



Job Submission Security	
IP Address Restriction	Allows only approved IP addresses to communicate with network clients
Basic Access Authentication	Authenticates remote users of Internet Services or Printing Protocol
Digest Access Authentication	Allows Web user identification to be established without a password
SSL/TSL for Web Submission	Restricts user access and defines encryption strength
Queue Lock	Feature enables the System Administrator to lock and unlock the queue
Network Security	
Firewall	Restricts access via IP filtering, domain filtering, and port blocking
Network Authentication	Restricts access to scan, email, and network fax features
Microsoft® Active Directory Services Feature	Reuses existing security accounts for authentication
IEEE 802.1x Support	Ensures devices connected to the network are properly authenticated
IPSec Support	Encrypts print jobs sent over the network with IPSec
IPv6 Support	Built-in support for networks utilizing the IPv6 standard
SNMP v3.0 Support	Enables network management of Xerox devices via SNMP-compliant applications
Device Security	
Hard Drive Erasure	Completely and permanently deletes all files after printing
Audit Logging	Tracks system activities, including print activities by user, time, and date
GUI Logging	Tracks mouse clicks within GUI by user
Device Access Password Protection	Device login utilizing network user name and password
Hide Job and User Name Display	Hides job details when non-authorized users view job queue
MICR Secure Mode	Disables all features that allow additional prints
Removable Hard Drives	Remove and protect classified or confidential information
Disk Overwrite	Electronically shreds data stored on the hard disk
Secure Web Page	Enables authorized user access to network features and management settings
Document Security	
Digitally Signed Documents	Creates signatures using a variety of methods, including S/MIME
Encrypted PDF	128-bit RC4 or 128-bit AES encryption
Specialty Imaging Text	Makes it virtually impossible to duplicate prints

Note: Features vary by product.

Call for protection. We have experienced analysts waiting to assess your organization's document security requirements and to work with you to develop a plan to ensure that they're met. To begin the process or to learn more about security features for specific products, call 1-800-ASK-XEROX or visit [www.xerox.com/security](http://www.xerox.com/security).

To learn more about Specialty Imaging Text, visit [www.xerox.com/freeflow](http://www.xerox.com/freeflow).



# Security Capabilities

## Protect your business-critical information with Xerox.



# It's your confidential data. We help you keep it that way.

## Secure Documents



**Protecting sensitive, proprietary, or classified information is more critical than ever.** As more information is being created, distributed, and archived digitally, the risk that this data could be intercepted or corrupted increases.

Without the proper protection, hackers, disgruntled employees, or even spies can gain access to you or your customers' sensitive business information and make it public record with the click of a mouse.

And as if matters weren't complicated enough, many industries must now comply with government and state regulations, not to mention satisfy a customer base with deep privacy concerns.

Thankfully, Xerox has the security capabilities to help. For the last 20 years, Xerox has been a leader in providing secure document solutions to a variety of industries across the globe. In fact, every Xerox product and service we offer was designed with security in mind and to seamlessly integrate into existing security frameworks—giving you and your customers more protection and peace of mind.



## Xerox Security Goals

We've identified five key security goals in our quest to provide secure solutions to every one of our customers:

Confidentiality	Integrity	Availability	Accountability	Assurance
<ul style="list-style-type: none"> <li>No unauthorized disclosure of data during processing, transmission, or storage</li> </ul>	<ul style="list-style-type: none"> <li>No unauthorized alteration of data</li> <li>System performs as intended, free from unauthorized manipulation</li> </ul>	<ul style="list-style-type: none"> <li>Systems work properly</li> <li>No denial of service for authorized users</li> <li>Protection against unauthorized use of the system</li> </ul>	<ul style="list-style-type: none"> <li>Actions of an entity can be traced directly to that entity</li> </ul>	<ul style="list-style-type: none"> <li>Confidence that integrity, confidentiality, availability, and accountability goals are being met</li> </ul>

## Secure Documents

Used to share ideas and thoughts, or to provide a written account of ownership or obligation, documents provide the basis of business communication. As the use of computers continues to increase, so does the number of documents created every day.

