OpenText Cloud

OpenText™ Cloud: Fax Network Infrastructure for Security and Compliance

Protect fax data in today's highly regulated business environment

Depending on the industry, many enterprises must comply with a series of federal regulations. In fact, global enterprises must operate in a highly regulated world with ever-changing mandates that require sensitive business information remain secure within an organization's respective information infrastructure. For example, hard-copy documents left on departmental fax machines are highly susceptible to unauthorized access and, subsequently, regulatory compliance violations. Security breaches like this result in costly penalties, litigation, and ultimately damage to stakeholder relationships and brand reputations.

OpenText is committed to protecting customers' business-critical data, providing assurances through its Global Information Security organization. These assurances are designed to give customers the necessary security, compliance, and reporting they need to address their respective industries' most important regulatory requirements.

Security Policies and Procedures

Faxes typically contain highly sensitive information about business transactions and decisions. OpenText takes an active approach in promoting and executing activities for ongoing risk assessment. The idea is to make sure that all security standards, policies, and procedures assist in ongoing risk assessment. OpenText uses a comprehensive set of standards to protect its customers' fax data in a fully secure computing environment that utilizes best-in-class security policies and procedures:

- **Password management and rotation** - Rules are designed to enhance computer security by strictly requiring users to employ strong passwords and use them properly.

BENEFITS

- *Best-in-class security policies and procedures to protect critical fax data*
- *Comprehensive security infrastructure helps customers adhere to important compliance mandates*
- *Layered approach for reducing risk of confidential information leakage*

- **Logical access controls** - Policies enforce access control measures
  for all systems, processes, and information.
- **Physical security** - Hardened data centers feature advanced physical
  security at each location.
- **Ongoing network monitoring** - This leads to consistent identification
  and, ideally, prediction of suspicious network activity.
- **Acceptable business use policies** - Users must agree to these rules in order to access our network.
- **Change management** - Business functions are stabilized by requiring support personnel to document and coordinate proposed changes to our underlying systems.

Secure Connectivity Protocols

Security protocols are vital in protecting customers' fax data, particularly in transit. The OpenText cloud fax network is an environment made up of connectivity protocols that keep customers aligned with their most pertinent regulatory compliance mandates. There are two secure connectivity protocols that OpenText deems mission-critical for helping cloud fax customers meet best-in-class certifications:

- **Secured web connections** – OpenText supports a variety of protocols for the secure transmission of fax data such as TLS and HTTPS.
- **Virtual private networks (VPN)** – OpenText enables fax transmission across both shared and public networks, as if it were directly connected to a private network. All of this takes place as OpenText customers benefit from the functionality, security, and management policies of a virtual private network.

In addition, OpenText maintains multiple layers of hardware and logical access controls to protect the confidentiality and integrity of customers' data. Components of this infrastructure include:

- **Firewalls** – Firewall rules block any and all paths to the network that are not explicitly required by the application. Multi-tiered firewall architecture provides defense-in-depth between Internet/client usage web tier, applications tier and stored data tier.
- **Network Segmentation** – Separate network segments are used for production, development, and QA environments. Internet-facing servers are located in DMZ network segments (separated from the core network by stateful firewalls).
- **Intrusion Detection/Prevention Systems** – IDS/IPS devices are used at the firewall to monitor and prevent unauthorized activity.
- **ID Management Solution (UAM)** – LDAP for authentication to production systems.
- **Network Vulnerability Scans** – Performed routinely by the Global Information Security team using approved scanning vendor protocols.
- **Anti-Virus** – Trend Micro and CLAM AV.
- **Log Analytics/Monitoring** – Handled by a combination of IBM Netcool, HP OpenView and in-house developed monitoring applications.
- **Encryption: Data at Rest and Data in Motion** – Symmetric 128-bit AES encryption. Encryption keys are rotated every 30 days.

Extra layers of fax data transmission protection, such as these, help diminish risk around confidential information falling into the wrong hands. Specifically, they help ensure information is delivered to the intended recipient in tamper-resistant formats that shield from corruption while allowing customers to take advantage of well-established information security systems. Secure connectivity protocols are behind the OpenText commitment to help cloud fax customers achieve best-in-class security certifications for driving compliance.

