SHARP
Be Original.

Security White Paper
Synappx™ Cloud Print

Contents

Synappx Cloud Print Security White Paper

1. Introduction

Overview

Synappx Application Services help bring smarter office experiences. They are designed to help optimise hybrid collaboration experiences. Synappx application services are protected by a robust, layered security system that ensures the system, and its components are not opening points of vulnerability for your data or networks. Through a combination of world-class technology providers including Microsoft Azure, Google Workspace and security best practices, your use of the Synappx application services helps keep your information safe and secure while helping you enhance productivity in your office.

Security provisions related to Synappx application services are described in this white paper.

Synappx Cloud Print

Synappx Cloud Print leverages the Azure cloud and rich client technologies to help users increase productivity and work efficiently. Synappx Cloud Print is a full agentless cloud print management solution for Sharp multifunction printers (MFPs). It provides convenient and time-saving features including scanning to favourite destinations, secure print release, printing cloud files and copying on Sharp MFPs throughout your office. Synappx Cloud Print users can also use their mobile devices, allowing them to print any cloud corporate document as well as any document located in the mobile device's local storage. Synappx Cloud Print cloud software and services leverage the Microsoft Azure database, device provisioning and many other services.

2. Synappx Application Services

Synappx Application Services leverage the Microsoft Azure cloud platform services as a foundation. Microsoft Azure is a highly respected global cloud service with a wide range of features that are used by the Synappx applications, including the Azure Cosmos database, storage, several IoT Services, Key Vault, Security Centre monitoring, backup and more.

Synappx Application Services are hosted in secure Microsoft data centres located in the West Germany region. Microsoft Azure cloud and data centres are protected through Microsoft's security practices and are fully GDPR compliant. Each data centre provides local data redundancy. In addition, all communication between Synappx client applications and Synappx Application Services (hosted in Microsoft Azure) are encrypted via HTTPS (TLS v1.2, AES256), or secured through X.509 certificates, when using MQTT or MQTT Over WebSocket, AMQP or AMQP Over WebSocket (used by the MFP and Display Agent). Synappx Cloud Print does not store print documents in the cloud, only print related metadata.

Synappx Cloud Print services are accessed via a secure web portal and do not require a client application. Software licences are issued by the system which can be associated with each Sharp MFP & printer that the customer wishes to manage with a secure licence key between the MFP and the cloud application. After purchasing a Synappx Cloud Print licence, the licence is assigned to a unique MFP discovery by the administrator in the customer's local network. Synappx Azure database access is limited to whitelisted IP addresses from secure Azure App Services. Microsoft Key Vault is used for storage of SSL certificates, X.509 signing certificates, private keys, and other content requiring the highest security. Access to Microsoft Azure Key Vault is limited only to authorised Sharp service principals and system users with necessary access permissions.

The customer specific data used for the Synappx Cloud Print applications stored in the secure Azure cloud databases includes the following:

Common to all Synappx Cloud Print Application:

- Users first name, last name, email address (imported from Entra ID, formally Azure AD) or Google Workspace to Synappx by Admin) and IP address
- Administrator users first name, last name, and email address (imported from Entra ID) or Google Workspace to Synappx by Administrator)
- Automatic PIN generation for each user and administrator to authenticate and unlock the MFPs
- Card / badge ID created for each user and administrator to authenticate and unlock the MFPs
- Company domain aliases from Entra ID and Google Workspace
- Application usage data used to generate reports for customer use
- Synappx licence data (e.g., expiration)
- System and Administrator logs (including date and time for log events)
- MFP information (model name, IP address, serial number) discovered via Admin initiated SNMP discovery or manually added

Synappx Cloud Print Windows Client Specific:

- Users first name, last name, email address (imported from Entra ID) or Google Workspace
- Token key for SSO between Entra ID or Google Workspace

Data in Synappx databases is only accessible to active customers via the Synappx Cloud Print administration portal and limited authorised Sharp staff required for support purposes.

Overall, Sharp governance of the Synappx Application Services limits system access to minimal authorised staff for deployment and support purposes only. See Sharp security policy sections for more details.

