Cloud Portal Office Security Whitepaper

November 2015

Table of Contents

Introduction 2

Accessing Cloud Portal Office 2

- Account Authentication and Authorization 2
- Strong Password Policies 3
- Single Sign-on (SSO) 3
- Mobile Access 3
- AQUOS BOARD™ Interactive Display Access 4
- Sharp MFP Access 4
- Desktop Access 4

Handling Your Data 4

- File Transfer (upload/transit) 4
- Flexible Folder Permissions 5
- Global Permissions 5
- Audit Trail 5
- Encryption – In Storage 6
- Backup / Replication / Disaster Recovery 6
- Data Retention 6

Infrastructure Security 6

- Amazon Web Services 8
  - AWS Route53 (US Only) 8
  - AWS Virtual Private Cloud (VPC) 8
  - AWS Elastic Load Balancing (ELB) 8
  - AWS Elastic Compute Cloud (EC2) 8
  - AWS Simple Storage Service (S3) 8
  - Amazon Relational Database Service (RDS) 8
  - AWS CloudWatch 9
  - AWS Identity and Access Management (IAM) 9
  - AWS ElastiCache 9
  - AutoScaling 9
- Sharp Corporate Security 9
- Corporate Policies and Practices 9
- Sharp Administrator Access of Data 10

High Availability and Redundancy 10

Total System Verification 11

Summary 11

Introduction

Enterprises of all sizes, nature and type deal with and consume an array of different documents throughout their business process lifecycle. A Content Management System (CMS) is a business system that enables storage, tracking and management of the content produced, utilized and managed by an organization. With the evolving trend of cloud computing and its service models, the CMS is also now available as a Software-as-a-Service (SaaS) solution delivered and managed entirely from the cloud. The Cloud/SaaS CMS model presents a safe, flexible and efficient method to store, share, collaborate and manage electronic content across the enterprise. Businesses now have a central facility by which any employee can store and access electronic content and documents globally over a standard Internet connection.

With the managed service platform of a cloud CMS like Sharp's Cloud Portal Office, organizations can reduce internal Capital Expenditure (CapEx) and Operational Expenditures (OpEx), while focusing on their core business objectives. Cloud Portal Office also helps eliminates the need for expensive back up service, which was an essential add-on for the traditional document storage or CMS infrastructure. Organizations can rest assured that with Cloud Portal Office, their electronic content will be stored and secured through this service. The secure cloud-based delivery model of Cloud Portal Office provides users with the liberty to access their content on any supported device regardless of their physical location. This is a substantial benefit, specifically for organizations with employees who are always on the move and require universal access to their content.

Accessing Cloud Portal Office

In order to secure Cloud Portal Office, all of the system features are protected by a robust, layered security system. By using a combination of industry-standard security methods, we help ensure that accessing your data is safe and secure.

Account Authentication and Authorization

Cloud Portal Office establishes and manages robust access control and authentication architecture. Access to the system is controlled using role-based and tenant-based authentication process. Users are setup in different tenants associated with specific customer accounts and in accordance with their usage roles and permissions.

For example, each company account is provided with one or more Business Administrator level credentials. These accounts are typically used by IT to monitor and manage users within their company accounts. Similarly, Cloud Portal Office end-users are only allowed to view, store, share and extract documents within their company accounts, either directly or through an authenticated Cloud Portal Office client application. In case of unauthorized access, the system can be locked down to ensure complete data security. The Business Administrator does not need a Cloud Portal Office license in order to manage the system. However, with a Cloud Portal Office license, a complete access audit trail is available to the company's Business Administrator, which includes all activity within a company account. The Business Administrator cannot view any of the content stored in the system, just the activity.

Strong Password Policies

All document storage or retrieval requests made to Cloud Portal Office pass through a systematic and reliable authentication process. As a policy, all passwords must be at least eight characters long, and must contain at least one non-alphanumeric (symbol) character. Other password features include:

- Password resets (both by user and company admin)
- Password lockout after a set number of failed attempts
- Password session expiration after a set duration

All users of the system must provide a valid password to authenticate and use the document management services.