Compliance

The OpenText cloud fax network acts as a centralized information delivery center. Each phase of the delivery process is managed electronically and emphasizes data privacy throughout. The following is a list of compliance mandates OpenText helps customers adhere to as a result of a comprehensive security infrastructure offering.

HIPAA

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. It is a US Federal law that sets the standard for protecting the privacy and security of Protected Health Information (PHI).

OpenText helps drive HIPAA compliance, and is able to sign Business Associate Agreements (BAA) for the following services:

- OpenText™ Fax2Mail
- OpenText™ RightFax Connect
- OpenText™ RightFax Healthcare Direct

OpenText also maintains a comprehensive HIPAA Compliance Program to meet HIPAA/HITECH requirements:

- Annual HIPAA Risk Assessment
- Annual HIPAA Compliance Audit
- Annual Information Security Awareness Training
- Annual HIPAA Awareness Training
- Breach Notification Procedure

The following enhanced security features are also available in Fax2Mail to protect the security and privacy of Protected Health Information (PHI):

- Data encryption at Rest and in Transit
  - Symmetric 128-bit AES encryption.
  - Encryption keys are rotated every 30 days.
- Immediate Document Deletion
  - Document removed on final disposition of message.
- Encrypted Archiving
  - Documents archived with encryption enabled.
- No Archive Option
  - Customer may choose not to archive transactions.
- HIPAA Viewer Option
  - Restricts OpenText support personnel from accessing and viewing customer data.

OpenText maintains a HIPAA compliance program for the following processing locations:

- Ashburn, Virgina
- Tinton Falls, New Jersey

SOC 2, Type II

The Service Organization Control (SOC), SOC 2, Type II, defined by the American Institute of Certified Public Accountants (AICPA), is recognized worldwide as one of the strictest audit standards for service providers. It has been designed to meet the needs of the growing number of IT and cloud computing companies.

SOC2 allows the audited organization to demonstrate that it meets and exceeds the industry's accepted standards governing controls and protection of all hosted and processed data, on behalf of clients. SOC 2, Type II reporting is geared toward controls at service organizations relevant to five Trust Service Principals (TSP):

- **Security:** The system is protected, both logically and physically, against unauthorized access.
- **Availability:** The system is available for operation and use as committed or agreed to.
- **Processing Integrity:** System processing is complete, accurate, timely, and authorized.
- **Confidentiality:** Information that is designated "confidential" is protected as committed or agreed.
- **Privacy:** Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with the privacy principles put forth by the AICPA and the Canadian Institute of Chartered Accountants (CICA).

OpenText maintains a SOC2, Type II compliance program for the following processing locations:

- Ashburn, Virginia
- Slough, United Kingdom
- Tinton Falls, New Jersey
- Tokyo, Japan

PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of data protection mandates developed by the major payment card companies and imposed on businesses that store, process, or transmit payment card data.

As part of their contracts with the card companies, merchants and other businesses that handle card data may be subject to fines if they fail to meet the requirements of PCI DSS compliance.

The PCI Data Security Standard specifies 12 requirements for compliance, organized into six logically related groups called "control objectives."

At a summary level, the PCI compliance checklist for merchants and other businesses that handle payment card data consists of 12 requirements mandated by the PCI DSS:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

OpenText maintains Level 1 Service Provider PCI Compliance for the following data center:

- Ashburn, VA.

OpenText maintains a comprehensive PCI Compliance Program to meet PCI DSS requirements and undergoes annual third-party QSA PCI certification audits.

