RICOH
imagine. change.

Ricoh essentials security guide

Layered security for today's digital workplace

Hybrid work and the need to operate in a digital-driven world has accelerated transformational change for organizations as they modernize capabilities and broaden potential markets. As organizations work towards a modern workplace, the resulting fragmented landscape of tools and technologies reveal security, privacy, and operational gaps.

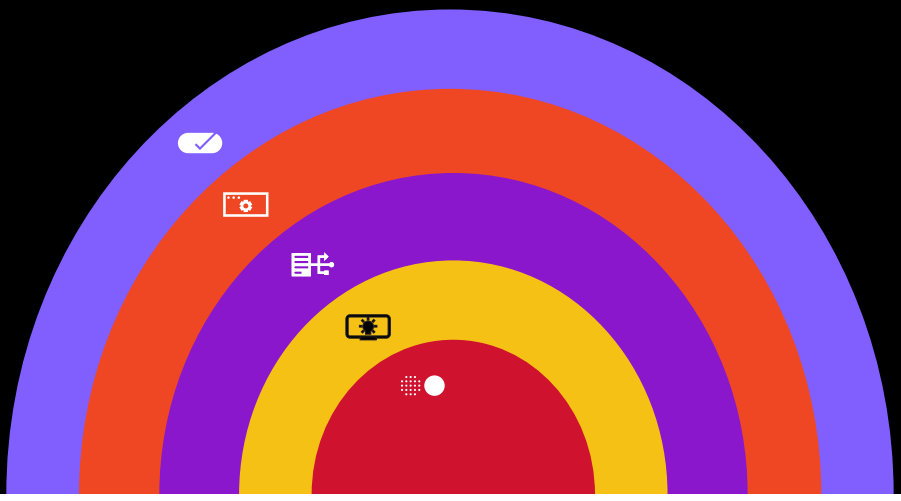
Keeping things secured — protecting processes, systems, applications, and devices from data breaches — is a never-ending, worry-driving effort that weighs on the minds of leaders. Not only does every attack cost the business financially, but it also puts the entire organization at risk.

As risks increase, organizations must secure their digital investments, and consider the growing demand from partners, customers, and regulators to comply with security requirements. Ricoh delivers the tools and expert guidance today's organizations need to safeguard information, build brand trust, and protect core investments. We do this with a strategic, multi-layered approach that covers potential vulnerabilities and threats across all areas of the business.

All our services, solutions, and devices are designed with a security-focused, data-driven approach from the start of product design through implementation. Our industry-leading security services — including consultancy and managed services — complement our device and solution security layers to optimize document, data, device, and information security.

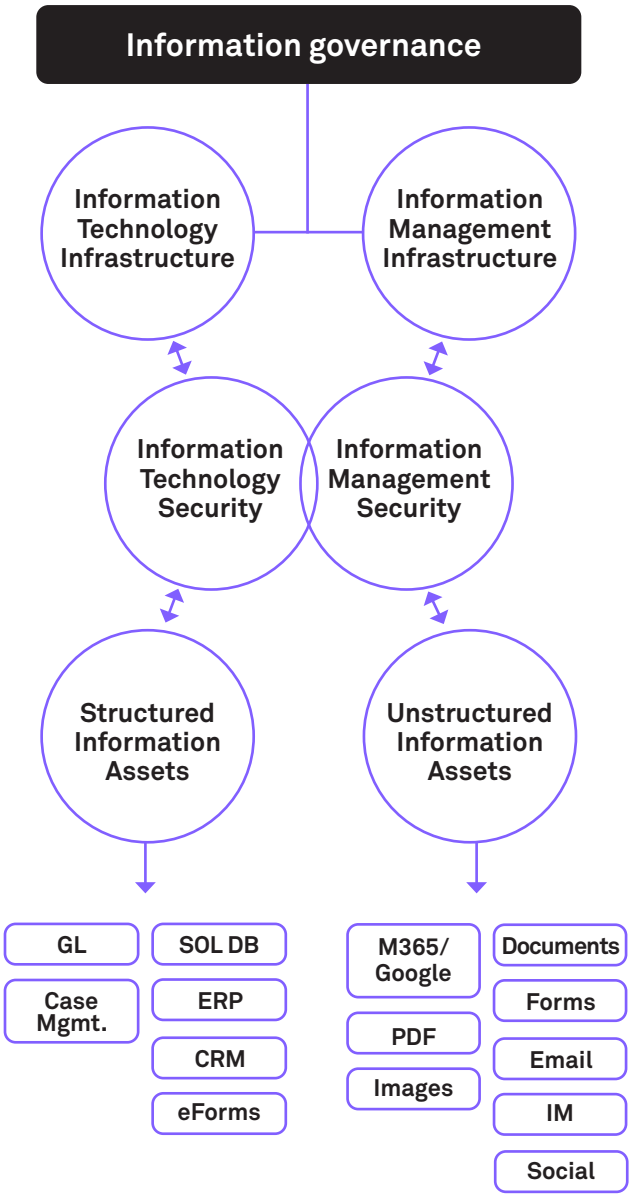
In this overview, learn how Ricoh's robust portfolio of services, solutions, and devices utilize a multi-layered security approach that protects your business and enables you to grow with confidence.