Single Sign-on (SSO)

Cloud Portal Office offers Central Authentication Server (CAS) authentication for all customer accounts, which allows businesses to manage user accounts from a single system (Sharp Cloud Portal). When a business removes an account from the portal, that user will no longer have access to Cloud Portal Office. The CAS/SSO system is secured by:

- Separation from the Cloud Portal Office infrastructure with Amazon Web Services (AWS)
- Communication through 256-bit HTTPS (Port 443) and exchanged security keys

Mobile Access

With the rising trend of enterprise mobility, smart phones and tablets are now common access points for business content. Users with Cloud Portal Office Mobile on their devices can access Cloud Portal Office to retrieve documents within their repositories over a secure SSL connection. For additional security:

- User needs to authenticate with Cloud Portal Office for data access
- User credentials are encrypted on the mobile device for seamless subsequent access
- All access to system encrypted via TLS v1.2 AES256 (Port 443)
- User access controlled centrally by CAS/SSO server
- In case of a mobile device theft, the user can reset their password from the browser to prevent unauthorized access.
- If an employee leaves the organization or their device is lost or stolen, their CPO files can be remotely wiped from the device using MobileIron's "Retire Device" feature.*

* "Retire Device" feature is available directly through MobileIron, a third party solution provider. Any reference in this document to MobileIron and its services is for informational purposes only. Sharp does not make any warranty regarding MobileIron's products or services. To enable the MobileIron "Retire Device" service, your company must be a MobileIron customer and the CPO app must have been deployed to the user as a MobileIron managed app. When a mobile device is compromised or an end user separates from the company, a "Retire Device" event is sent to the mobile device by the MobileIron administrator. For more details and subscription information please contact Kate Dietrich at MobileIron at Phone: 650-605-7044, Email: kdietrich@mobileiron.com.

AQUOS BOARD™ Interactive Display Access

Businesses with Sharp AQUOS BOARD displays can connect to Cloud Portal Office with our Cloud Portal Office Meeting Room software. The display device connected to a computer installed with Cloud Portal Office Meeting Room client software allows users to seamlessly and securely authenticate and search for documents on Cloud Portal Office. Additional security features of the software include:

- Authentication and communication over TLS v1.2 AES256 (Port 443)
- Temporary access to files on public or private AQUOS BOARD displays (WebDAV)
- Secured WebDAV communication to create, change and access content
- 30-minute inactivity-based session timeout to minimize idle sessions
- Guest user feature for time-limited, folder-limited file upload access
- Upon logout all Cloud Portal Office folders/files will no longer be visible on the AQUOS BOARD display to prevent unintended access
- User access controlled centrally by CAS/SSO server

Sharp MFP Access

Businesses with supported Sharp OSA®-enabled multi-function peripherals (MFPs) can access Cloud Portal Office directly with the Cloud Portal Office Scan/Print application. Once installed, an account user is able to browse, scan and print files residing on Cloud Portal Office directly on the MFP. Access on the MFP has the following security features:

- User authentication to prevent unauthorized access
- Password encrypted and never stored on the MFP
- Secured TLS v1.0 AES256-SHA1 (Port 443) channel between MFP and Cloud Portal Office system
- User access controlled centrally by CAS/SSO server

Desktop Access

The Cloud Portal Office Desktop application enables a PC/Mac desktop computer to store, access and synchronize documents with Cloud Portal Office. All network communication between Cloud Portal Office and the desktop computer is carried out over HTTPS (Port 443) secured channel. Passwords are securely encrypted on the desktop and authenticated over HTTPS with the Cloud Portal Office before the user can perform any sync-specific operations.