For more information on Microsoft Azure security, see the following links related to features used by Synappx Application Services:

- Overview: https://docs.microsoft.com/en-us/azure/security/security-white-papers
- Data Encryption at Rest: https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest
- Azure Network Security: https://docs.microsoft.com/en-us/azure/security/security-network-overview
- Azure Functions and Serverless Platform Security: https://docs.microsoft.com/en-us/azure/security/abstract-serverless-platform-security
- Azure Storage Security Guide: https://docs.microsoft.com/en-us/azure/security/security-storage-overview
- Security Management in Azure: https://docs.microsoft.com/en-us/azure/security/azure-security-management
- Azure Management-Governance: https://docs.microsoft.com/en-us/azure/governance/

3. Synappx Cloud Print Administrator Portal

Administrators access, configure, and manage the Synappx Cloud Print services through the Synappx Administrator Portal web pages. Managing users, MFPs and Printers, security rules, additional Admins and more are performed via these secure web pages. The administrator performs Licence management via the Administrator Portal and licence status where applicable can be reviewed. The administrator can view and run analytics reports to gain insight into their print usage. Other reports, for example System, Administrator and Check-in logs can be downloaded for further analysis.

Synappx Cloud Print Supported Domains

For Microsoft 365 and Google Workspace accounts, Synappx Cloud Print services collect information from the domain aliases supported in the account's EntraID or Google Workspace system. For Microsoft 365 accounts, in the Admin Setting/Supported Domains web page, if the Azure Global Admin does initial permission opt in.

Currently Synappx Cloud Print supports only the primary domain and not secondary domains.

User Authentication

Synappx Cloud Print services leverage Microsoft 365 or Google Workspace user credentials to avoid having to set up, manage and protect separate Synappx user database. By design, Synappx Application Services do not have access to Microsoft 365 or Google Workspace customer passwords. The system leverages Azure Active Directory or Google Workspace Directory and relies on authentication tokens to identify Administrators and users. User identity is confirmed with your Microsoft Entra ID (for Microsoft 365 accounts) or Google Workspace Directory (for Google Workspace accounts) using a secure identity partner Auth0 and these user passwords are never stored in Synappx or Auth0 systems. The Synappx platform securely stores the user email address, IP address and first/last name only. No other personally identifiable information about the user is known or stored by the Synappx system. Auth0 has many certifications for cloud security including: ISO27001, ISO27018, SOC 2 Type II, HIPAA BAA, Gold CSA STAR, GDPR compliance and more.

For more information about Auth0 and security provisions, please see: https://auth0.com/security/

Roles Based Access

Access to the Synappx Administrator Portal and Synappx applications are controlled using tenant-based and role-based authentication processes. The first Administrator, details provided by the customer, is identified as part of the purchase order process. Additional Administrators can be added after successful log-in to the Synappx portal and acceptance of the terms of use and privacy policy by the first Administrator.

Only Administrators designated or assigned by the customer can access, configure, licence, and manage Synappx service users and workspaces, view reports, etc. from their account via the secure web portal. All communications with the Admin Portal are via HTTPS/SSL (TLS1.2) port 443 to protect data in transit.

Administrator User Types:

- Primary Admin: The first administrator who is only one person in one tenant. This user role has the same privileges as an administrator.
- Administrator: This user role can manage users, roles, licences, and data entities such as workspaces, MFPs, and agents. Also, this user role can see Administrator log, System log and Analytics reports.

User Types:

- User: This user role can access Synappx Windows Client, Synappx User Portal and Synappx Cloud Print mobile application.

Administrators and Users can use their normal Microsoft 365 or Google Workspace credentials to access Synappx Services once added to the system and their account is activated by the administrator.

Granting Synappx Cloud Print Services Privileges

Microsoft 365 Users

To use Synappx Cloud Print services including Administrator Portal, Windows Client and Cloud Print Mobile application, the user is required to grant permissions shown in the table below. Permission consent screen is shown for every user for the first-time log-in or in-line with the customers company security authentication polices.

