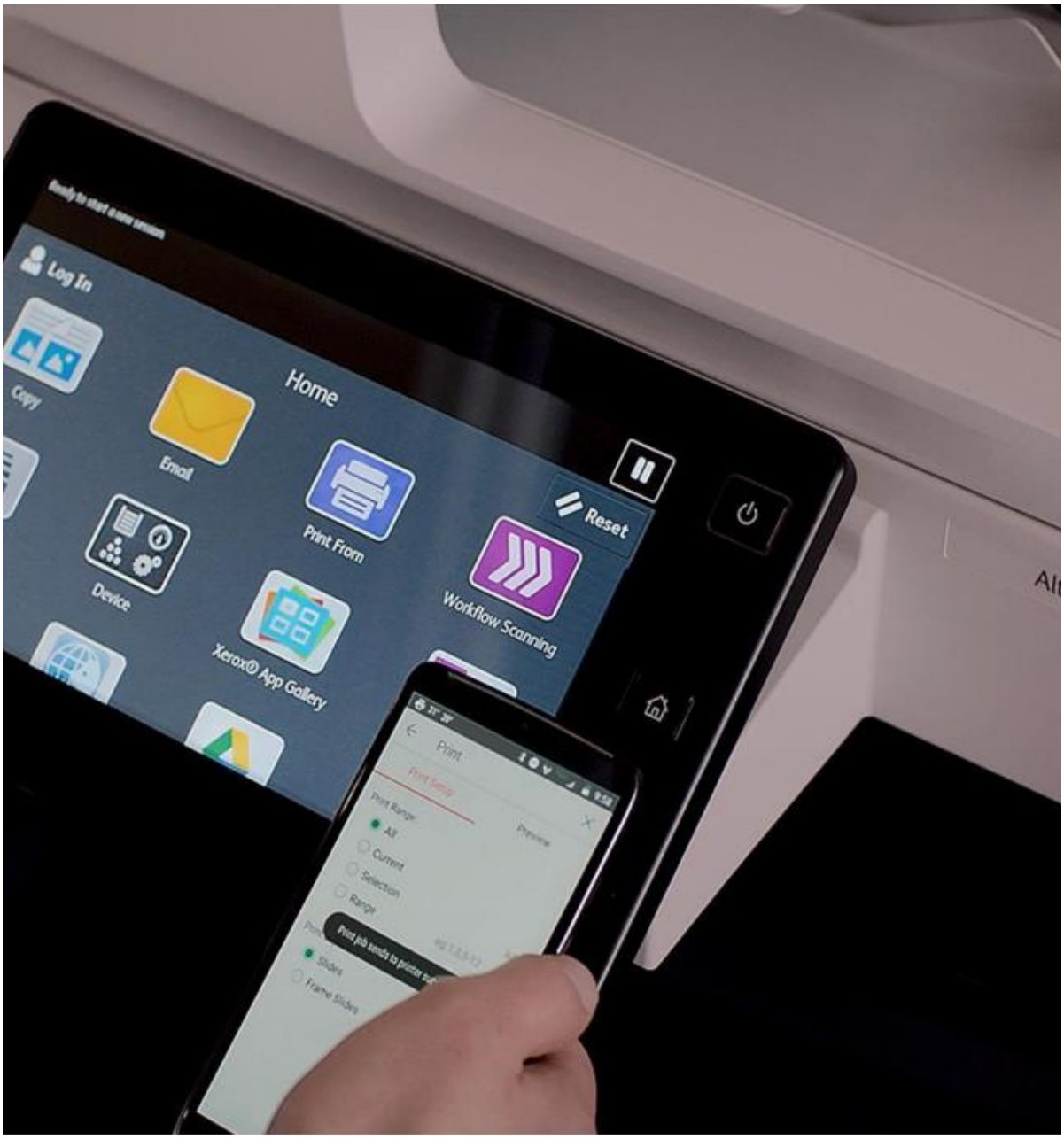
Security Guide

Xerox® Workplace Kiosk App



Document Version: 3.0 (December 2023).