- **Process & Information Security**
- **Systems Security**
- **Application Security**
- **Device Security**
- **Data Security**



Layer 1 – process and information security

Digitalization requires the integration of digital technology across all areas of the business, fundamentally changing how we operate and deliver value to our customers. It also brings a cultural change that requires employees to adapt to a more dispersed workplace, adopting new processes that can enable them to be productive both in the office and remotely. Business leaders must adapt and become aware of process and data security risks.



Information governance

Poor information administration practices can expose any organization to a variety of risks that can lead to significant financial penalties and reputational loss. Understanding what information and data you need to keep, and how you can improve the way it is managed, reduces these risks and protects you from scrutiny.

Information governance security services support establishing and maintaining ongoing information confidentiality, integrity, and availability. These focused services assist organizations in meeting security policies and achieving compliance with a variety of federal, state, and industry regulations — including the ability to audit and demonstrate compliance in an efficient manner.

Every digital transaction between businesses and their customers produces a trail of data. Data may be highly sensitive, requiring security, privacy, and discovery controls; other data has no value and simply takes up space, commonly referred to as ROT (redundant, obsolete, or trivial) data. It is estimated that ROT data accounts for a minimum of 25-30% of company data, with other sources saying it can be much higher.

Knowledge of the information you have and where it's located is a fundamental first step to information security. Ensuring the protection of sensitive data such as personally identifiable information (PII) and payment card industry (PCI) information is critical in mitigating potential risk.

90%+ of data is unstructured[1]

Unstructured data is information that hasn't been organized into a traditional, structured database format, which means it isn't accessible, tracked, or leveraged for business insights. Without managing your repository — most of which is unstructured — you're at risk of storing high quantities of ROT data and exposing your organization to risk and vulnerability if breached.

Unstructured data is a key contributor to security breaches, privacy violations, high IT costs, and compliance penalties. When considering cybersecurity, unstructured data is often the low-hanging fruit cyber criminals will target to gain access to deeper systems. They are looking for things they can monetize, such as names, addresses, dates of birth, social security numbers, passwords, credit card numbers, banking information, or contracts. Unfortunately, this sensitive data is often found throughout the infrastructure, making it difficult to track and keep secured.

Here are four key areas to improve the handling of data and information governance:

1. **Data discovery solutions**

   Automated data discovery solutions are an efficient and secured way to identify and locate sensitive data ownership and permissions across unlimited endpoints. Protect your organization by reducing ROT data assets, proactively managing the lifecycle of your data, and ensuring compliance with privacy regulations. Data discovery also remediates data by restricting access, encrypting, archiving, redacting, or moving sensitive data to secured locations.

2. **Data lifecycle management**

   This security best practice seeks to mitigate an organization's risk through the management of data, including sensitive and valuable information throughout the entire information lifecycle. Ricoh professional services and managed services teams can assist in any step of this process.

3. **File analysis**

   The nature of your data is as varied as your business. Your responsibilities for safeguarding it and opportunities to benefit from it are hindered without reliable knowledge of what you have. By performing automated analysis of your file repositories and email systems, you can identify sensitive and valuable data and take necessary actions. Thorough file analysis is not just a point in time event — best practices state it should be incorporated into ongoing workflows.