Permissions Requested	Definition	Admin Portal	Cloud Print Windows PC Client	Cloud Print Mobile
Microsoft Graph:				
• Calendars.ReadWrite.Shared	Allows the app to create, read, update (e.g. extend time) and delete events in all calendars the user has permissions to access. This includes delegated and shared calendars.	No	No	No
• User.Read	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	Yes	Yes	Yes
• Directory.Read.All	Allow the app to read sub domains.	Yes*	No	No
• Files.ReadWrite.All	Allows the app to read, create, update, and delete all files the signed-in user can access.		Yes	Yes
• Group.Read.All	Allows the app to list groups, and to read their properties and all group memberships on behalf of the signed-in user. Also allows the app to read calendar, conversations, files, and other group content for all groups the signed-in user can access.	Yes*	No	No
• People.Read	Allows the app to read a scored list of people relevant to the signed-in user. The list can include local contacts, contacts from social networking or your organisation's directory, and people from recent communications (such as email and Skype).	No	No	No
• Team.ReadBasic.All	Allows app to get a list of Teams to retrieve documents for the user to share.	No	No	Yes
• User.Read.All	Allows the app to read the full set of profile properties, reports, and managers of other users in your organisation and locations on behalf of the signed-in user.	Yes*	No	No

• User.ReadBasic.All	Allows the app to read a basic set of profile properties of other users in your organisation on behalf of the signed-in user. This includes display name, first and last name, email address, open extensions, and photo. Also allows the app to read the full profile of the signed-in user.	Yes	No	No
• offline_access	Allows the app to read and update user data, even when they are not currently using the app to keep log in state,	Yes	Yes	Yes
• email	Allows the app to read your users' primary email address.	Yes	Yes	Yes
• openid	Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.	Yes	Yes	Yes
• profile	Required to obtain user profile information (e.g. user first and last name, email address) from EntraID (previous Azure AD).	Yes	Yes	Yes
• Mail.Read (Category: Application)	Allows the app to read mail in all mailboxes without a signed-in user	Yes	No	No
• Mail.ReadWrite (Category: Application)	Allows the app to create, read, update, and delete mail in all mailboxes without a signed-in user. Does not include permission to send mail.	No	No	No

* These permissions are optional. On the Administrator Portal, the Azure Global Administrator can grant global permission shown in the table below. If the permissions are granted, the following features can be available:

・Group search for users and workspaces

・Automatically sub-domains are listed in the "Supported Domains" page. This page is available for future evolution of the service. Today is only the primary domain is supported.

Permissions Requested	Definition
Microsoft Graph:	
• Directory.Read.All	Allows the app to read data in your organisation's directory, such as users, groups, and apps.
• Group.Read.All	Allows the app to list groups, and to read their properties and all group memberships on behalf of the signed-in user.
• User.Read.All	Allows the app to read the full set of profile properties, reports, and managers of other users in your organisation, on behalf of the signed-in user.

Google Workspace Users

To use Synappx applications including Administrator Porta, Windows Client and Cloud Print Mobile application, the user is required to grant permissions shown in the table below. A permission consent screen is shown for every user for the first-time logging in.

Google API Scopes Requested	Definition	Admin Portal	Cloud Print Windows	Cloud Print Mobile
https://www.googleapis.com/auth/admin.directory.domain.readonly	Allows the app to read domain information for supporting multi-domain feature.	Yes	No	No
https://www.googleapis.com/auth/admin.directory.group.readonly	Allows the app to retrieve group, group alias, and member information to add groups via the Admin Portal.	Yes	No	No
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly	Allows the app to retrieve calendar resources to add workspaces via the Admin Portal.	No	No	No
https://www.googleapis.com/auth/admin.directory.user.readonly	Allows the app to retrieve users or user aliases to add users via the Admin Portal.	Yes	No	No
https://www.googleapis.com/auth/calendar.readonly	Allows the app to have read-only access to Calendars.	No	No	No
https://www.googleapis.com/auth/calendar.events	Allows the app to have read/write access to events on a calendar and update it (e.g. extend the meeting time).	No	No	No
https://www.googleapis.com/auth/drive	Allows the app to have access to authorised user's Google Drive files (excluding the Application Data folder) to list files.	No	No	Yes
https://www.googleapis.com/auth/directory.readonly	Allows app to see and download your organisation's Google Workspace directory	No	No	No
https://www.googleapis.com/auth/userinfo.profile	Allows app to use personal information user has made publicly available to get username and avatar image.	Yes	Yes	Yes

However, the following features are unavailable until the custom role is assigned to the user.

・Group search for users & workspaces

・Automatically sub-domains are listed in “Supported Domains” page. This page is available for future evolution of the service. Today is only the primary domain is supported.

Custom role requires the permission shown below which can be set from the Google Admin page.

