Xerox® Capture & Content Services

Security White Paper

2024

Introduction

Xerox® Capture and Content Services (CSS) streamlines the flow of information, harnessing the power of AI to process and integrate data seamlessly into your business operations. Through every step, from data capture to delivery, we prioritize security and risk management. Xerox is dedicated to implementing rigorous security measures to keep customer data safe.

SCOPE OF THIS DOCUMENT

This client-facing white paper offers an overview of the security processes related to the cloud environment that hosts the CCS applications and to the imaging centers where physical and digital collateral are processed. The paper covers both physical and electronic controls for the following Global Capture Platform programs.

- Production Workflow Manager
- Capture & Content Services Analytics (CCA)
- Xerox® Intelligent Document Processing Platform (IDP)

CUSTOMER DATA

The information transferred from customer premises is combined with a customer-specific data set found within our cloud environment. A variety of customer data including personally identifiable information (PII) may be collected depending on the services provided. How we handle information security is highly regulated based on existing regulations, internal standards, and specific customer requirements. The information we handle is customizable based on the service and customer requirements. We comply with all regulations relevant to the data types we are handling. The regulations include, but are not limited to:

- FedRAMP Authorized services to capture data from multiple sources, automate extraction of data critical to business processes, streamline and improve cycle times, deliver data securely, efficiently, and on-demand.
- Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) regulations in the US for ensuring security and privacy of protected health information and payment card data, respectively.
- General Data Protection Regulation (GDPR) regulations in Europe for ensuring the protection of personal data and privacy.

Finally, the CCS applications are tested against internal Xerox processes for risk assessment and mitigation.

DATA USE

Production Workflow Manager

Production Workflow Manager oversees and manages the entire digitization process from intake to delivery, with a strong emphasis on protecting sensitive data throughout its lifecycle. PWM's secure architecture ensures that all data and documents are handled with the highest level of confidentiality and integrity, making it an essential tool for modern business operations. PWM is deployed in our data centers.

Capture & Content Services Analytics

Data is used in thoughtfully designed, interactive dashboards that provide users a way to gain insights from the data. The components processing the ingestion of data are on-premises in our data centers co-located with the data sources. Data access is read only.

Intelligent Document Processing

Data is solely used to process an item submitted into the system and is not maintained after delivery to the designated end point hosted environment. Some of the data types processed by IDP include:

- Client document data
- Operational data
- System data

ARTIFICIAL INTELLIGENCE

AI's powerful and evolving capabilities help Xerox to process and analyze documents which provides our customers a deeper understanding of their operations. We comply with applicable AI laws and have internal policies that ensure the following standards are met:

- Transparency:
  - Traceability: identification of the reasons why an AI-decision was erroneous.
  - Explainable: decisions made by an AI system can be understood and traced by human beings.
  - Communication: AI systems should not represent themselves as humans to users.

- Human Oversight: AI systems should support human autonomy and decision-making.
- Accountability: Ensure responsibility and accountability for AI systems and their outcomes, through all stages of their development, deployment, and use.
- Non-discrimination: Support for diversity and fairness. Avoidance of unfair bias, accessibility and universal design, and stakeholder participation.

  Additional information regarding our AI policies is shared on the Xerox policy page.

DATA PRIVACY AND PROTECTION

The CCS user data is stored on servers physically located in highly secure data centers across supported regions, including North America and Europe. When handling personal data, we comply with all privacy laws applicable to data we collect and process in connection with all our products, services, and solutions. We monitor laws in relevant geographies to ensure that we are staying current in our compliance. This includes, but is not limited to, the EU GDPR, the UK GDPR, PIPEDA, and applicable U.S. state privacy and data protection laws such as the CCPA. You can access the Xerox Privacy Policy here.

PHYSICAL SECURITY

Physical security for the CCS data center is managed by Microsoft; they make every effort to control physical access to the areas where customer data is stored. They have a department dedicated to designing, building, and operating the physical facilities that support Azure. For greater detail on the layers of protections that Microsoft has established, please refer to the articles Microsoft published addressing how they secure physical facilities (Azure facilities, premises, and physical security) or where your data is located.

To ensure that these security measures meet evolving requirements there are physical security reviews. They also have established best practices for wiping data and disposing of equipment to protect customer data.

Capture & Content Services – Imaging and Indexing Centers

Access to the imaging and indexing centers requires authenticating against multiple security controls. All physical entryways are monitored for unauthorized access. Use of recording devices such as portable personal cameras and camera phones is strictly prohibited. Physical security measures include:

- The facility is not located near any high-risk facilities or high crime areas.
- All external windows employ bulletproof glass. The facility uses a gated barbed-wire, pressure sensitive fence and vehicle barriers where applicable. Critical areas, such as external air intakes and shipping docks employ measures to prevent unauthorized access.
- Imaging and Indexing center access is restricted to approved individuals and requires two-factor authentication against an electronic badge reader. Badge readers are found at interior and exterior access points. Separate Access Control Lists (ACLs) are maintained for each access level.
- All access is monitored and recorded by cameras. Surveillance video is securely retained for at least 90 days.
- On-site security personnel control visitor access to secure facilities, monitor the surveillance video, and conduct random walking rounds throughout the facility.
- Badge card access transaction records are retained.
- All access logs and personnel access rights are reviewed monthly.
- All hosting assets are contained within secured racks. The racks are in a secured cage within the data floor. Access to the cage and racks is restricted. The cage and racks do not display the names of their tenants.
- Access to removable media and drive bays is restricted. Retired media is sanitized prior to disposal. The sanitization process follows standard procedures established by Xerox Corporation in accordance with Department of Defense guidelines.

