



Hosted Testing and Grading

Technical White Paper

July 2014

www.lexmark.com

Lexmark and Lexmark with diamond design are trademarks of Lexmark International, Inc., registered in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2014 Lexmark International, Inc.

All rights reserved.

740 West New Circle Road
Lexington, Kentucky 40550

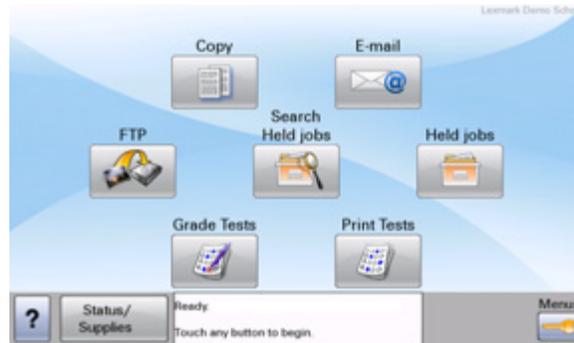
Introduction

In schools everywhere, teachers are continuously asked to do more testing, assessment, and reporting. At the same time, student-to-teacher ratios are increasing, and manual grading can't keep up with demand. Automation helps, but current solutions for automatically grading test forms require expensive specialized equipment and pre-printed forms that must be kept in inventory. IT staff are stretched, and specialized systems require extra maintenance time that isn't always available. Also, as more data is kept electronically and online, privacy and security remain principal concerns.

Lexmark™ Hosted Testing and Grading is a cost-effective solution that automates testing, reporting, and assessment using only Internet-connected Lexmark *multifunction printers* (MFPs), which, unlike specialized equipment, can be used for all printing and scanning as well. Hosted software minimizes system maintenance, and a robust security architecture protects students' data.

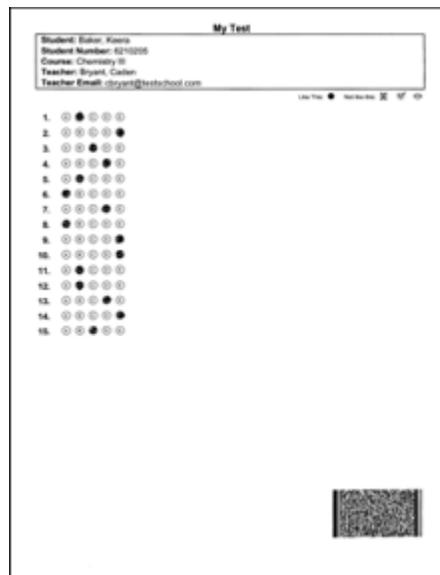
How can Hosted Testing and Grading benefit my school?

Lexmark Hosted Testing and Grading is a software solution that simplifies and accelerates the classroom testing process using Lexmark MFPs that support the Lexmark *Embedded Solutions Framework* (eSF) v2.0 or higher.



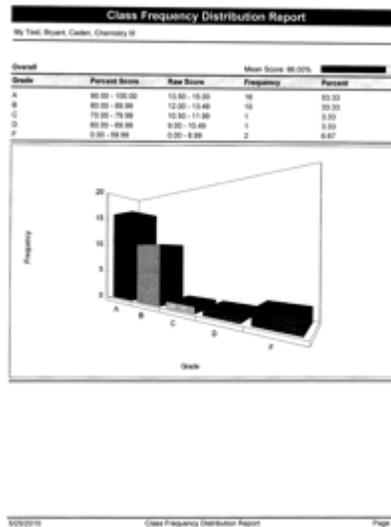
With Lexmark Hosted Testing and Grading, teachers can:

- **Print bubble sheets**—By answering prompts on the printer control panel, teachers can quickly generate a test packet that includes bubble sheets personalized with students' identification and a blank answer key, all using plain paper instead of expensive traditional bubble sheet forms.