・Admin API privileges – Users.Read, Groups.Read, Domain Management

Importing Users or from EntraID (previous Azure AD) or Google Workspace

Administrators can directly import users for Synappx Cloud Print from Microsoft 365 (EntraID) or Google Workspace. Manual entry of users is also permitted. Since Synappx Cloud Print licensing is per MFP users in the supported domains and in Entra ID or Google Workspace can be added and activated/deactivated without any licence required. Communications with Microsoft Azure and Google Workspace for User import is via HTTPS (port 443). Users with Microsoft 365, Google Workspace can also be manually added by searching the user-directory. The procedure how to import users is covered on the Admin Guide:

Synappx Cloud Print Analytics Reports

Synappx helps Administrators understand and streamline their print usage. Data generated in the Synappx reports is stored on secure Microsoft servers. User usage specific information in the reports is only available to Administrators and others within the customer via the analytics pages. An anonymised summary data about customers' service usage is available to Sharp for purposes of support and product enhancement over time. When the Customer stops the Synappx Cloud Print Services, the data is retained for 45 days after the service is terminated by the customer to allow time to renew the services. After this gray period, all data associated with the customer tenant is deleted and cannot recover. See Sharp Corporate Security, and Sharp Privacy Policy for more details.

Synappx Cloud Print System Logs, Admin Logs

Synappx Cloud Print includes a System Log containing information about system events. These include conditions that might require Administrator intervention to correct an issue or perform troubleshooting. System logs can be exported by Admins as a .CSV file for further analysis. System logs are retained by the Synappx system for 30 days.

There is also an audit log that contains information about Admin interactions with the Admin Portal. Because multiple Admins can be assigned and provided access to the Synappx Admin Portal, this log captures major actions taken by the admins. Admin Logs can also be exported as a .CSV file for analysis. Admin logs are retained by the Synappx System for 90 days.

Synappx Cloud Print Zero Trust Architecture Design

Synappx Cloud Print is secure by design. Sharp has implemented a Zero Trust Design, which is a security framework that requires all users, whether in or outside the SME's network, to be authenticated, authorised, and continuously validated for security compatibility before being granted access to applications or data.

There are several components that comprise this approach, first, all authentication and identity management is managed through an Active Directory, which essentially means the user is authenticating to the solution using their network assigned authentication. Identity Management is in the Cloud and today Synappx Cloud Print is connected with Entra ID (Azure AD) or Google Workspace, which is inherently secure.

Secondly, only metadata concerning the print job is sent to the cloud. This means, if a user is standing on a train and releases a document for print, all they are doing is sending an instruction to the cloud saying it has released this print. The document to be printed never leaves the company network.

The third and final step is at the device itself, which we think is an incredibly important step and there are several options to help security. Secure Print Release means that a user must authenticate themselves at the device, whether via password, pin number or card / badge. Additionally, this is supported by an array of administrator controls that can define levels of security, such as adding two-factor authentication, for example. At this point, the device (MFP) using IPP protocol, it will pull from the customer laptop from the local customer network.

On the case when the user want to use the mobile app, the first step is manage by EntraID or Google Workspace from the mobile app, the customer select from the corporate network drives, folders the document to print and the final step is at the device itself, a user must authenticate themselves at the device, whether via password, pin number or card / badge and the document is pull from the customer network location. On this process, Zero Trust still working and not documentation or information leaving customer network environments. Synappx Cloud Print is not storage customer users document on Synappx cloud storage and only metadata is shared.

4. Agentless Communications and Secure process

Synappx Cloud Print is a cloud solution which does not require any agents in the customer network. It is important to allow the appropriate ports and elements to allow Sharp devices and users reach the Synappx Cloud Print as part of the Zero Trust Design.

All communications between the Synappx Cloud Print Windows application, Sharp devices, and Synappx Cloud Print Administration portal use IPP, HTTPS (Port 443, 57100), SNMP or MQTT Over WebSocket, AMQP or AMQP Over WebSocket and Azure Service Bus.

The Synappx Cloud Print cloud services maintain separate signing certificates for each Synappx customer. This ensures agents are provisioned only within their associated tenant registry.