ENVIRONMENTAL CONTROLS

The data centers employ the following proactive methods to monitor and maintain environment controls:

- Modern fire suppression technologies.
- Redundant power generation capabilities that can use a variety of fuel sources.
- Use of generators that can run indefinitely and that are routinely tested.
- Use of Uninterruptible Power Supply (UPS) and Heating/Ventilation/Air Conditioning (HVAC) systems that are a minimum of N+1 redundant, ensuring that a duplicate system can immediately come online in case of a system failure.
- Monitoring of air quality to detect potential issues such as a fire or damage to the facility.
- Use of server power supplies and servers supporting load-balanced applications that are distributed across multiple electrical circuits.
- Proactive monitoring of circuit load to assure proper power distribution.

NETWORK SECURITY

- The network infrastructure is segmented and secured by routers, firewalls, IDS/IPS systems (intrusion detection and prevention), application layer content switches, and network switches.
- The routing environment has ACLs configured to restrict unauthorized access and Quality-of-Service (QoS) configured to prevent Denial-of-Service (DoS) events.
- The firewalls are configured to permit only required incoming and outgoing services at each tier. Servers are only provided with outgoing Internet access if required for an application or service they host. For servers requiring Internet access, that access is restricted to specific destinations when possible. Firewall rules and configuration are

annually reviewed by Xerox Corporate information security professionals.

- Application layer switches provide hardware-based load-balancing and Secure Hypertext Transfer Protocol (HTTPS) termination, as well as additional protection against DoS events.
- Layer 2 switches employ Virtual Local Area Networks (VLANs) to further segment network traffic.
- Changes to device configurations follow a strict change management process requiring documentation and approval of the requested change.
- There is a process to assure the security of the hosting environment DNS against cache poisoning and other DNS-specific threats.
- Servers do not have routable IP addresses on any interface. Internet-facing interfaces are provided with access through Network Address Translation (NAT) of non-routable private addresses.

Xerox® Capture and Content Services has been certified by BSI to ISO/IEC 27001.

SYSTEM SECURITY

A standard process exists for testing and securing servers before they are deployed into the production environment. This process is derived from industry best-practices and recommendations by our Global Security Services group, the Center for Internet Security (CIS), CERT, and SANS. The process employs template-based server deployments, group policies, and regular system audits using industry-recognized security tools to discover improper configurations and known vulnerabilities.

- Malware prevention tools are in use to secure all servers against viruses, spyware, and rootkits. For enhanced security, a next generation AI driven threat protection tool is deployed to servers, and all updates and notifications are automated. Members of the hosting team receive reports detailing the current malware protection status of all servers in the hosting environment.
- Third party, accredited auditors provide additional verification of security controls. These audits may include process, documentation reviews, and penetration tests.
- A patch management procedure exists for testing and verifying Operating System (OS) patches before deployment in the production environment. An enterprise patch management tool provides controlled patch deployment and notification of missing patches. Patches are downloaded automatically based on server role and installed software. The patches are applied during a maintenance window within 30 days of patch availability and successful staging. Current patch status for all servers is reported monthly to Xerox Cybersecurity. Additionally, members of the hosting team receive monthly reports detailing the status of all patches released in the past 90 days.
- For servers requiring Internet Information Services (IIS), a standard process exists for assuring secure IIS instances. This process includes testing of IIS and the methods employed for the server's secure communications to verify their proper operation. Only "safe" IIS methods are employed. IIS is configured to protect against Uniform Resource Locator (URL) injections and other known attacks.
- For servers requiring SQL Server, a standard process exists for assuring secure SQL Server instances. The database servers are located on a separate non-routable private network. SQL Server and application users are created using the least-privileges model. Unique users are created for each application's database access. SQL connection strings are encrypted in storage.
- Special securely maintained registry keys can be employed in an emergency to harden the servers against DoS attacks that manage to circumvent the network layer controls. These registry keys harden the Transmission Control Protocol (TCP) stack against TCP SYN Floods and other recognized attacks, as well as hardening the Server service against attacks that disable file sharing.
- All servers are scanned on all network interfaces on a regular basis by security tools to maximize protection against known attacks and Windows vulnerabilities, and support compliance with pre-defined policies.
- Access to application file stores is restricted to members of the hosting team, application service accounts, anti-virus service accounts, and backup service accounts. Each customer is logically separated using its own separate folder in each application's file store. Customer folders are named with Globally Unique Identifiers (GUIDs) and not the customer's name. Web Services are restricted to the required interfaces. Inter-application Web Services not required to listen on the Internet are restricted to a private internal network.