Contents

1. Introduction 5

Purpose 5

Target Audience 5

Disclaimer 5

2. Product Description 6

Overview 6

Workplace Kiosk ConnectKey App 7

Workplace Kiosk Progressive Web App 7

Kiosk Server 8

Workplace Kiosk ConnectKey App Server 8

Workplace Kiosk PWA Server 8

Kiosk Portal 8

Xerox Workplace Suite 9

Stripe 9

SendGrid 9

OpenText XM Fax (Xmedius Fax) 9

System Workflows 10

User Session 10

Payment Processing 10

Job Processing 11

Merchant Onboarding 12

Host Onboarding 12

3. Kiosk Security 14

4. User Data Protection 15

User Data Protection within the Product 15

User Data at Rest 15

Data Persistence 15

User Data in Transit 16

Secure Network Communications 16

Email Signing and Encryption using S/MIME provided by SMTP 16

5. Additional Information and Resources 17

Security Xerox 17

Responses to Known Vulnerabilities 17

Additional Resources 17

1. Introduction

Purpose

The Xerox® Workplace Kiosk App is a ConnectKey App installed on select Xerox ® VersaLink ® Models which enables the device to be used for print, scan, fax, and copy for-pay services. The user accesses the progressive web app (PWA) kiosk interface by scanning a QR code displayed on the device UI with their personal mobile device. The highly secure, cloud-based kiosk is designed to be placed in convenient locations to provide document services for remote workers and people on the go. The kiosk requires a physical network connection.

The purpose of the Security Guide is to disclose information for the Xerox® Workplace Kiosk App with respect to data security when using the app. Data security, in this context, is defined as how data is stored and transmitted, how the application behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes design, functions, and features of the Xerox® Workplace Kiosk App relative to Information Assurance (IA) and the protection of customer sensitive information. Please note that the customer is responsible for the security of their network. The Xerox® Workplace Kiosk App does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity, or Xerox® Workplace Kiosk App features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

This document should be read in conjunction with the Security Guides of the Xerox ® Device upon which the Xerox Workplace Kiosk App is installed and the Xerox ® Workplace Suite.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security. It is assumed that the reader is familiar with the apps; as such, some user actions are not described in detail.

Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. Product Description

Overview

Xerox® Workplace Kiosk App consists of the following components:

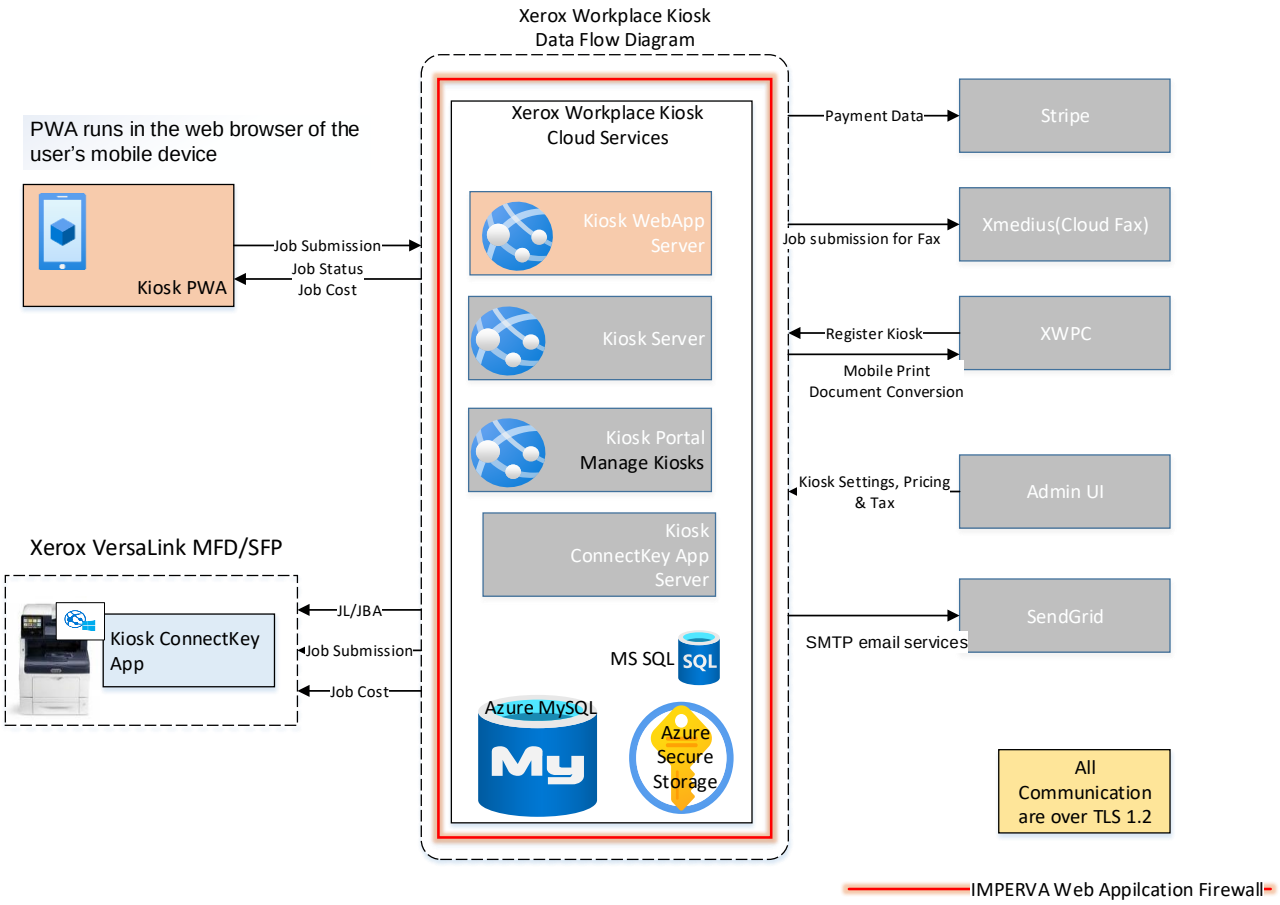
- Workplace Kiosk ConnectKey app which is installed on select Xerox VersaLink multi-function or single function devices. (Hereafter referred to as MFDs.)
- A Progressive Web App (PWA) which runs in the web browser of the user's mobile device.
- A cloud-based Kiosk server, which enables communication between the ConnectKey app and the PWA, and implements various kiosk features.
- A cloud-based Workplace Kiosk ConnectKey app server which hosts the app.
- A cloud-based server which hosts the PWA.