Synappx Cloud Print MFP Device Discovery

To automate the collection of MFP information (needed to configure the Synappx Cloud Print MFP services), the Synappx Cloud Print Windows client includes the ability to find MFPs using SNMP discovery when the user is authenticated as an administrator. Discovery is automatically initiated after the administrator adds the IP ranges in the Synappx Cloud Print Administrator Portal. This will be trigger in automatic in backend the SNMP from the Synappx Cloud Print Windows Client into the network. As part of the Zero Trust Design, this action will retrieve all MFPs in the Synappx Cloud Print Administrator portal in automatic (this action could take up to 15min as per the worst-case latency tested). The following information about the MFP is collected as part of this process and sent to the Synappx Cloud Print cloud:

- MFP ID that system creates (e.g. Sharp MX-C301W 63004882), Manufacturer, Model Name, Serial Number, Device Name (If Set), Location (If Set), Network IP Address

Application Security

All communication between endpoints and Synappx Cloud Print services secured and encrypted via TLS v1.2 AES256 (Port 443) or X.509 client security over MQTT, MQTT Over WebSocket, AMQP or AMQP Over WebSocket. Synappx users authenticate with Synappx applications using Microsoft 365, Google Workspace or Synappx non-enterprise guest credentials the first time he/she uses the Synappx app, when there are credential changes (e.g. password update), they log out of the mobile app and/or after 30 days or more with no app use. Synappx leverages:

- Auth0 (User authentication delegation to Entra ID, Google Workspace and for Synappx non-enterprise guest user database)
- Entra ID (User authentication with Microsoft 365 account) or Google Workspace (User authentication with Google Workspace account)

User passwords are not stored on the client device; instead, a secure JWT token is provided after user password validation with Entra ID or Google Workspace system via a partner Auth0.

Synappx Cloud Print Windows Application

Synappx Cloud Print Windows application is designed to be installed on user PC connected to the local customer network behind the firewall and protected. Synappx Cloud Print client is designed under the following security philosophy:

- User passwords are not stored on the Synappx Cloud Print client. A secure JWT token is provided after user password validation with EntraID (previous Azure AD) or Google Workspace system via a partner Auth0.
    - User access token is stored on local user computer
        - ID/Password for proxy are stored on local storage. (Encrypted using AES128)

- Only metadata is shared between PC client and Synappx Cloud Print cloud backend when the user print a document from their PC.

Synappx Cloud Print Windows application is published on Microsoft Store. When an application is published to the Microsoft Store, Entra ID/Azure administrators gain Centralised control to securely deploy the app to their users directly through the platform. This ensures compliance with organisational IT policies by eliminating unauthorised installations and reducing shadow IT risks. Additionally, automatic updates triggered by the publisher are seamlessly pushed to end users once approved by administrators, aligning with security policies. This streamlined process guarantees that users always operate the latest patched version, minimising exposure to vulnerabilities while maintaining governance over update timing (e.g., testing critical updates before rollout). By enforcing these controls, organisations proactively mitigate risks, maintain compliance, and strengthen endpoint security across hybrid ecosystems."

Key Security Benefits Highlighted:

1. **Centralised Governance:** Admins control app deployment, ensuring only vetted software is distributed.
2. **Automatic Patching:** Immediate delivery of security updates reduces exploit risks from outdated software.
3. **Policy-Driven Compliance:** Updates require administrative approval, aligning with audit and regulatory requirements.
4. **Cross-Platform Consistency:** Unified management for Entra ID simplifies secure app distribution in hybrid environments.
5. **Reduced Attack Surface:** Eliminates user-side manual updates, curbing human error and vulnerability gaps.

Synappx Cloud Print Mobile Application

Synappx Cloud Print mobile app offers features including print/copy/scan on Sharp MFPs. Security features associated with the Synappx Cloud Print mobile clients are:

- User login into the application using the EntraID or Google Workspace authentication, token is created via partner system Auth0. No password and ID are stored on the Mobile app.
- For cloud storage service's file and folder access, users can configure Synappx mobile application to access files from supported cloud storage sites. Some cloud sites are pre-configured via Single Sign On (SSO) to minimise set up time.
    - Microsoft 365 users: SSO to One Drive for Business, SharePoint Online and Teams.
    - Google Workspace users: SSO to Google Drive.
    - Apple iPhone users: SSO for iCloud and Local files.
- Optional cloud site set-up (e.g., Dropbox, Box)
    - For storage sites of interest, users can enter their username and password which are validated with the cloud storage sites. If validated, a secure token is provided and stored in Synappx mobile (and secure token is also in Azure Key Vault for Box and non-enterprise Google Drive) to avoid the user having to re-enter those credentials unless they are no longer valid (e.g., password change, account deactivated, etc.).
    - Sharp and component suppliers do not have access to user cloud storage site passwords.
      You can find all cloud storage options that the user can configure, here: App Setup | Synappx Support Centre