4. **Data classification**

   Data classification uses automated AI-based technology to categorize or index your documents so the data can then be easily extracted, exported, accessed, and protected. Implementing a system to classify your data can strengthen your security and enforce policies. It can also transform data generated from various physical and digital workflows into intelligence to enable better decision-making, more responsive customer service, and efficient operations. Ricoh security and process specialists have a deep understanding of information generated from print and digital workflows as well as archiving and email security — so the right approach is applied when classifying your data.

[1] IDC. "High Data Growth and Modern Applications Drive New Storage Requirements in Digitally Transformed Enterprises," July 2022.

Transaction and process automation

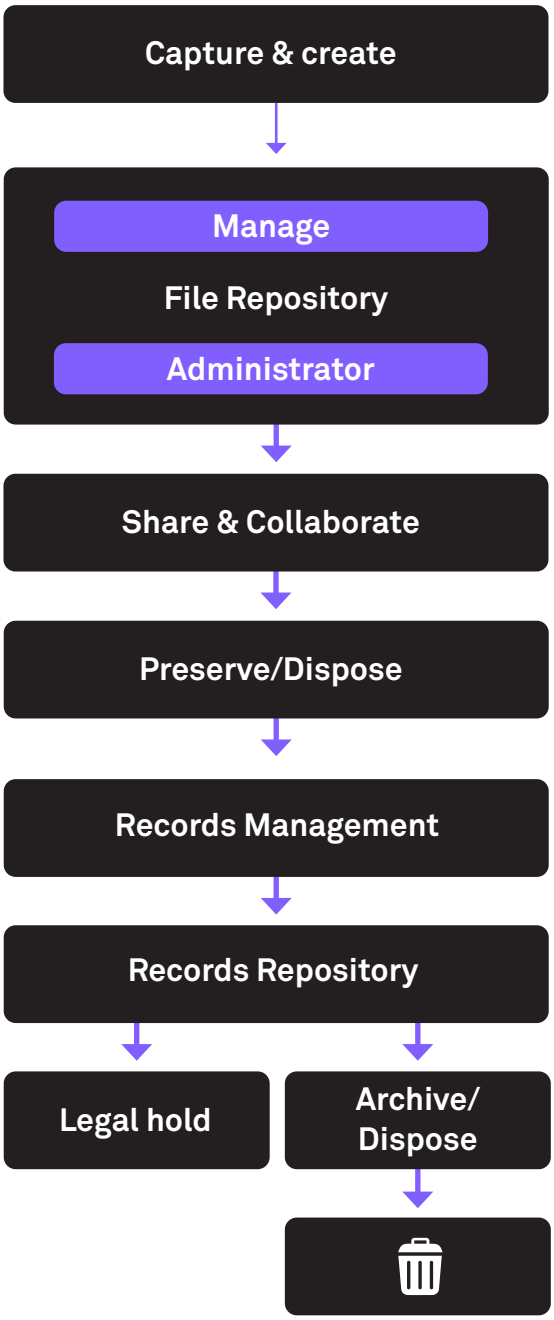
Most transactions and business processes essentially follow a similar path. We collect or capture information, store and manage it, share and collaborate with the information, and then preserve or dispose of the results.

As the way we communicate, collaborate and create evolves, the need for secured and sustainable solutions becomes more apparent. The core of what we do — sourcing, creating, capturing, and managing information — is integral to success, and, therefore, must be protected from potential threats.

Automated business processes streamline how information moves and flows through your business, which is especially important with hybrid workplaces and remote workforces that need secured access everywhere.

Robotic process automation (RPA) provides organizations with a virtual workforce or bots that tackle repetitive business tasks, accelerating the way we work. RPA tools have their set of security standards with measures such as enterprise-grade encryption, role-based and permission access, Active Directory authentication, database encryption, and more.

Inbound information such as email, mail, web form submissions, document scans, and e-commerce must be received and handled securely. Integrating them with secured, automated workflows helps ensure data is safe and assists with information governance and compliance.



