Security Guide of Xerox® Translate and Print

Secure translations anytime, anywhere.

xerox™

Security Guide

Information in any language is a strategic business asset and its safety and availability affect practically all aspects of a business.

To ensure comprehensive protection of your information including personal information, documentation, payments data, submitted documents and ready translations, all data must be protected simultaneously. That is why the Xerox® Translate and Print offers in-depth defense and protection of your data no matter where your translation is.

THE LEADING STANDARDS FOR SECURITY

The cloud-based Xerox® Translate and Print is optimally flexible and reduces the time, cost and security concerns of managing translation projects associated with traditional agency or freelance translators. To ensure the safety of your projects in the cloud, we utilize leading standards for security so you can submit your highly sensitive and confidential documents and data knowing your information is protected.

BEST-IN-CLASS MANAGED AND DEDICATED CLOUD HOSTING

Xerox® Translate and Print is hosted on the Microsoft Azure Network – the world's most secure cloud based network.

Microsoft provides security for the hosting environment that includes physical security, fault-tolerance, redundancy, operations and personnel security. Microsoft's security procedures include encrypted communications and encrypted storage for all data as well as operational processes, identity and access management, intrusion detection, DDoS attack prevention, penetration testing and more. Click on this link to get a full description of the security levels provided.

https://azure.microsoft.com/en-us/support/trust-center/

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 Type 1 and Type 2 certification. For a comprehensive overview, please follow the link:

https://www.microsoft.com/en-us/trustcenter/Compliance/SOC?downloadDocument=nli&documentId=d37a4378-8fe8-4a2d-aeff-902bb6f1c200

For more information, contact us directly at contact@xeroxtranslates.com.

SECURE WEB COMMUNICATIONS

All web communications between servers and browsers are encrypted using TLS 1.2- the industry's best data encryption technology. This makes an HTTP Secure (https) server connection possible, allowing information breaches to be prevented.

CLEAR DATA LOCATION

All customer data is currently processed and stored on servers at Microsoft Windows Azure data centers within EU. The data is contained in blob storage format which is encrypted by default. The geo replication is currently limited within the EU.

In future, Xerox® Easy Translator Service may be hosted in other regions to meet requirements of customers from those regions. Customers will then be able to decide where they wish to store their data.

Need another location? Please, let us know at contact@xeroxtranslates.com.

STATE-OF-THE-ART CONNECTKEY® TECHNOLOGY FOR SECURE MFP TRANSLATIONS

The Xerox® Translate and Print MFP application based on state-of-the-art Xerox® ConnectKey® technology lets users get translations instantly on the spot using typical scanning methods.

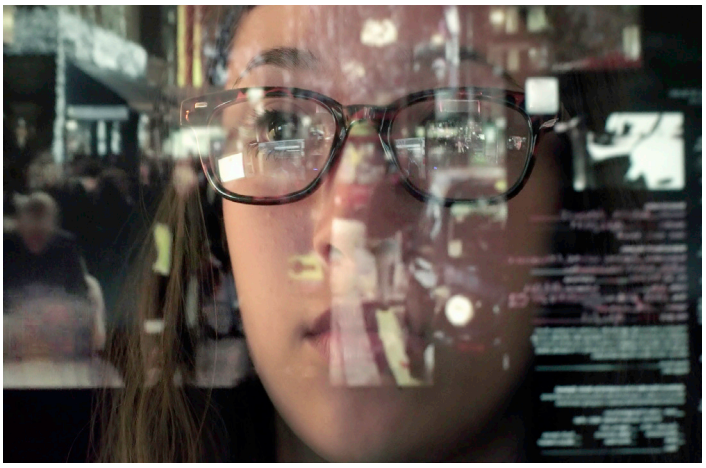
To protect your MFP translations from potential outside threats, ConnectKey® Technology features industry's most comprehensive approach to security that includes our groundbreaking partnership with McAfee and Cisco®. For a full description, click the following link:

https://www.xerox.com/en-us/connectkey/secure-network-printing

Security Guide

THE LEADING STANDARD IN THE CARD PAYMENT INDUSTRY

To protect your financial transactions, we only use the most trusted security standard in the card payment industry: The Payment Card Industry Data Security Standard (PCI DSS). PCI DSS compliance requires adherence to strict data encryption methodologies, fraud detection, fraud prevention and network and traffic monitoring services.



COMPLETE CONFIDENTIALITY WITH MACHINE TRANSLATION

Every enterprise wants to know how our machine translation service is better and more secure than most others, including weaker, but essentially free services. One of the most important differences is security.

Free services save and reuse all submitted text to improve the quality of future translations. It does not matter whether the translations are yours or belong to another user. Anyone who uses this free service can see information from previous orders - including yours - in their translation results. In fact, when using such a free service you make your information publicly available and unwittingly or unknowingly forfeit its confidentiality. Most security officers are familiar with the problem of agreeing to giving away your irrevocable rights to your company's data.