- File print from cloud location.
    - Synappx Cloud Print can print up to ten files across configured cloud storage sites, (100MB file size limitation). Files from iCloud, local iOS device storage, and Google Drive have a 30MB file size limit. Supported Google files stored in Google Drive only can be selected for cloud file printing.
    - Some Sharp device models may require additional expansion kits:
        - Direct Print Expansion Kit
        - Adobe PostScript 3 Expansion Kit
    - File formats supported are:

File Extensions	Google Applications
• .txt • .tiff • .jpeg • .png • .pdf* • .ps* • .docx** • .pptx** • .xlsx**	• Google Docs*** • Google Slides*** • Google Sheets*** • Google Drive*** • Google Jamboard**

- Authenticate to Synappx Cloud Print at the MFP using PIN, Card etc [View Image].
- Select the 'mobile print' option on the MFP panel [View Image].
- Select Print Cloud Files [View Image].
- The Recently Modified list displays files modified within the last 30 days from all configured sites with the most recent files shown at the top.
- Teams shows files created or modified by you within the last 30 days. Only files you created or modified in Teams folders will display in Recently Modified to print.
- New file uploads may not be immediately reflected in the Recently Modified list.
- Files from some configured cloud sites begin to display from the date of first access.
- SharePoint and Dropbox files are not included in Recently Modified list but can be selected for printing by browsing to the folder with the targeted file(s).
- iCloud and local files on iOS devices do not appear on the Recently Modified list. Those files are only accessible through the browse feature.
- The device will load recently modified files from your configured cloud storage folders. Select up to ten files from the cloud folder browsing, search feature, or Recently Modified list. Then select Print [View Image].
- Scan the QR code on the MFP panel to start the print job.

The documents selected to print on the customer cloud storage is not storage on Synappx Cloud Print and its delivery directly after authentication from customer cloud storage to the Sharp device as part of the Zero Trust Design.

Synappx Cloud Print mobile app is published on the Apple App Store or Google Play Store enables Entra ID and Google Workspace administrators to securely deploy the app to users across managed corporate devices and Bring Your Own Device (BYOD) environments. By enforcing authentication via Entra ID or Google Workspace, administrators ensure only authorised users access the application, aligning with zero-trust principles. Administrators can grant download permissions without restrictions while maintaining security, as identity verification acts as a gatekeeper. Automatic updates are triggered upon publisher release and pushed to end users once approved by IT teams, ensuring compliance with IT and security policies. This process guarantees users always operate the latest version with critical patches, reducing vulnerabilities. For BYOD scenarios, app data can be containerised or encrypted, preventing corporate data leakage on personal devices while respecting user privacy."

Key Security Benefits Highlighted:

1. **Zero-Trust Authentication**: Mandatory Entra ID/Google Workspace login ensures only verified users access apps, even on BYOD.
2. **Unified App Governance**: Centralised control over deployment (managed + BYOD) minimises shadow IT and enforces policy compliance.
3. **Automated Vulnerability Mitigation**: Timely, policy-approved updates eliminate delays in patching exploits.
4. **BYOD Security**: Containerisation/encryption protects corporate data without compromising personal device privacy.
5. **Conditional Access Integration**: Admins can enforce additional safeguards (e.g., multi-factor authentication, geofencing) for high-risk scenarios.
6. **Audit-Ready Compliance**: Detailed logs of app deployments, updates, and user access simplify regulatory reporting (e.g., GDPR, HIPAA).

Cross-Platform Flexibility:

- Supports hybrid environments (Entra ID for Microsoft ecosystems, Google Workspace for Android/Google-integrated workflows).

- Aligns with Mobile Application Management (MAM) frameworks to secure apps without full device control.

Synappx Cloud Print QR Code Generation

Synappx Cloud Print platform use the QR Code standard to provide an easy method to authenticate and validate the end user on the different process. As soon as the QR Code is generated and linked to a specific user, based on the standard, the back platform generates a new QR Code. This procedure happens in real time across all MFPs activated with Synappx Cloud Print solution.