Handling Your Data

File Transfer (upload/transit)

Only an authenticated user will be able to upload files into Cloud Portal Office. The system implements security architecture according to industry standards for SaaS applications, with firewalls installed at external and internal boundaries of the network to provide protection against unsecured connections and traffic. The Cloud Portal Office system is deployed inside a Virtual Private Cloud (VPC) to provide maximum security from outside attacks and unauthorized access. By default, only port 80 and 443 are opened and all unnecessary ports are closed.

(Handling Your Data: File Transfer Continued)

The Cloud Portal Office system requires that all data in transit must be authenticated even if they are sent over a secured HTTPS (Port 443) connection. Furthermore, transmitting data over HTTPS prevents the data from being tampered with, forged or eavesdropped.

- TLS-based security (with 256-bit key encryption) for data transmitted to and from the clients to the Cloud Portal Office system
- Establish and maintain protected connections for each file transfer between the system and device applications

Flexible Folder Permissions

Uploaded files automatically inherit the permissions of the folder they were saved to according to the authenticated user's settings. Once the file is uploaded, the folder permission can be set to share that file with other members within the company account. As an added security measure, sharing is limited to within the company account. To share with individuals outside, the Business Administrator would have to create a user account with the company's account. This ensures that no "leakage" of company Intellectual Property occurs without the explicit consent of the business.

- Folder/subfolder-level viewing, downloading and sharing permissions
- Share with individual Cloud Portal Office users or preset user groups within the same company account
- Configure notifications to notify you when someone updates a shared file or folder
- Detailed audit trails for each file and folder

Global Permissions

Each Cloud Portal Office company account will have one or more Business Administrators with restricted access for account-level features, including:

- Add new account users and grant proper permissions
- Upgrade user accounts for additional features or storage requirements
- Create groups and assign members to groups
- Remove users from company account to restrict access
- Reset user password
- Cancel unassigned licenses

Audit Trail

Cloud Portal Office provides activity logging as a default service for each tenant within the system. It automatically records supported events, operations and transactions performed on the system. This information is available for Cloud Portal Office Business Administrators with a Cloud Portal Office license, as well as end-users (for their own account activity).

System logging for the purpose of performance measurement, service monitoring and security tracking is also an essential component of Cloud Portal Office. It provides granular event and operations logging features for

(Flexible Folder Permissions: Audit Trail Continued)

all the different components of the system, delivering a composite insight into the Cloud Portal Office system. An audit log of the system, which provides Information Security (IS) auditors with insightful data about system activity, about access to the system and internal events. For security reasons, system logging will not be accessible for Business Administrators or end-users.

Encryption – In Storage

All user files stored in Cloud Portal Office are encrypted using AES 256 key encryption.

Backup / Replication / Disaster Recovery

Cloud Portal Office documents are stored on AWS Simple Storage Service (S3), which includes automatic replication. S3 provides several layers of backup and replication to ensure data integrity. Additionally, when the file data is at rest, it is secured using AES encryption with 256 bit key. So, if someone gains access to the S3 bucket, they will not be able to decrypt the data without the secured encryption key.

Besides documents on S3, all other Cloud Portal Office files are stored on AWS Elastic Block Storage (EBS), which provides high availability and high reliability storage. The whole EBS volume is automatically replicated to prevent data loss due to failure of any single hardware component.

In the event of a disaster, Cloud Portal Office will recover according to our disaster recovery policies:

- All system images are recovered to previous snapshot
- File data and databases are restored from separate S3 storage used for snapshots
- System is audited to ensure integrity of data

Data Retention

All data within Cloud Portal Office are retained according to the data retention policy outline in the Cloud Portal Terms and Conditions.

The Cloud Portal Office application handles the backup and recovery of individual users' data using the built-in "Recycle Bin" concept. The "Recycle Bin" provides special storage and file handling. When a user deletes files they are moved into "Recycle Bin" storage. At this point, the user may restore the files from the recycle bin if desired. However, when the user empties the recycle bin all the "deleted" files will be removed permanently from the given user space.