Common processes where intelligent business platforms, such as data capture and workflow applications, can be applied are:

- Invoice processing
- Loan processing
- Claims management
- Human resources onboarding
- Patient records and forms
- Student transcripts and records
- Maintenance and sales orders

Outbound information is subject to the same security and privacy requirements; it's the organization's responsibility to determine whether the information you produce and distribute should be encrypted, require user authentication, or be tracked.

Business leaders should consider these processes:

- Accounts payable
- Secure e-signatures
- Mail processes
- Customer communications

Automating processes uncovers new possibilities for the way people work and offer many benefits — but digitized data requires focused protection from the point of origin and throughout its lifecycle. Scanned paper documents, fax transmissions, form submissions, captured images, and other data enter your organization's systems through various methods, which warrants scrutiny of how you protect that valuable information.

Secure capture and digitized documents

Automating data capture, classification, extraction, and export can accelerate the flow of information, providing convenient access to those who need it. Controlling and governing access to information — especially sensitive information in digital formats — requires formidable security capabilities across multiple touchpoints.

Sensitive data can be personally identifiable information (PII), proprietary, intellectual property (IP), or fiduciary, among others, and can lead to hefty fines if not safeguarded. However, if the data is to be protected, it must be transformed from unstructured data into actionable, structured data. Let's explore how intelligent capture and secure eForm solutions can protect your valuable data.

1 Intelligent document capture processes

Intelligent capture solutions transform documents into a structured, secured format so data can be exported into any workflow, application, or repository, such as ERP, ECM, CRM, RPA, iPaaS, analytics, or line of business system.

The documents must first be digitized or scanned. During the scanning process, authentication methods validate authorized users and administrators can lock down access to certain processes — even limiting what users can see — to prevent improper use. You can also protect converted files with permission settings and password control.

Most intelligent capture solutions do not store data; they simply pass the digitally transformed data through to other applications or repositories. Since information can be vulnerable to compromise if intercepted, security measures are used to protect data in use. Cloud services also make use of built-in encryption, decryption, authentication, and use Transport Layer Security (TLS) for transmission.

2 Secure eForms

Electronic forms provide a consistent way of submitting structured information into a system and can provide a secured option to the alternative paper or email approach. However, improperly coded or unprotected electronic forms can pose a security risk.

A form that has not been secured correctly can be a gateway to falsified information or attempts to introduce malicious code. Intelligent forms creation software can do the hard work for you, behind the scenes — constructing proper forms with features including electronic signature fields, location services, access control, attachment management and, most

importantly, workflow management. Monitor and analyze your form-based workflows with full tracking of critical processes and approve or deny form submissions before they continue to their destination.

Secured management and administration

Securely managing large volumes of data while complying with regulatory controls and audits can be daunting. However, a data system that handles your information securely, seamlessly automates your workflows, and enables remote access is critical to optimizing your hybrid workplace's business processes.

How do you achieve this while ensuring your data is protected from outside threats, internal security breaches (accidental or deliberate), data loss, or compliance violations?

1. **Document management services and solutions**

   Effective document management solutions provide much more than just a secured storage repository. Access controls limit use to only those who have authorization, along with permissions control of who can view, share or update certain documents. When document activity is tracked, you know who is viewing and using your data.

   Audit trails provide a record of this activity and custody down to the individual document level. With versioning and retention policies, you can ensure documents are handled in accordance with financial, legal, or other requirements. Whether a document management solution is delivered as a cloud service (such as DocuWare) or deployed on-premises, stored files are protected at rest, during transmission, and at the time of access. This is accomplished through encryption, secured transmission, and various options for file controls.

2. **Controlled print output**

   Multifunction printers bring efficient output to multiple users, along with the capability to protect printed information. Whether printing from desktop computers or mobile devices, outputting sensitive information remains in the authorized person's control. In addition, full-featured cost control tracking and chargeback provide comprehensive accountability of user behavior and a way to identify out-of-the-ordinary patterns or abuse.

3. **Secured document release**

   By incorporating Secured Document Release, sensitive information printed to centralized servers or cloud services will not be picked up by mistake or by anyone seeking to steal confidential information. Instead of submitted print jobs going directly to a device, they are encrypted and held in the originating user's print queue.