If you are interested the standard associated with QR Code technology, please check Standard section here: QR code - Wikipedia

5. Corporate Security

Sharp maintains a robust information security programme to protect the confidentiality, integrity and availability of all information assets processed and/or stored within Sharp's business systems. Sharp management recognises the rapidly evolving and growing risks associated with the protection of Sharp and our valued business partners' information assets and is regularly researching, reviewing, and investing in procedural and technical countermeasures to help optimise security assurance. A team of dedicated professionals are continuously assessing the business environment utilising their professional expertise to enhance and continuously improve Sharp's information security posture. In addition to these internal efforts, Sharp utilises strategic partnerships with industry leading service providers to test, monitor and audit our implemented information security programmes.

Corporate Policies and Practices

Sharp has implemented several policies and procedures to ensure the security of Sharp and our business associates' information assets. All of Sharp's policies and procedures are regularly reviewed internally and updated annually. All of Sharp's policies and procedures are audited annually by our Internal Audit team and by our external auditors, as well as ISO/IEC 27001 certification and compliance.

The following list is a representative example of the policies currently in place as of the date this document was published:

- IT Security
- IT Access Control
- IT Change Management
- IT Threat and Risk Assessment
- IT Incident Handling
- IT Disaster Recovery
- IT Records Management
- IT Computer

Sharp is ISO/IEC 27001:2022 certified (renewed June 17, 2023)
https://global.sharp/corporate/eco/governance/security/

Due to the confidential nature of the content of these policies they are not regularly distributed but can be made available for review with Sharp upon execution of a Nondisclosure Agreement.

Sharp Administrator Access of Data

Sharp IT or Support may occasionally need to access your data in order to provide support on technical issues. Access permissions for these types of issues will be limited to the minimum permission necessary to resolve your issue. Sharp administrators are granted careful role-based permissions in order to uphold data security for the customer:

- Ability to view and update customer account information, such as account status and email address, but not customer files.
- Ability to see the file tree and file names but not view or download the actual files.
- Synappx users, admins and dealer admins all have appropriate access to items within their scope of authority and nothing else. System administration is strictly controlled and limited to Sharp authorised personnel. Sharp admins can only access information critical to the operation of the system. At no time are users of the system allowed to access the database or other system components directly.
- Note: Data related to your Synappx services will be deleted 45 days after a subscription termination date.

Sharp Privacy Policy

Please see the Synappx service terms of use and privacy policy at:

Add our URL for Sharp.EU

6. Summary

Making the move to cloud-based, on-the-go collaboration and meeting services offers businesses an economical way to support increasingly mobile workforces. Indeed, to build collaborative, responsive office environments, adoption of cloud and mobile technology is not a case of “if” but “when.”

Organisations that embrace cloud-based services fully utilise their existing technology investments, including computers, mobile devices, and MFPs. Combined with the Synappx subscription-based services, the elimination of capital expenditures for internal IT resources means even lower total cost of ownership. Yet some decision makers struggle with what cloud implementation entails, in terms of balancing convenience with accessibility and security. Sharp Synappx Cloud Print services help remove these barriers with a security-driven architecture and hardware/software synergy that enables agile workgroups, which can quickly respond to business demands.

Welcome to Sharp

Sharp Europe enables small to large businesses and organisations across Europe to enhance performance and adapt for their workplaces of the future through a range of business technology products and services.

Sharp services and products range from printers and advanced flat screen technologies, collaboration platforms in partnership with other leading brands, through to full IT services for small companies to large Enterprise businesses and organisations.

As a manufacturer and a service provider, Sharp is uniquely positioned to provide trusted advice and assurance to customers on how technology can work together seamlessly.

Design and specifications subject to change without notice. All information was correct at time of print. Sharp, Synappx and all related trademarks are trademarks or registered trademarks of Sharp Corporation and/or its affiliated companies. Internet Explorer, Microsoft, Office 365, OneDrive, and Azure are registered trademarks of Microsoft Corporation in the United States and/or other countries. Android and Google are trademarks of Google LLC. All other company names; product names and logotypes are trademarks or registered trademarks of their respective owners. ©Sharp Corporation 2025. Ref: Synappx Cloud Print Security White Paper (v1.0). All trademarks acknowledged. E&O

www.sharp.eu

SHARP

Be Original.