Infrastructure Security

The Cloud Portal Office system ensures end-to-end security, availability and integrity of the whole system through integrated security tools and features. This is primarily delivered through the native AWS Identity and Access Management (IAM) and CloudWatch monitoring application.

IAM is a user and group-based security mechanism, which restricts only authorized or group-specific users to access the Cloud Portal Office infrastructure. IAM has several layers of security checks. These include passwords and access keys. IAM enables managing and assigning roles and setting permissions to users and

(Infrastructure Security Continued)

applications on their usage/rights. This ensures that only legitimate system administrators can view, edit or operate the Cloud Portal Office system.

CloudWatch serves as a guardian to the Cloud Portal Office system infrastructure, providing a centralized interface for all the activities within the cloud. It is used by the system administrators to track performance metrics, gain insights into the system and perform maintenance activities in the event of an abnormality. It has native support for all AWS components and can collect performance metrics from all configured services. The administrators can set automated notifications when a specific event or performance threshold occurs or a metric reaches a selected level.

In addition to Cloud Portal Office's security architecture and countermeasures, system security is further strengthened by the security measures AWS brings into play across its cloud and storage services. The IT infrastructure that AWS provides is designed and managed in alignment with the best security practices and a variety of IT security standards, including:

- Service Organization Controls 1 (SOC 1)
    - Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
    - International Standards for Assurance Engagements No. 3402 (ISAE 3402)
- Service Organization Controls 2 (SOC 2)
- Service Organization Controls 3 (SOC 3)
- Federal Information Security Management Act (FISMA)
- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- DOD CSM Levels 1-5
- Federal Risk and Authorization Management Program (FedRAMP)
- Payment Card Industry (PCI) Data Security Standard (DSS) Level 1
- International Organization for Standardization (ISO 9001)
- International Organization for Standardization (ISO) 27001 Standard
- US International Traffic in Arms Regulations (ITAR) – Only AWS GovCloud (US) region
- Federal Information Processing Standard (FIPS 140-2)
- Multi-Tier Cloud Security (MTCS) Level 3

In addition, the flexibility and control that the AWS platform provides allows customers to deploy solutions that meet several industry‐specific standards, including:

- Health Insurance Portability and Accountability Act (HIPAA)
- Cloud Security Alliance (CSA)
- Criminal Justice Information Services (CJIS)
- Family Education Rights and Privacy Act (FERPA)
- Motion Picture Association of America (MPAA)

Note: For additional information on AWS security, please refer to Amazon's security white papers (https://aws.amazon.com/security/).

Amazon Web Services

Being an industry-recognized and certified provider and host to billions of objects of data, AWS must maintain the highest standard of information security. AWS achieves this by maintaining tested, authentic, and result-driven information security technical and business processes, best practices and security frameworks.

Below are some of the major AWS components utilized by the Cloud Portal Office system and the security mechanisms employed:

AWS Route53 (US Only)

Route 53 is a domain name service that provides the ability to connect Cloud Portal Office users with the Cloud Portal Office application. It is a highly scalable and robust service that protects Cloud Portal Office from DDoS attacks from malicious users and is only available to Cloud Portal Office in the US.

AWS Virtual Private Cloud (VPC)

VPC enables provisioning an entirely stand-alone, unshared and secured private cloud within the AWS infrastructure. It provides a separate access control mechanism, creation of security groups and filtering of inbound and outbound traffic.

AWS Elastic Load Balancing (ELB)

ELB distributes incoming Cloud Portal Office user traffic across multiple Amazon EC2 instances while providing TLS encryption. Besides providing high-availability (HA) and redundancy, when used with Amazon VPC and security groups, it also extends an additional security layer for the system.

AWS Elastic Compute Cloud (EC2)

Elastic Compute Cloud (EC2) is the raw computing infrastructure in the AWS service/product offering, providing massively scalable and robust server computing instances or virtual servers. Each instance can be separately configured for access control, traffic filtering and the ability to create publicly and privately online servers. The communication between Cloud Portal Office users/applications and the EC2 instances within the Cloud Portal Office system is sent through a secured and encrypted channel.