When you order machine translation with Xerox® Translate and Print, you can be assured your information is never reused for other parties' translations.

We guarantee that it will not be disclosed to any third parties – ever.

This means that with Xerox® Translate and Print you can confidently submit even your most confidential and highly sensitive content.

ORGANIZATIONAL SECURITY MEASURES

Xerox® Translate and Print is designed to be run without routine access to customer data by Xerox® personnel. A limited number of authorized Xerox® personnel may technically access customer data, while nobody at Xerox® can review your data.

Access to the service by Xerox® employees is controlled and logged. While there are several access levels, only a limited number of employees have access to the part of the system containing confidential data.

As part of the development and maintenance process, access to the different parts of the system is strictly segregated between the team members according to their roles.

Production and development environments are also segregated so that no user data is used for testing.

In accordance with our procedures, Xerox® employees are not permitted to review client documents and translation results, except in exceptional circumstances where a document:

- causes the service failure.
- leads to the abnormal consumption of computing resources.
- leads to additional exceptional cases connected with the functionality of the service.

A limited number of authorized Xerox® personnel may review this image for the sole purpose of reproducing and fixing the issue this document has caused. In such cases, only a derivative document, without any personal/ confidential data, can be used to fix the issue.

DATA INTEGRITY

The system prevents data from being damaged, corrupted or tampered with during storage, processing or transmission.

Protection during storage is ensured by back-up infrastructure and strict segregation of data. Additionally, the data is always protected by firewall and antivirus software.

Protection during transmission of data is ensured by using encrypted communications.

Cloud nature of the system backend empowers easy and timely updates. The users can be sure that the most current version of the system is deployed.

ConnectKey® Technology gives the IT personnel an easy and familiar way to deploy newer versions of the Xerox® Translate and Print application on the MFPs.

During processing, the system prevents unauthorized elements to be injected into user data. This is achieved on several levels.

Protection from such defects is built-in into service technology and does

not only rely on organizational measures. For machine translation, the output of the system is strictly determined by the input. Only non-executable plain text data is being returned by the translation sub-system.

The system prevents the insertion executable output as translation for non-executable content. Executable links in the source documents are not translated.

At the development stage following the industry-standard systems development life cycle is followed. Quality assurance process within SDLC ensures the correct functionality of the service, adherence to strict data encryption, network and traffic monitoring methodologies and practices.

COMPLIANCE OVERVIEW

At Xerox, the security, privacy and availability of our customers' data is our priority. We believe that a sound compliance and risk management strategy is as important to the success of an organization as the company's product strategy. To the end, our cloud strategy includes a coherent approach to keeping your data safer, more secure and available.

To protect the system from the physical layer all the way through the software layer, we use a rigorous set of specific security activities spanning software development practices, processes and tools that are integrated into multiple stages of the product lifecycle. This helps protect the Xerox infrastructure, applications and services and certifications.

Which Standards does Xerox Focus on? Xerox demonstrates our commitment to security by implementing and requiring our partners to implement a range of important industry standards and complying with government regulations concerning security and privacy of data. While there are numerous industry standards and certifications comprising of thousands of different requirements for compliance in the cloud, Xerox determined that significant overlap exists between these requirements and focuses on those that most significantly affect our customers.

As new security standards and regulatory requirements are developed and adopted by the industry, Xerox will review then and adopt those with relevance to our customers.

INDUSTRY STANDARDS

Xerox focuses on meeting compliance of the following primary industry standards:

SOC – The Service Organization Control(SOC) reporting standard has been established by the American Institute=the of Public Accounts (AICPA). Xerox currently utilizes SOC 2 reporting standard. SOC 2 reports are based on a third-party attestation of compliance with AICPA Trust Service Principals relevant to security, availability, confidentiality and processing integrity.

PCI DSS – The Payment Card Industry Data Standard (PCI DSS) is a proprietary information security standard for organizations that handle payment card information, such as credit card numbers. PCI DSS certification of our payment partners increases controls around cardholder data management. Utilizing PCI DSS compliant service providers enables Xerox to help customers and meet PCI requirements for safe handling of personally identifiable data associated with a cardholder.

Response to known vulnerabilities: Xerox maintains a website, https://www.xerox.com/security with up to date security vulnerability status, white papers, Common Criteria Certification, Intel Security McAfee information, and a portal to submit security questions to Xerox.

CONCLUSION

Xerox deploys a company wide security strategy. With the people processes and technology, as well as a range of oversight, audit and follow up mechanisms in place, Xerox ensures our ongoing commitment to help protect our customers and their data.

contact@xeroxtranslates.com

www.xeroxtranslates.com

xerox™