The Xerox® Workplace Kiosk App utilizes the following existing services as part of its solution:

- Xerox Kiosk Portal – Used to manage kiosks
- Xerox Workplace Suite – Used to enable the email to print workflow.
- Stripe – Provides payment services
- SendGrid – Provides SMTP email services
- Xmedius (OpenText XM Fax) – Provides Fax services

All Xerox cloud components (kiosk server, ConnectKey app server, PWA server, portal) are hosted in Microsoft Azure and are secured via TLS. All public access to these components are protected by the Imperva Web Application Firewall. A secondary instance of all services as well as a mirrored database are hosted in another geographic region in case failover is required.

The following illustrates the Workplace Kiosk architecture and components.



Workplace Kiosk ConnectKey App

The Workplace Kiosk ConnectKey app leverages ConnectKey Xerox Extensible Interface Platform (EIP) technology to execute copy, print, scan to email and fax jobs on the device. The ConnectKey app communicates with the kiosk server through REST and SOAP based APIs and a web socket connection to enable bidirectional communications. All interfaces use https encrypted communications.

Workplace Kiosk Progressive Web App

The Workplace Kiosk Progressive Web App is accessed by the user by scanning a QR code displayed on the MFD UI, with their personal mobile device. The user enters payment information and initiates jobs through the PWA. Payment information and ApplePay and GooglePay are handled by Stripe through an embedded iFrame within the PWA web page. All payment information is handled through Stripe's PCI DSS compliant APIs. The Xerox portion of the app never handles any of the user's payment information. The PWA communicates with the kiosk server through REST API calls. All interfaces use https encrypted communications.

Cookies are used to maintain the destination email address for the email workflow if enabled by the user.

Kiosk Server

The kiosk server manages the user session and provides a communication conduit between the PWA and the device. It computes job pricing and sales tax and manages the session total. It manages the payment session with Stripe through Stripe's PCI DSS complaint API. It forwards PWA job requests to the ConnectKey app and receives job execution status from the ConnectKey app. It collects usage data that allows kiosk owners and program management to assess the performance of their business and stores that data in a database. None of that data includes personally identifiable information (PII) of the user. It communicates with Xerox Workplace Suite to implement the print from email workflow. All interfaces use https encrypted communications. Clients must provide a session based shared secret to access the APIs implemented by this server.

The kiosk server logs debug information or sends email notifications to the Workplace Kiosk administrators when an unexpected event occurs on the server. Neither the logging nor the email notifications captures PII.

Workplace Kiosk ConnectKey App Server

The Workplace Kiosk ConnectKey App server hosts the pages of the application. This component does not store any data nor hosts any APIs.