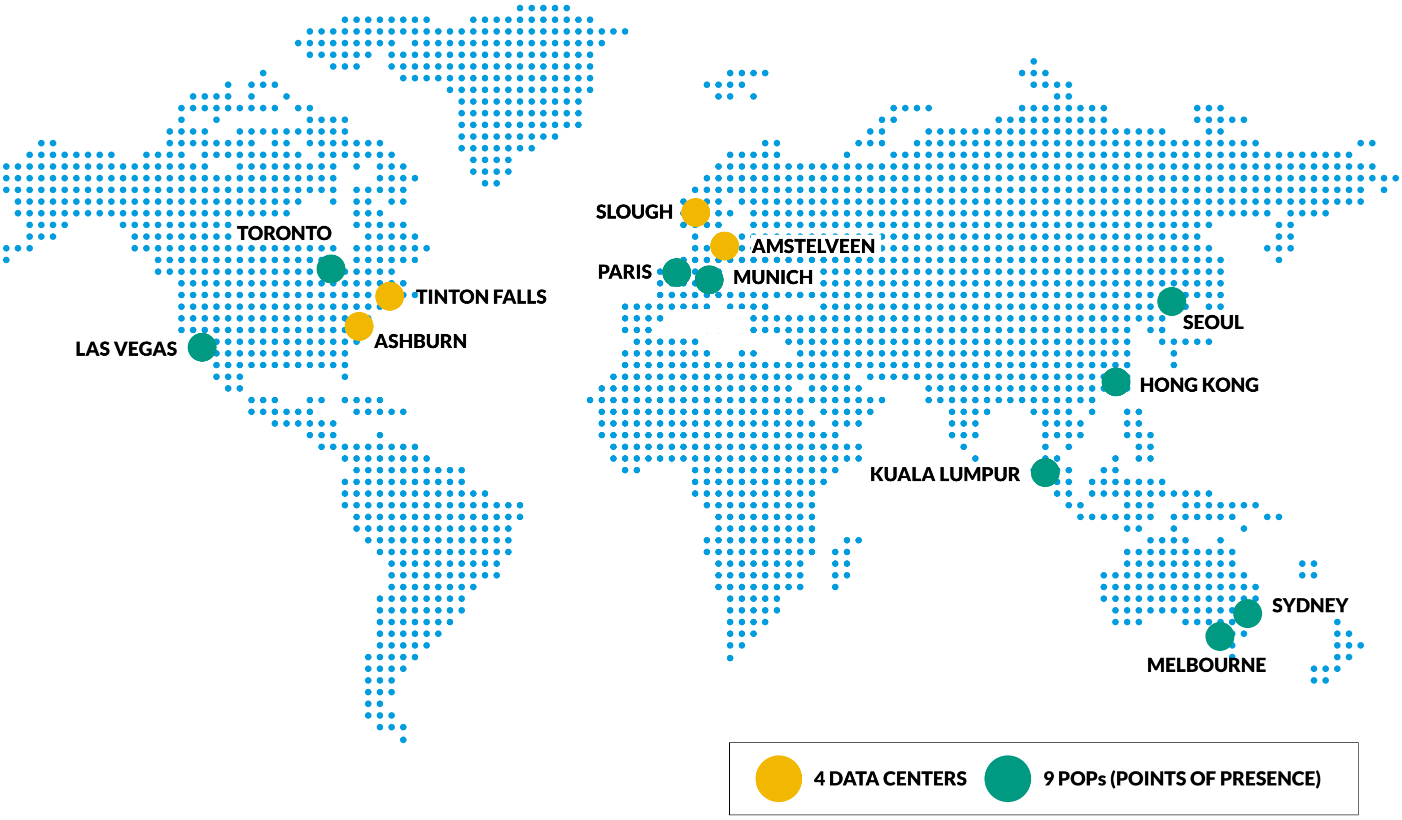
The OpenText Cloud

The OpenText Cloud helps customers rapidly integrate data and process flows both within their organizations and with their business partners. The network has global reach and scale that enables OpenText to address even the most complex enterprise information management challenges. The OpenText Cloud is built on a sophisticated, secure, and global platform infrastructure that has delivered superior, enterprise-grade transactions in total:

- $6.5 trillion in commerce from transactions processed annually
- $350 million plus investment in cloud fax infrastructure
- 2 billion faxes
- Customers served, 24/7
- 99.5% plus Network Availability Service Level Agreements (SLAs)

Size and Strength of the OpenText Cloud

OpenText Cloud faxing is supported with five geographically dispersed data centers and nine more points-of-presence around the globe, making it the largest network for faxing in the world. Additionally, the OpenText Cloud has two data centers in Europe for 100% in-region processing for complete data sovereignty. The OpenText Cloud is built on a sophisticated, global infrastructure that delivers superior, enterprise-grade service.



faxsolutions.opentext.com

NORTH AMERICA +1 800 304 2727 • EUROPE, AFRICA +31 (0)23 565 2333 • MIDDLE EAST +971 4 390 0281
JAPAN +81-3-4560-7810 • SINGAPORE +65 6594 2388 • HONG KONG +852 2884 6088 • AUSTRALIA +61 2 9026 3400