Patch management process includes:

Operating System Patches for all Third-Party applications.

We monitor for new vulnerabilities through multiple sources, including automated tools and subscribing to common mailing lists, threat intelligence feeds, and security audits.

REMOTE MANAGEMENT

Servers in the hosting data center are remotely managed via an encrypted channel from management stations located on a secure network. Team members use an encrypted Virtual Private Network (VPN) connection to authenticate to the secured network before connecting to the hosting data center. The VPN connection utilizes multi-factor authentication, with one of the factors being authentication to an Active Directory domain.

Restricting access is imperative for Xerox. We use role-based access control (RBAC) to assign permissions to users, using the need to know and least privilege security principles. For information about RBAC in Azure, see What is Azure role-based access control (Azure RBAC). Access to Azure resources for Development and Operations staff is controlled

via Xerox Azure Active Directory authentication with additional two-factor authentication (2FA).

APPLICATION SECURITY

A standard process exists for testing and securing the applications that reside in the hosting environment. This process is derived from industry best-practices and recommendations by Xerox Global Security Services, CIS, CERT and SANS Institute. The process employs a strategy based upon regular auditing of systems using industry-recognized security tools to discover improper configurations and known vulnerabilities.

- The Capture and Content Services applications that are multi-tenant manage multiple customers from the same database. The applications are designed with granular security roles so that users, or groups of users, have only those privileges and data access rights needed to perform their approved job functions. Proper role implementation is verified through a standard process.
- Applications are scanned using an industry-recognized application security tool throughout the software development lifecycle. Security gaps are closed prior to deployment of new applications or patches to existing applications. The security scans verify protections against known attacks, including SQL Injection, Blind SQL Injection, Cross Site Scripting, POSTDATA Injection, and Buffer Overflows. The scanning tool is updated on a regular basis to assure protection against emerging threats. Scanning includes both applications and Web Services. In addition, we complete static and dynamic code evaluation.
- Users are authenticated with Azure Active Directory (Azure AD).
- Applications support the enforcement of a password policy consisting of length, complexity, and session timeout requirements. Account lockouts result in an event log entry, an application log entry, and notification to the hosting team. Application operations are verified to assure that passwords are stored, supplied, and submitted in an encrypted format and that users cannot access unauthorized application areas.
- Application inputs are validated at the client and server to prevent malformed or incorrect data from being entered, stored and displayed.
- Application outputs are validated to assure that outputs cannot cause malicious code execution on the client.

Identification of Vulnerabilities

Our security team regularly conducts annual third-party penetration testing as well as monthly vulnerability scans, and regular internal network and server security audits as part of the normal operating procedures within the Xerox hosted environment.

DATA ENCRYPTION

Microsoft data centers negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

All transactions with Azure Storage take place over HTTPS.

LOGGING AND AUDITING

Azure logs are collected in the following categories:

- Control/management – provides information about create, update, and delete operations.
- Data plan – provides information about events raised due to Azure resource usage (e.g., diagnostic logs).
- Processed events – provides information about processed events/alerts.

More details about the Azure security measures are documented on the Azure Security pages.

BACKUPS AND ARCHIVING

Capture & Content Services Analytics

Backups are encrypted at the storage level. The backups are replicated to the disaster recovery site for redundancy and validated periodically by authorized operations personnel.

Intelligent Document Processing

All data is backed up daily and replicated to the DR data center. All backup data is kept for a 4-week period. Backups are performed using an industry-leading backup software, Veeam, which enables continuous protection of the infrastructure environment.

REDUNDANCY AND DISASTER RECOVERY

Redundancy is employed at every opportunity to meet or exceed contracted uptimes.

- All data is backed up daily and replicated to the DR data center. All backup data is kept for a 4-week period. All data centers are under contract control of Xerox, operated by Microsoft.
- We have a mature Business Resumption Plan, Disaster Recovery Plan, and Emergency Preparedness Plan in operation at each of its locations.
- Disaster recovery for cloud storage systems is managed by Microsoft Azure. For additional details on how Azure manages hardware disaster recovery, please refer to Azure global infrastructure.

CERTIFICATIONS AND ACCREDITATIONS

- Our ESS Information Security Management System is ISO 27001 certified. You can search the BSI certificate directory to confirm the ISO/IEC 27001 s. Adherence to the ISO 27001 standards is assessed

annually and certified every three years. The ongoing certification process requires both internal and external audits.

- The Microsoft run data center is NIST SP 800-53, for security and reliability
- The Xerox CCS environment is subject to an annual SOC2 Type 2 conducted by an independent third party. See our Security Compliance page for more information.
- We also perform independent, third-party penetration testing of the environment.

To learn more, visit us at www.xerox.com/CaptureandContent.