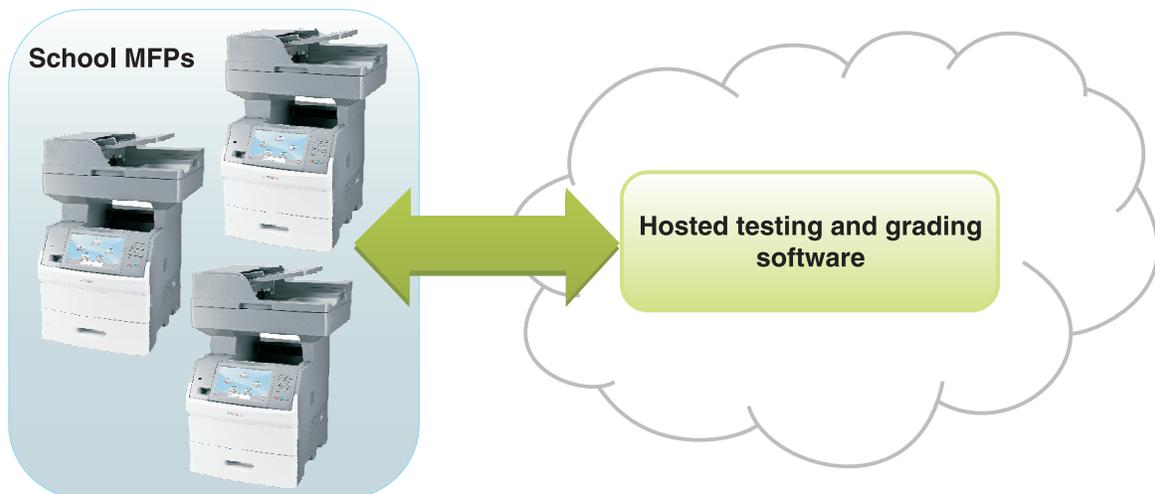
- **Grade tests instantly**—Once completed, test forms are scanned directly from the printer and graded within minutes.

- **Compile grading reports**—E-mailed, stored, or printed reports provide immediate feedback on individual student performance and potential trouble areas.