   The user can only release the print job when they are present at the device of their choice and have provided authentification. The print queue can reside on-premises or in the cloud, and print data can be sent over a secured web connection and encrypted in transit.

4 Mobile printing

With a changing workforce, mobile device printing is a critical capability in many organizations. Enabling this involves both process and technology infrastructure considerations. On the process side, users can prevent sensitive information from being left unattended at a printer by using authenticated print release with their mobile devices.

Printer selection is handled on the mobile device, and output takes place when someone is present to securely release and retrieve the information. For infrastructure, you can protect print stream data and manage mobile printing processes with various deployment choices — depending on security policies. These can include both an on-premises mobile print server(s) or an off-premises mobile print cloud platform. Activity from mobile devices can be tracked alongside traditional printing with user/device detail reporting — so that mobile printing is tracked. Mobile device management can also be supported.

5 Authentication and usage

Preventing the misuse of resources reduces operating costs, restricts user activity to enforce accountability, and provides insight to spot irregularities through reporting.

Printing rules can include setting page limits by device, restricting color usage, enforcing duplex, restricting access to certain settings, and more. Budgetary account limits for copying and printing can be set up by the user — and include tracking walk-up activity at a multifunction printer.

Because users must authenticate to print, the print rules you set are automatically enforced and activity is attributed back to the user. You can associate document printing, scanning, and faxing to a specific client/matter for the purpose of billing — which enables detailed activity reports around a project or confidential topic.

Secured sharing and collaboration

Sharing and collaborating may involve both sending and receiving information. It may rely on several systems validating information or it may involve human-in-the-loop processes that include all of the above. Information may be used internally or externally, or both, and it may be integrated into a collaborative system such as Microsoft Teams. Key considerations include how the collaborative systems use the information, and what the end state of the information will be when derived through the process.

1 Advanced faxing

Decrease the risks associated with stand-alone fax machines and replace manual routing with an automated delivery process. A safer method to get faxes into the hands of just the intended recipient often includes taking advantage of secured authentication, encrypted protocols, encrypting data at rest, and routing rules. This automation eliminates paper handling and reduces the risk of paper documents being picked up by unauthorized persons.

With administrative control over your fax environment, you can address compliance and policy requirements using several features — including verifiable document transmission and receipt, full audit trails of activity, and access to archived faxes of all inbound and outbound transactions.

Secured preservation and disposal

It's too easy to lose track of how much sensitive data your organization has, where it's located, and who has access to it. Without clear visibility of your organization's sensitive data, risk increases, and your organization cannot meet baseline security requirements.

1 **Retention and disposal**

Information policies determine the lifecycle and handling of different classes of data. Retention policies can determine when and how data is moved from your active repositories into an archived state, moved into an off-site cloud repository, or expunged from systems as warranted by policy. End-of-Life Information Disposal Services encompass cleansing data from multifunction devices to ensure that the NVRAM and drives of retired customer devices are wiped clean before disposal.

Layer 2 – systems security

As organizations digitalize their processes, IT professionals are tasked with delivering a seamless work experience in and out of the office, supporting all lines of business, and ensuring systems and data are protected.

Now, many customers require a work environment that is completely online. From communication to file storage, applications to user identities, and security, servers, and email — everything in the work environment must be accessible remotely and securely in the cloud.

The company's data and systems now operate within a borderless world of work. As employees access the network and applications from any location or device, attack surfaces multiply while threats, such as ransomware, are on the rise. Even the smallest crack in a network's defenses can bring serious consequences for the business.

Ricoh offers a robust portfolio of IT services and solutions that enable seamless and secured digitalization across all areas of your business. Let's explore the options.

Perimeter security

In today's workplace, where users frequently work remotely and systems and data often aren't located within the physical office space, the boundaries that once defined what was inside and outside of the network have been blurred, introducing new vulnerabilities, and making security management more complex.

1. **Firewalls**

   Firewalls are designed to protect your network's infrastructure and improve site-to-site connectivity. Today's most advanced firewalls provide enhanced capabilities that allow real-time protection against malware, vulnerabilities, and network attacks. Intelligent analysis allows for deep application context, combining human and machine learning to apply rules specifically to allow or deny traffic.