Due to the fact that documents often contain valuable information such as trade secrets, document management and protection has become vital to every organization. Xerox recognizes this need and has created a variety of security solutions to help.

## Xerox Document Security Features Include:

### Digitally Signed Documents

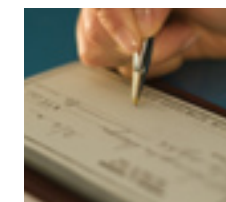
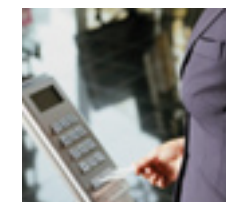
- Creates a signature using a variety of methods, including S/MIME.

### Encrypted PDF

- 128-bit RC4 or 128-bit AES encryption for PDF files.

## Specialty Imaging Text

- Enables users to add a level of security and authentication to documents using a FreeFlow® Print Server. It includes MicroText Mark, Correlation Mark, GlossMark®, Infrared Text, and FluorescentMark, which can be used in the healthcare, financial services, federal government, and higher education industries for a variety of applications.



## Healthcare

Add hidden lines, text, or graphics to identification cards or bracelets and parking passes with Specialty Imaging Text to ensure authenticity. It can also be used to create fraud-resistant prescription pads, which contain hidden elements to make it virtually impossible to counterfeit them.

## Government

Increase security by developing fraud-resistant identification badges, letterhead, certificates, and more. Virtually any output can have built-in security features with Specialty Imaging Text.

## Financial Services

Use Specialty Imaging Text to create identification cards with built-in security features, including content that's only viewable under direct UV light. Fonts and graphics can also be used to authenticate checks, corporate letterhead, customer statements, and more.

## Education

Ensure event tickets, parking passes, identification cards, diplomas, and more are legitimate by embedding Specialty Imaging Text into each document. Using more than one font adds multiple layers of security, making it even harder and more costly to make forgeries.



**Security is not optional.** Customer privacy concerns and government security regulations are changing the way many industries conduct business today. Here, you'll learn more about the industries experiencing the most change and the security challenges they're facing.

### Secure Devices



#### Secure Devices

Today's digital presses can print on demand, copy, scan to network destinations, send email attachments, and more. Available in full color or monochrome, each is designed to maximize productivity and increase the profitability of the organization using them.

However innovative, devices are not immune to security threats. If not properly protected, they can provide an entry point for hackers to access your network or allow employees to print and remove classified data without your knowledge. Xerox security solutions can prevent these problems before they happen.

#### Xerox Device Security Features Include:

##### Hard Drive Erasure

- Algorithms completely and permanently delete all files after printing.

##### Audit Logging

- Tracks print, scan, and network fax activities by user, time, and date.

##### GUI Logging

- Tracks mouse clicks within the Graphic User Interface (GUI) and associates them with the current user.

##### Device Access Password Protection

- Device login utilizing network user name and password.

##### Hide Job and User Name Display

- Hides job details when non-authorized users view job queue.

##### MICR Secure Mode

- Disables all features that allow additional prints to be produced (e.g., Sample Print, Reposition Output, etc.).

##### Removable Hard Drives

- Remove and lock up storage drives when system is not in use to protect classified or confidential data.

##### Disk Overwrite

- Performs a multiple overwrite of the partitions that contain customer jobs.

##### Secure Web Page

- Enables authorized users access to network features and management settings.

#### Healthcare

Thanks in large part to advances in information technology—including the use of hand-held computers—the healthcare industry is experiencing all-time highs in patient care and worker efficiency. However, these innovations have also created the need to share important medical data and patient information electronically—and that's where security becomes a major concern.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was put in place by the federal government to force all healthcare organizations to apply uniform data management practices to protect patient information and patient privacy at all times. Under HIPAA, an audit trail is required to track who viewed data, when they viewed it, and if they had the proper authorization to do so.

#### Government

Today, local, state, and federal governments have put an emphasis on simplifying processes and improving cross-agency collaboration to provide better outcomes for the citizens they serve. To do so, they're employing various initiatives to take advantage of the latest technologies, while putting strict regulations in place to ensure the information being shared is safe and secure.