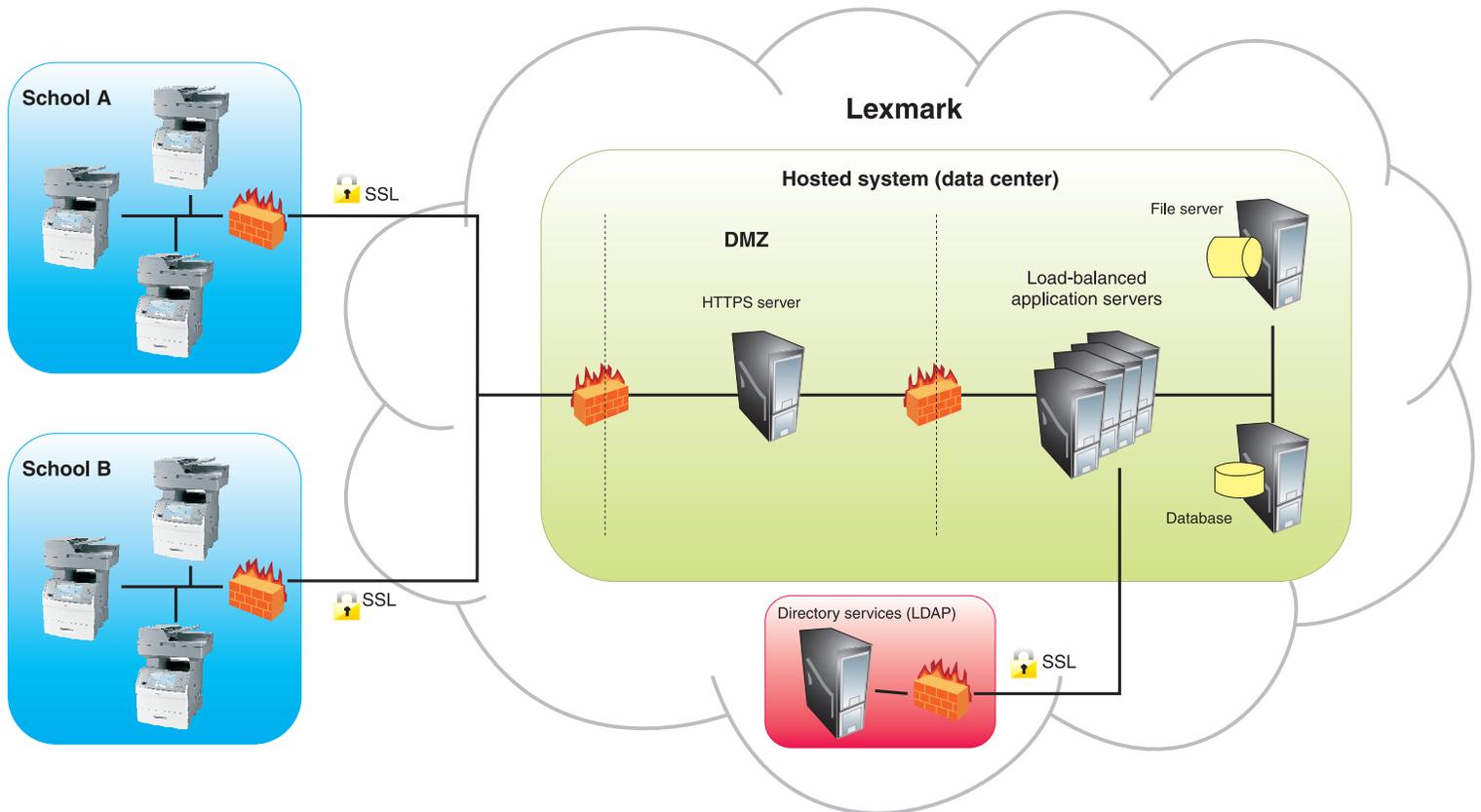


The solution is accessed through applications installed on your printers. Processing is performed using remotely hosted software, which has important advantages:

- No equipment is required besides your Internet-connected, eSF-capable Lexmark MFPs and your existing proxy server.
- The solution requires virtually no maintenance after it is installed.
- The hosted software can be updated without user intervention.
- The small eSF application installed on printers can be easily upgraded.
- You can easily add many more printers after initial implementation.



Solution components



The Hosted Testing and Grading solution contains the following components:

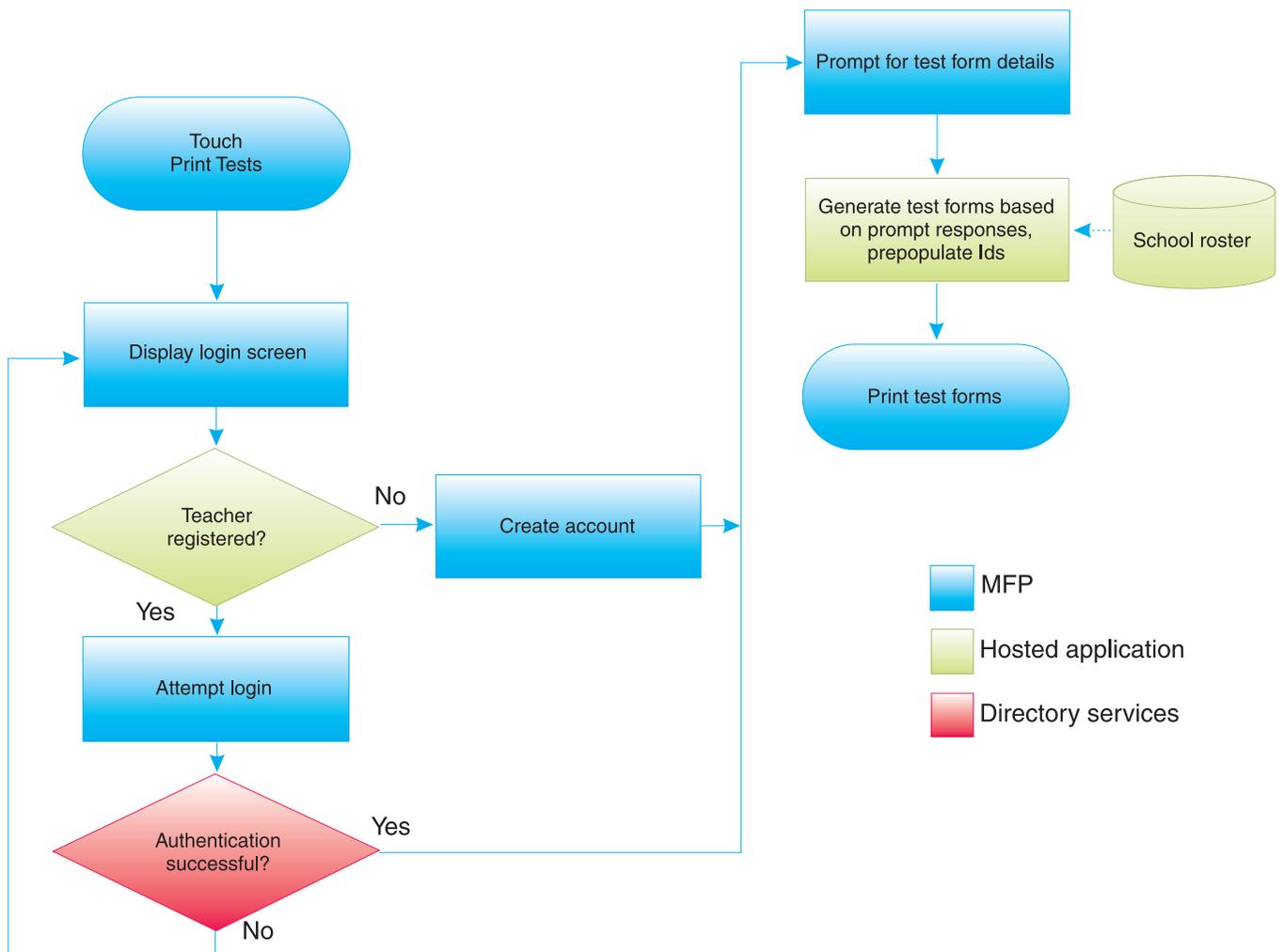
- An application installed on each of your printers that allows users to print and grade test forms and print reports
- Hosted software that provides the following functions:
 - Managing user and device authentication
 - Managing the school roster
 - Creating test forms
 - Providing *optical mark recognition* (OMR) and processing for grading test forms
 - Compiling reports
- An agent installed on some of your printers that synchronizes your school roster with the hosted software

The computers and firewall appliances used by the hosted application are located in a secure and environmentally stable data center that provides third-party managed hosted services. The facility is subject to a yearly SAS 70 Type II audit.