Workplace Kiosk PWA Server

The Workplace Kiosk PWA server hosts the pages of the PWA application. In addition to hosting the PWA pages, the server manages and temporarily stores documents used in the browse to print workflow. Clients must provide a shared secret to access APIs implemented by this server.

Kiosk Portal

The Kiosk Portal provides kiosk management facilities. It allows the kiosk owner to specify pricing for jobs run on their kiosk and the taxes that should be collected. The portal allows kiosk owners and Xerox management to look at or run statistical reports that allows them to assess the performance of their business. None of these reports contain PII of the customers.

The portal collects limited PII (email address and names) related to merchant or host administrators that need access to the portal to manage the business. This data is only available to authorized portal administrators.

Access to the portal is controlled through a username (email address) + password login. The password must be a minimum of 14 character with a combination of upper and lowercase letters, numbers and special characters. The account locks and the password must be reset after 6 failed login attempts.

The kiosk server communicates with the portal via REST APIs to retrieve kiosk information from the database or store kiosk usage information into the MySQL database. All interfaces use https encrypted communications. Clients must provide a shared secret to access the APIs implemented by this server. The Azure GRS is enabled for the MySQL database.

Xerox Workplace Suite

The Workplace Kiosk App leverages the document storage and conversion capabilities of Xerox Workplace Suite to implement the print to email workflow. The kiosk server communicates with Xerox Workplace Suite via REST APIs to verify the release code + email address combination, to initiate conversion of the document and to retrieve the url of the document. All interfaces use https encrypted communications. Clients must provide appropriate credentials to access the APIs implemented by this server.

Stripe

Stripe is an industry leading PCI DSS certified provider of payment services. The PWA and kiosk server complies with the requirements of the Stripe APIs to maintain secure payment workflows. Clients must provide appropriate credentials to access the APIs implemented by Stripe.

SendGrid

SendGrid is an industry leading provider of SMTP relay services. Communication with the server is through standard SMTP protocols. The client must provide appropriate credentials to connect to the server.

OpenText XM Fax (Xmedius Fax)

OpenText™ XM Fax™ is a cloud-based digital fax solution which provides fax transmission services for the Xerox Workplace Kiosk app. XM Fax is ISO 27001, PCI DSS, CSA Star level 1 certified. All interfaces use https encrypted communications. Clients must provide appropriate credentials to access the APIs implemented by this server.

System Workflows

User Session

The user session starts when the user scans the QR code and enters their payment information and typically ends when the user explicitly checks out. The system prevents other users from joining the same user session by doing the following:

- The QR code includes a unique randomly generated session key that changes at each session boundary. The session key is also changed every 10 minutes while the system is idle. If the user attempts to scan a previously displayed QR code or reload the url from a previous session, an error occurs since the session key does not match and the session is not started.
- The system allows only one user in a session at a time. If 2 or more people scan the currently displayed QR code, the first person to enter valid payment information will control the session. Subsequent users will be prevented from entering the session even if they enter valid payment information.

The system ensures that every user session will end and transaction will be finalized by trying to detect if the user abandoned the session or some other error occurred which prevented the user from ending the session properly. In addition to an explicit user checkout, the following conditions will result in the session ending:

- User hasn't responded to a user prompt displayed in the PWA (e.g., job cost approval, start next job) for more than 1 minute.
- The PWA has disconnected from the session for more than 1 minute and no job is currently in progress. A disconnect can occur for a number of reasons including the user closing the PWA browser tab or the user device losing network connectivity.
- The websocket connection to the ConnectKey app disconnects for more than 1 minute. A disconnect can occur for a number of reasons including the VersaLink device losing network connectivity, the VersaLink device being powered off or rebooted, or the user pressing the home button and then Reset.
- The ConnectKey app reloads. A reload can occur for a number of reasons, including the user pressing the Home button, then reset, then the Workplace Kiosk app icon, or the VersaLink device system timer expiring,
- The session has lasted more than 30 minutes.

Payment Processing

The system ensures that payment for jobs executed on the device will be received by preauthorizing a merchant configured amount on the user's payment card. When the session ends, the amount of the charge is finalized and the user receives a refund for the amount of the preauthorization not utilized.

If the user approves the cost of a job that would result in the cart total exceeding the current preauthorized amount, the user is asked if it is OK to increase the current preauthorization. If the increase is successful, the previous authorization is cancelled and the session continues. If the increase is unsuccessful, the user is asked if they want to enter a new card.

In order to support increasing the authorization on the user's payment card, the payment method is temporarily stored in Stripe using a temporary user account. When the session ends, this user account is deleted. This temporary user account is never accessed outside of the session in which

it was created, even if something prevented the account from being deleted at the end of the session.