The Federal Information Security Management Act of 2002 (FISMA) was established to bolster computer and network security government-wide. It requires that all networked devices—including those used by contractors—meet strict information assurance goals such as integrity, confidentiality, and accountability.

#### Financial Services

Direct deposit, online banking, debit cards, and other advances in information technology are revolutionizing the financial services industry. Today, more business is being conducted electronically than ever before. Though more convenient for both customers and businesses, this heavy use of technology has its own set of security concerns.

The Gramm-Leach Bliley Financial Services Modernization Act of 1999 (GLBA) was instituted to ensure financial institutions that collect or receive private customer data have a security plan in place to protect it. To reach compliance, organizations must complete a risk analysis on their current processes and implement firewalls, restrict user access, monitor printing, and more.

#### Education

Today's educational institutions—including K-12, colleges, and universities—are a hotbed of technology. Transcript requests, financial aid applications, and even class notes can all be found online. Since some schools have their own medical centers, they also have to store and share medical information electronically. This interactive environment enhances the student experience and improves staff productivity, but it also makes schools susceptible to security threats.

Since these institutions manage a variety of information, many state and federal regulations apply, including the Computer Fraud and Abuse Act, USA Patriot Act, HIPAA, and GLBA. However, the most applicable regulation to the education industry is the Family Education Rights and Privacy Act (FERPA).

This act prohibits the disclosure of personally identifiable education information without the written permission of the student or their guardian.

**With so many regulatory and compliance measures to respond to, Xerox has looked to the federal government requirements, among others, as guidelines. By developing solutions that strive to meet the most stringent security standards, we can offer highly secure solutions to all of our customers—regardless of business sector.**

# Secure from start to finish.

Xerox production printing solutions provide end-to-end security solutions that allow you to restrict access, track usage, and protect the data that flows through your entire system during day-to-day operations. With standard and optional security features at every step of the document life cycle, we can help ensure your information is safe and secure.

## Secure Job Submission



### Secure Job Submission

Since the introduction of digital printing, job submission has evolved from a manual process to a fully automated one. Today, customers can submit, manage, reorder, and output their digital jobs anytime, anywhere using an online print center.

Online job submission is convenient for your customers, but it can also be a convenient entry point for hackers to access your system. Proper protection is critical to make sure that only authorized users are logging in to your system remotely. Xerox job submission security features can do just that.

### Xerox Job Submission Security Features Include:

#### IP Address Restriction

- Allows only approved IP addresses to communicate with specific network clients.

#### Basic Access Authentication

- Industry-standard method of authenticating a remote user of Internet Services (HTTP) or the Internet Printing Protocol (IPP) and Digest Access Authentication (DAA).

#### Authentication Feature

- Maintains security by allowing only authorized users to access the system.

### SSL/TLS for Secure Web Submissions

- Provides ability to restrict user access while user selectable encryption strengths provide additional security.

### Queue Lock

- Queues can be locked and unlocked by the System Administrator. Also, the operator can change Accept/Do Not Accept and Release/Do Not Release Jobs attributes.

## Secure Networks



### Secure Networks

The positive impact networks have had on business over the past 15 years is undeniable. They've enabled email, Internet, remote printer access, and file sharing—boosting productivity in organizations all over the world.

Though networks have many positives, they also have always come with one underlying concern: security. How do you ensure that they're properly protected so intruders can't gain access to confidential information? Xerox security solutions can provide you with the protection you need.

### Xerox Network Security Features Include:

#### Firewall

- Restricts access via IP filtering, domain filtering, and port blocking.

#### Network Authentication

- Restricts access to scan, email, and network fax features.

#### Microsoft® Active Directory Services Feature

- Reuses existing security accounts for authentication.

#### IEEE 802.1x Support

- Ensures devices connected to the network are properly authenticated.

### IPSec Support

- Encrypts print jobs sent over the network with IPSec.

### IPv6 Support

- Built-in support for networks utilizing the IPv6 standard.

### SNMP v3.0 Support

- Enables network management of Xerox devices via SNMP-compliant applications.