Application flow

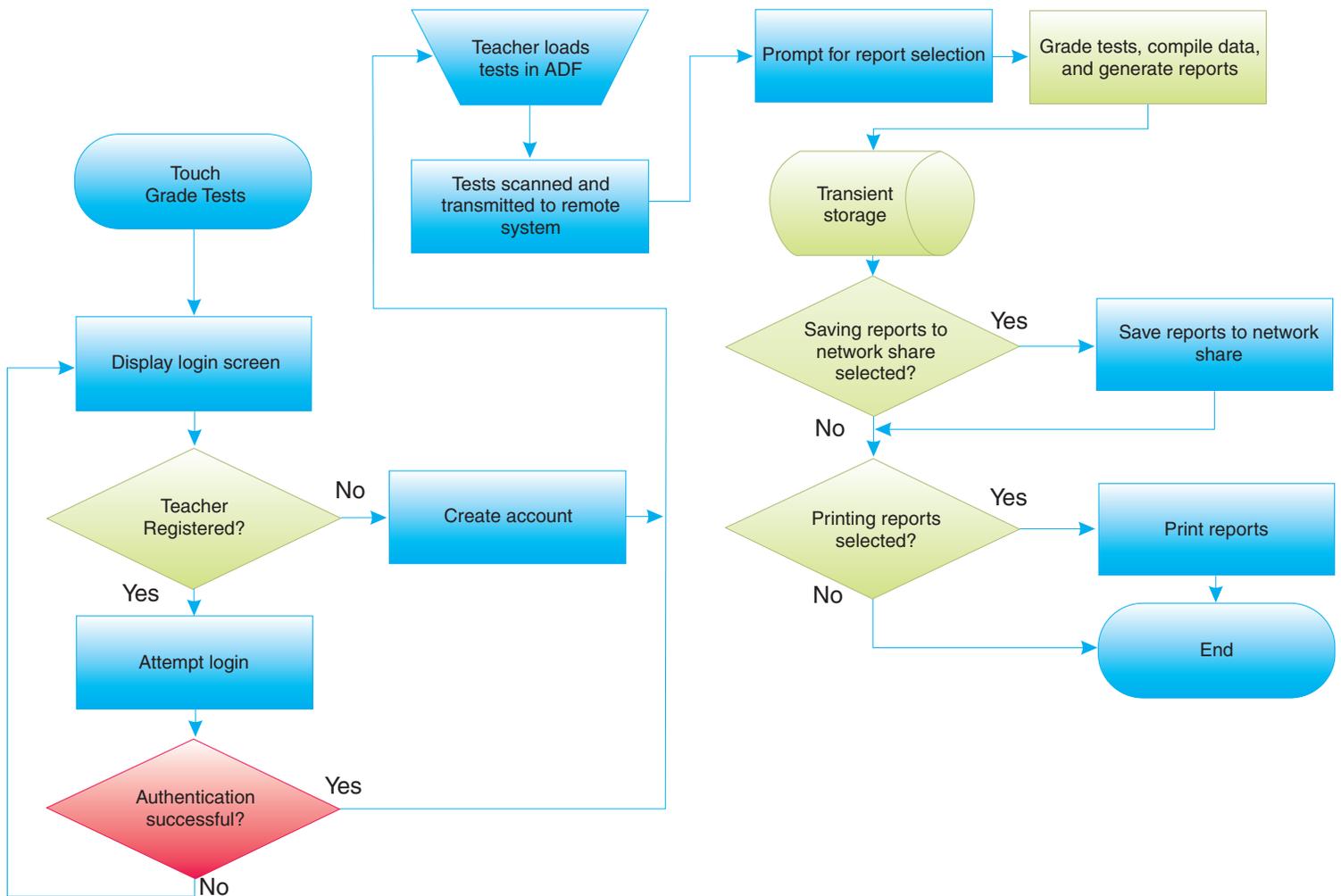
Printing tests

- 1 The teacher touches **Print Tests** on the printer control panel.
- 2 The printer prompts for credentials:
 - If already registered, the teacher enters his or her password and is authenticated by the hosted software.
 - If not already registered, the teacher can register with the hosted software as a new user from the printer control panel.
- 3 The printer prompts for the details of the requested test forms, including the test name and the number of questions to include on the form. Prompts also determine the class for which test forms are being created so that identifying information can be pre-printed for each student. Other prompts and information to include can be customized for your site.
- 4 The details are processed and the test forms are created by the hosted software.
- 5 The printer retrieves and prints the requested forms.



Grading tests

- 1 The teacher touches **Grade Tests** on the printer control panel.
- 2 The printer prompts for credentials:
 - If already registered, the teacher enters his or her password and is authenticated by the hosted software.
 - If not already registered, the teacher can register with the hosted software as a new user from the printer control panel.
- 3 The teacher loads the completed bubble sheets in the *automatic document feeder (ADF)*.
- 4 The printer scans the tests and securely sends them to the remote system for grading.
- 5 The printer prompts for the type of reports desired, whether they should be printed or stored on the network, and any other available delivery options.
- 6 The hosted software grades the tests and compiles the requested reports.
- 7 The grading reports are printed or stored as requested.



How is my data protected when using Hosted Testing and Grading?

Data exchanged with and stored by the hosted application

Data	Sent to the hosted application	Received from the hosted application	Stored in the hosted application database	Temporarily stored on the hosted application file server ¹	Sent from the hosted application to the directory service
Login credentials —The user name and password used by each teacher to log in to the application	X				X
School roster —Contains directory-level information about students (ID and name only), teachers, and classes	X	X	X		
Blank test forms —The empty bubble sheets to be distributed to students. These forms may have identifying information pre-populated.		X			
Completed test forms —The bubble sheets to be graded after the test has been administered.	X			X	
Grading reports ² —Graded tests and compiled data from the graded tests.		X		X	

¹ Files created during grading are stored on the file server for processing and transmission back to the printer. These files may be retained up to a few hours.