All payment processing is performed using Stripe's PCI DSS certified APIs. All references to user payment methods and transactions are made through a tokenized Stripe identifier. These identifiers can only be used in conjunction with the Xerox Stripe secret key. The only identifiers stored by Xerox are the transaction IDs that are displayed on the customer receipt and merchant account IDs that are required to perform transactions on the merchant's behalf. All IDs are encrypted in the database.

If the transaction involves a kiosk that has a revenue share arrangement with the host, the revenue share amount is transferred to the Xerox platform account and held until a payout is made. Payouts are performed monthly based on the previous month's transactions. A running total of the amount owed to each host is maintained in Stripe. A payout is made if a minimum payout amount has been accurred less payout fees. If a payout is made, the money is transferred to the host account and immediately paid out to the host's designated bank account. If a payout is not made, the accured revenue rolls over to the following month.

Job Processing

For each job initiated, the user presented the estimated cost of the job based on the scanned images for copy and scan jobs and the decomposed images for print jobs. If the user approves the job cost the job is then processed. If the user cancels the job after cost approval, the job cost is adjusted based on the delivered output. If the system cancels the job due to a system error (e.g., couldn't reach the SMTP server), the user is not charged for the job. The user is never charged more than the estimated cost of the job.

Copy Job Processing

The system uses the MFD's native copy job service to process copy jobs. Copy job data is never transmitted off of the device.

Email Job Processing

The system uses the MFD's native email job service to process email jobs. Email jobs are sent to SendGrid for routing to their final destination. The SendGrid account used to process emails is configured to not save sent emails so user documents typically only reside on the SendGrid server long enough to forward the document to the recipient mailbox. The user is not able to personalize the email subject or message body so no user information is contained in the message itself. A log of the transmitted emails is retained on the SendGrid server for up to 7 days in case a messaging problem needs to be investigated. The only user data retained in this log is the recipient email address.

Browse to Print Job Processing

When the user initiates a browse to print job the selected document is converted and temporarily stored on the PWA server in encrypted blob storage. The document is then retrieved by the MFD. The document is automatically deleted from blob storage as soon as the user session has ended or after 15 minutes, whichever comes first.

Email to Print Job Processing

Users submit documents they want to print via email to the XWPC where they are securely stored and converted into printable format. A six digit release code is returned to the user via email for use during the kiosk session. The user must enter the six digit release code and the first three

characters of the email address used to submit the document to print the document during their kiosk session. The release code is valid for up to 3 days and any document that is printed is deleted after 24 hours. If the document is not printed after 3 days it is automatically deleted.

Fax Job Processing

Fax jobs are processed and transmitted by XM Fax. Each merchant must purchase their own XM Fax account to offer fax services on their kiosk.

When a user initiates a fax job, the system initiates a scan job on the MFD which files a PDF document to the kiosk server, which then forwards the file to XM Fax for transmission using the kiosk owner's XM Fax account credentials. When the transmission is complete, a transmission report is sent to the user via email.

The kiosk owner's XM Fax account should be configured for Zero Retention policy. This policy ensures fax images are deleted immediately after fax delivery. Note, however, that during transmission and while the job is waiting for transmission, the XM Fax account owner (i.e., the kiosk owner) can log into the account and view the fax document.

Print From PC Job Processing

Kiosk owners may optionally enable a Print from PC workflow to support a more traditional print workflow for their users. This capability is normally only enabled in libraries or other environments where the kiosk owner is supplying the PC and can ensure the PC is properly configured.

In the Print from PC workflow, users can submit print jobs using the normal File->Print mechanism. The print driver is configured to submit only Secure Print jobs and users are required to enter a PIN during the submission process. The kiosk is configured to only accept print jobs from these selected PCs through IP filtering. Submitted jobs are held on the kiosk until released by the user by entering their PIN.

During the user's kiosk session, the user may select Print from PC to access the list of documents that were submitted to the device. The user is prompted for the PIN when attempting to release the document for printing. Documents not released after the kiosk administrator configured maximum hold time are automatically deleted. (Usually < 8 hours.)

Merchant Onboarding

In order for Xerox to process transactions on behalf of a kiosk owner (merchant) through Stripe, the merchant must establish an account with Stripe. The Stripe onboarding process is fully handled by Stripe through their website. During the Xerox merchant onboarding process, the merchant administrator receives an email asking the merchant to establish an account with Stripe. The link contained within that email goes to the Stripe website. The only data Xerox receives from that process is the merchant's account ID.