AWS Simple Storage Service (S3)

Simple Storage Service (S3) is the cloud storage infrastructure of AWS that provides tremendously scalable storage architecture. It enables storage and retrieval of large amounts of data anytime, anywhere on any device over the Internet. Amazon S3 provides several layers of information security, including Identity and Access Management (IAM), bucket policies, query string authentication and access control lists (ACL's).

Amazon Relational Database Service (RDS)

RDS is a managed service for relational database. RDS manages the database instance by performing backups, handling failover and automatically patches the database software. We are using RDS PostgreSQL Multi-Availability zone deployed in VPC for network isolation with high availability and automated fail-over from primary database to a synchronously replicated standby database. Automated backups enable point-in-time recovery.

(Infrastructure Security: Amazon Web Services Continued)

AWS CloudWatch

CloudWatch is a cloud monitoring solution that monitors, manages and collects measured statistics into the cloud resources and applications in a cloud environment. It provides a system-wide yet centralized interface to monitor cloud resource utilization, performance and health of the system.

AWS Identity and Access Management (IAM)

Amazon IAM is the primary information security application by AWS that enables managing and securing access to all cloud resources under a user-, group- and role-based access mechanism.

AWS ElastiCache

ElasticCache improves the performance of web applications by allowing us to retrieve information from a fast, managed, in-memory caching system. We use Amazon ElasticCache for Redis, which enables the management, monitoring and operation of Redis nodes. Redis replication group has a primary and supports up to five read replicas. ElastiCache automatically detects the failure of the primary and selects the read replica and promote to primary.

AutoScaling

Auto Scaling enables us to follow the demand curve for our applications closely, reducing the need to manually provision EC2. CloudWatch sends alarms to trigger scaling activities and Elastic Load Balancing helps to distribute traffic to EC2 instances within Auto Scaling groups to run at optimal utilization.

Sharp Corporate Security

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

Corporate Policies and Practices

Sharp has implemented several policies and procedures to ensure the security of Sharp's, and our business associates', information assets. All of Sharp's policies and procedure are regularly reviewed internally and updated at least annually. All of Sharp's policies and procedures are audited annually by our independent Internal Audit team and by our external auditors.

(Sharp Corporate Security: Corporate Policies and Practices Continued)

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 and Mobile Device Management
- ISMS Policy

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 see the file tree and names, but not view or download the actual files
- Ability to view and update customer account information, such as account status and email address, but not customer files
- Access by all Sharp administrators is always logged
- Cloud Portal Office users, business administrators and dealer administrators all have appropriate access to items within their scope of authority and nothing else. System administration is strictly controlled and limited to Sharp authorized personnel. Sharp administrators 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.

High Availability and Redundancy

Cloud Portal Office utilizes redundant web, database and data centers to ensure continuous operations during disasters of many types. Smaller issues such as minor hardware failures are handled without affecting end user experience or IT involvement. Minimal data loss and end user inconvenience is expected for larger issues such as natural disasters.

Total System Verification

Cloud Portal Office is also inspected externally by a third-party security company (McAfee® Foundstone® security assessment) to defend against external risks, such as Cross-site scripting (XSS), SQL injection and application vulnerabilities.

Summary

Making the move to cloud-based, on-the-go collaboration and storage services offers businesses an economical way to support increasingly mobile workforces. Indeed, to build collaborative, responsive office environments, adoption of cloud technology isn't a case of "if" but "when."

Organizations that embrace cloud services fully utilize their existing technology investments, including computers, mobile devices, interactive display systems and MFPs. Combined with a pay-as-you-go document management service, 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 Cloud Portal Office removes these barriers with security-driven architecture and hardware/software synergy that forms agile workgroups, which can quickly respond to business demands.