² Though grading reports are transmitted from the hosted application through the Internet, the requesting printer manages storing reports on a file server within the school network. Only e-mails containing links are sent from the hosted application, but reports are still saved on the file server. Hence, the school must also have sufficient security to protect data in the file server or multifunction printers that are used to access data.

Information and network security

Lexmark designed the Hosted Testing and Grading solution to comply with data security requirements in a number of ways. Primarily, only the "directory-level" personal data is stored. This data is generally unregulated data that includes student ID, student name, teacher ID, teacher name, and teacher e-mail address. These are the basic elements that are essential for the grading service.

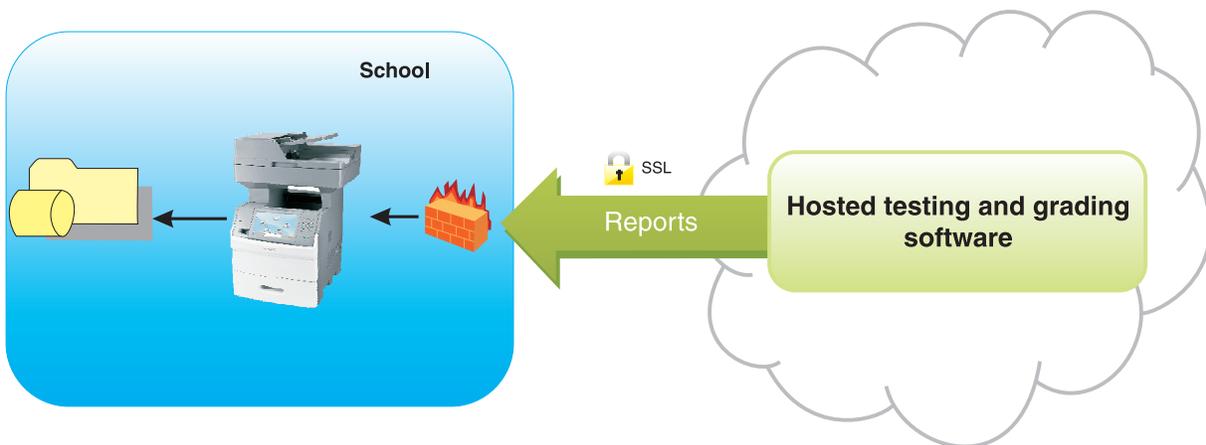
This section explains the technical methods utilized by Lexmark to ensure security of all data exchanged within this system.

Protecting data in transit

The hosted application uses *Secure Sockets Layer* (SSL) technology to protect all data exchanged between printers and the hosted system. When connecting, the printer authenticates the Web server using the server's certificate. The printer and server then negotiate encryption and establish a public key for the printer, paired with the server's private key. All subsequent communication between the server and printer is authenticated and encrypted.

The credentials that a teacher uses to log in to the application are encrypted and sent through the secured connection to the application. The application server communicates with a directory service for authentication. This directory service may be on a separate network, but the connection between the application server and the directory service server is also secured and encrypted.

If grading reports are saved on a file share on the school network, they are encrypted and sent to the printer as normal, and then the printer saves them to the network share through the local network. E-mailed reports are saved to the school network in the same way, and notification e-mails that direct users to the network location can be sent instead of the reports themselves.



Protecting data inside the application

The hosted application is protected by a dual-firewall DMZ, which contains the Web server. The outside firewall allows outside traffic to communicate only with the Web server.

The Web server imposes a filter to allow connections only from the Hosted Testing and Grading application on a Lexmark printer. Once the initial connection is validated, the printer logs in to the server using basic authentication with credentials stored in the local application to confirm that it belongs to a registered school. This authentication is transparent to the user.

All accepted and rejected connections to the Web server are logged. The logs are scanned regularly for suspicious activity.