The account only allows transactions for kiosk purchases, with proceeds going to the merchant less any fees or revenue share arrangements made by the merchant. Payouts from that account are controlled by the merchant through Stripe.

Host Onboarding

If a revenue share arrangement has been made between the kiosk owner and the host, the host must establish an account with Stripe. The Stripe onboarding process is fully handled by Stripe

through their website. During the Xerox Host onboarding process, the host administrator receives an email asking the host to establish an account with Stripe. The link contained within that email goes to the Stripe website. The only data Xerox receives from that process is the host's account ID.

The account only allows transfers from the Xerox platform account into the host account. Xerox can trigger payouts from the host account but only to the host designated bank account.

3. Kiosk Security

An MFD installed with the Workplace Kiosk App is likely to be in a publically accessible location so that customers can perform their own jobs. The MFD requires a network connection with Internet access. The customer must have a mobile device with either cellular or wifi internet access. For wifi access, the customer and the MFD do not need to be on the same network.

To prevent users from bypassing the kiosk pay for use requirement, the MFD must be properly configured. The system uses the MFD's native security mechanisms to implement the required security. The kiosk owner must do the following to properly secure the device:

- Use a network firewall to prevent unauthorized users from accessing the device.
- Use MFD IP filtering to further restrict access to the device to only select PCs on the network. Ideally, all access is restricted.
- Disable all print job submission mechanisms including AirPrint, Google Cloud Print, Mopria, IPP, LPD and Port 9100.
- Configure all apps as hidden except the Workplace Kiosk App, Jobs App and Device App.
- Restrict access to the Jobs App and Device App to require administrator login.

4. User Data Protection

User Data Protection within the Product

The Xerox® Workplace Kiosk components are hosted on the Microsoft Azure Network. Microsoft's Azure data center operations feature comprehensive information security policies and processes using standardized industry control frameworks, including ISO 27001, SOC 1, and SOC 2.

For a full description, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security.

For more information regarding user data protection provided by the Xerox® Multifunction Device, please reference your specific model's Security Guide.

User Data at Rest

Data Persistence

Print Jobs

Files selected for print in the browse to print workflow are temporarily persisted in encrypted blob storage for a maximum of 15 minutes. The file is retrieved by the MFD through a 50 character randomly generated filename.

Azure blob storage is encrypted using 256-bit AES encryption, and is FIPS 140-2 compliant.

See the Xerox Workplace Suite security guide for security information regarding documents submitted via the print my email workflow.

Print from PC jobs are temporarily held on the MFD until released by the user or until the maximum hold time is reached, whichever comes first. The file cannot be accessed without the user entered PIN.

Email Jobs

Documents scanned and emailed by the user are sent to SendGrid for routing to the final destination. The SendGrid account used to process emails is configured to not save sent emails so user documents typically only reside on the SendGrid server long enough to forward the document to the recipient mailbox.

Email addresses entered by the user for scan to email are not saved by Workplace Kiosk. The destination email address is maintained in SendGrid for up to 7 days to allow mail send problems to be investigated.

Merchant Account Information

Merchant administrator information (e.g., email address) and merchant and kiosk physical address are stored in the kiosk database. This data is encrypted in the database.

Fax Jobs

Documents scanned and sent as faxes are temporarily stored on the Kiosk server and then forwarded to XM Fax, before being transmitted to the fax destination. The scanned document resides on the kiosk server until the document is transferred to XM Fax. It is then deleted. The document stays on the XM Fax server until it is successfully transmitted to the fax destination. If the initial transmission attempt fails, the XM Fax server will wait a configured amount of time and retry the transmission a configured number of times.

User Data in Transit

Secure Network Communications

The Xerox® Workplace Kiosk EIP app and API require that the device can communicate over port 443 outside the client's network. All communication between all aspects of the application, including, but not limited to the PWA, ConnectKey app, XIPK portal, database, encrypted blob storage, Kiosk server, Xerox Workplace Suite and Stripe are encrypted using HTTP Secure (TLS).

Email Signing and Encryption using S/MIME provided by SMTP

The product uses SMTP to transmit data to the email server. Email authentication, encryption, and signing are utilized.

5. Additional Information and Resources

Security Xerox

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in the discovery and remediation of vulnerabilities in Xerox® Software and Hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Additional Resources

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/

Table 1 Security Resources