAE 3402 (formerly SAS 70)
  - SOC 2
  - SOC 3
  - FISMA, DIACAP, and FedRAMP
  - DOD CSM Levels 1–5
  - PCI DSS Level 1
  - ISO 9001 / ISO 27001
  - ITAR
  - FIPS 140-2
  - MTCS Level 3
- The data centers are staffed with accredited technicians.
- The data centers are secured using two-factor authentication, video surveillance, intrusion-detection systems, and 24/7 security personnel.
- The data centers are equipped with digital surveillance systems.
- The data centers are equipped with state-of-the-art fire detection and suppression systems.
- The data centers have environmental controls for temperature and humidity.

- All customer data is stored on servers in North America (USA or Canada).
- Magnetic storage devices that have reached the end of their useful life are demagnetized and physically destroyed in accordance with industry-standard best practices.

Availability

- Fully redundant IP connections.
- Multiple independent connections to Tier 1 Internet access providers.
- 24/7 uptime monitoring with escalation to Lexmark representatives for any downtime.
- All services have quick failover points and redundant hardware across multiple availability zones.
- The services are scalable to meet demand.
- The data centers are equipped with backup generators.
- The servers have redundant power supplies and uninterruptible power supplies.
- Application services are load-balanced, stateless, and redundant to make sure that a server is always ready to handle requests.

Network security

- Secure layered stateful firewalls restrict access to servers.
- The network provides protection against traditional network security issues such as DDoS attacks, MITM attacks, IP spoofing, port scanning, and packet sniffing.
- The cloud servers have antivirus and threat-detection software to protect against malware and targeted attacks.
- Layered intrusion-detection systems continuously monitor for unauthorized access.
- Next-generation persistent-threat monitoring ensures high threat prevention performance to safeguard against malicious activity and prohibited access.
- Network security audits are performed regularly using an automated security assessment service.
- All environments are logically isolated using secure virtual private clouds.

Storage security

- All data, both at rest and in flight (inbound and outbound), in encrypted.
- All off-site backups are encrypted.
- Sensitive data elements are doubly secured using layer encryption.
- Customer data is stored on RAID 1 arrays.
- Backups occur internally daily and hourly to a centralized backup system for off-site storage.
- Encrypted off-site backups are replicated in real time to centralized backup systems in North America (USA or Canada).

Organizational security

- Role-based advanced access control systems are used to restrict administrative access based on a user's role.
- Access controls to sensitive data on the databases and systems are set on a need-to-know basis.
- Access to server control panel requires multifactor authentication.
- System audit logs are maintained and monitored.
- Internal information security policies are reviewed and updated regularly.
- Background screening on all employees is performed.

Software

- Engineers use industry-standard best practices and secure coding guidelines.
- The latest patches are applied regularly to all operating systems and application files.

Handling of security breaches

No method of data transmission over the Internet, or method of electronic storage, is completely secure. Lexmark cannot guarantee absolute security. If Lexmark learns of a security breach or potential security breach, then the affected users are notified electronically so that they can take appropriate protective steps. Lexmark may also post a notice on the website.

User responsibilities

Lexmark makes sure that the systems are secure, but keeping data secure also depends on users. Users must create complicated passwords and store them safely to maintain the security of their account. Users must not divulge their passwords to anyone, write it down where it could be associated with another personal ID, or reuse it in another location. Devices used to access the Lexmark Cloud Services must have sufficient security to keep any data downloaded away from prying eyes.

Privacy

Information collected by Lexmark

Lexmark requires the following data to enable and maintain the user's account:

- Email addresses
- Names
- Student ID numbers

How information is used

The information collected is used only for the limited purposes of Lexmark Testing Assistant and its related functionality and services. These limited purposes are as described in this **Privacy Policy** and as permitted by applicable laws. These limited purposes include circumstances where it is necessary to fulfill your requested services, or where you have given us your express consent. Other purposes include the following:

- Sending you technical notices, updates, security alerts, and support and administrative messages.
- Monitoring and analyzing trends, usage, and activities about Lexmark Testing Assistant to help in future product development.
- Personalizing and improving Lexmark Testing Assistant, and provide features to customize your experience and match your usage and preferences.

Data and reports are not released, sold, reproduced, transferred, or otherwise exploited or disclosed.

Testing Assistant

Ports and protocols used when grading printed tests

Lexmark Testing Assistant is a cloud-based application that provides an online standardized test grading service for instructors. This application uses HTTPS to establish communication between the cloud service and a browser on the computer of the instructor.

HTTPS port 443 is the only port used between Lexmark Testing Assistant and the computer of the instructor. However, the application may also use other services using other ports for various functions that occur outside the firewall of the school. Since these actions happen outside the firewall, it is not necessary to modify their firewall to accommodate other functions.

To use Lexmark Testing Assistant, instructors and students must have an email account. While not part of the Lexmark Testing Assistant solution, email servers and clients use Simple Mail Transfer Protocol (SMTP) and Internet Messaging Access Protocol (IMAP). The email service may use SMTP port 25 or 587, while IMAP may use TCP ports 143 (unsecured) and 993 (secured).

The Lexmark MFPs used with Lexmark Testing Assistant are configured to send scanned images of the answer sheets to the cloud. The MFP can use either of the following apps to scan images:

- **Scan to Email**—This built-in app uses SMTP to send emails to Lexmark Testing Assistant. The default SMTP port is 25, but some schools may also use SMTP port 587.
- **Grade Test**—This custom eSF app uses HTTPS port 443 when sending scanned images of the answer sheet to the cloud.

Ports and protocols used when grading online tests

With Lexmark Testing Assistant, instructors can email the links to online tests to students. The students take the tests, and then submit them for grading.

When an instructor sends the email, email servers and clients use SMTP and IMAP. The email service may use SMTP port 25 or 587, while IMAP may use TCP ports 143 (unsecured) and 993 (secured).

Students accessing online tests use HTTPS port 443.

Notices

Edition notice

February 2023

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user’s responsibility.

For Lexmark technical support, go to **http://support.lexmark.com**.

For information on Lexmark's privacy policy governing the use of this product, go to **www.lexmark.com/privacy**.

For information on supplies and downloads, go to **www.lexmark.com**.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Trademarks

Lexmark and the Lexmark logo are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

All other trademarks are the property of their respective owners.

Index