The inside firewall allows connections to the application server only from the Web server in the DMZ, and the file server and database are only connected to the application server. Thus, no outside traffic can directly access the file server and database where school information is stored. All requests must be authenticated in the DMZ and pass through the application server as part of the normal flow of the application.

In the data center that houses the equipment for the hosted application, the Lexmark network is segregated from other customer networks in the data center, as well as the internal network of the data center itself. Only a physically secured, password-protected management workstation is allowed to interface with the Lexmark network. No inter-client network traffic is allowed. The data center conducts regular penetration testing and vulnerability analysis on the internal network.

The data center provides the following security:

- Monitoring of network traffic for suspicious activity, with immediate notification of Lexmark administrators in the event of a suspected breach
- Monitoring security advisories, forwarding those that may affect the hosted application to Lexmark
- Application of security updates to the operating system on each computer in the hosted system

Physical security and reliability

Protecting the infrastructure of the hosted application

The data center that houses the equipment for the hosted application maintains policies and standard operating procedures to protect data contained in customer systems from unauthorized access, including the following:

- The data center enforces a code of conduct, acknowledged by each employee upon hiring and yearly thereafter, including rules restricting access to customer data to those with a “need to know” and “right to use.”
- Any candidates for employment must be fully qualified for the job opening, and all hires are contingent on a background check, reference check, and drug screening.
- New employees undergo orientation with a focus on confidentiality and security.
- Employees are regularly trained in processes, management of confidential customer information, and emergency procedures, and incentives are offered for advanced training and technical certifications.
- Established policies are enforced in contracts with third-party vendors.
- Physical access to the Lexmark system is only granted to Lexmark employees and third-party contractors pre-authorized by Lexmark, and all access is recorded in a visitor register.
- Security personnel are on duty at all times to control physical access to the facility, together with badge access and forced-entry alarms at outside doors. All entrances and open floor space are monitored by video surveillance. Separate key card access is required for access to equipment areas, and the equipment for the Lexmark system is in a locked cabinet.
- Operations staff are on duty at all times to monitor equipment and escort employees of customers and third-party contractors that have been authorized to enter the facility.
- The facility is subject to a yearly SAS 70 Type II audit.

Maintaining the reliability of the hosted application

The data center provides redundancy and monitoring in all systems to avoid single points of failure:

- The system receives conditioned power with redundant feeds and redundant uninterruptible power supplies with automatic failover. The facility itself is equipped with emergency backup power. The quality of the commercial power supply is monitored, and all failover to uninterruptible power supply batteries and emergency backup power is automatic.
- Temperature and relative humidity are maintained with redundant HVAC systems that can withstand the loss of one air handler and retain full capacity. All computer room air conditioning units are monitored for leaks.
- The system is connected to redundant Ethernet connections. All network equipment that provides Internet connectivity is duplicated, with dual power supplies. The fiber IP backbone has diverse entry points into the building and diverse paths to connected equipment.

Fire protection for the facility includes:

- A very early smoke detection apparatus (VESDA) system, which triggers an operator alarm, alerts the local fire department, and starts a countdown for automatic suppression
- An automatic fire suppression system in the equipment area with manual override available in case of a false trigger
- Fire extinguishers for use of the staff in exiting the building

All systems in the facility are scheduled for periodic preventative maintenance.

Since the printers and file shares reside in a school network, the school is also responsible in keeping the accounts, printers, and downloaded data safe.

Summary

Schools need a cost-effective, low-maintenance, and secure automation solution to respond to increasing needs for testing, assessment, and reporting with limited resources. Lexmark Hosted Testing and Grading prints test forms, grades tests, and compiles grading reports using only Lexmark MFPs and a hosted application, which eliminates the need for specialized equipment and minimizes maintenance.

A robust security architecture protects data. All communication with the hosted application is authenticated and encrypted. The application is protected by a dual-firewall DMZ, including a Web server that only allows connections from authenticated printers with the solution installed. Connections are monitored, and the network is segregated within the data center. Additionally, the data center maintains procedures, policies, and systems that ensure physical security and reliability of the equipment used by the hosted application.