2. **Identity and authentication management**

   Using only a password to authenticate users leaves organizations vulnerable to external threats. If a password is weak, brute force attacks can crack it within seconds; and, if it's exposed elsewhere, you're essentially handing cyber criminals the keys to your network. Introducing additional layers of authentication (multi-factor authentication or MFA) makes access more difficult for attackers. Password authenticators verify the user's identity by comparing entered credentials against records in an authentication server. If a match is found, the system will grant access.

   When data is shared across disparate technology solutions, it's very difficult to track the identity of users. That's why many organizations bring the entire work environment into a single cloud-based environment where identities, apps, files, and devices are all managed centrally. Microsoft Azure Active Directory is a leading platform that offers deeper levels of authentication and access control. For example, the ability to limit access to a specific region and enhanced user authorization features can create a more secured workplaces.

3 Penetration testing

How secure is your data? The only way you can know for sure is to test your current security by trying to get in from the outside, the way a hacker would. Testing like this reveals where your network is strong — and where you require deeper security protection.

Penetration testing and assessments will uncover weaknesses in your networks, applications, and security controls. It can also confirm the effectiveness of the various security policies, procedures, and technologies.

Testing should focus on malware analysis, reverse engineering, cryptography, exploit development, offensive and defensive security, and should provide clear, actionable insights with next steps for effective remediation.

Network security

As organizations continually shift to hybrid work, and allow users to regularly log into the network from outside the office or on unsecured devices, the need for securing access within the network has increased. Increased digitalization of processes means a larger volume of data in rest, motion, or use, exposing organizations to risk. That's where vulnerability assessments come in.

A vulnerability assessment is comprised of two components:

- Vulnerability scanning and reporting
- Analysis and remediation planning

Ricoh security engineers scan externally facing assets for vulnerabilities such as missing patches, outdated software versions, open ports, and operating system services.

From there, we report the findings and develop a remediation plan tailored to the customer. Vulnerability assessments can be conducted on a recurring basis or as a point-in-time service.

Endpoint protection

Endpoints are today's most common entry points for malware, ransomware, and social engineering. If a cyber criminal gains access to one of your endpoints, they can potentially find ways to burrow further into the network to access sensitive data or launch large attacks.

It's not enough to buy antivirus software and simply set it and forget it. Robust endpoint security allows you to protect your systems anytime employees access the network using devices such as smartphones, laptops, or tablets.

We can also provide the staff, time, and knowledge to assist with the creation and deployment of print device security policies, standards, and settings across a customer's entire fleets, including both Ricoh and other vendors' devices.

1 **Anti-virus software**

Anti-virus software falls into three primary categories: signature-based, behavior-based, and machine learning.

- **Signature-based:** The signature method compares the code of a suspicious file to a database of known malware signatures. If there's a match, the file is immediately flagged and blocked, contained, or deleted.
- **Behavior-based:** This software analyzes the behaviors of a file (such as rapid encryption), which enables it to discover new malware it hasn't seen before. Because cyber criminals are constantly evolving and developing new strains of malware, this provides much stronger protection than signature-based solutions.
- **AI-based:** Machine learning-based software is the latest and most robust type of anti-virus protection, applying algorithms and datasets to detect malicious patterns in malware on individual devices and across large networks.

2 **Web filtering**

Providing protective security and content filtering minimizes risks and maximizes safety as a critical component of defense. Filtering is commonplace for email, tools often referred to as anti-spam, email security, or email filtering. While providing email protection is important, it is only half the filtering solution.

Managed web filtering is designed to block malicious domains that may include harmful content such as ransomware, malware, viruses, and data phishing. Optionally, specified content types may be blocked based on individual business needs to prevent access to domains that may contain adult, gambling, crypto mining, dating, or other prohibited content.

3 **Mobile device management**

Mobile device management applications such as Microsoft Intune can be leveraged to deploy application management when securing apps on a user's mobile device limiting data migration. It can be leveraged when securing an entire mobile device, also protecting against malware and enabling complete removal of company data in the event of a threat or employee departure.

Expert cybersecurity management

Being prepared starts with embedding intelligent cybersecurity services and solutions into your core business processes and ensuring rigorous management by IT cybersecurity experts.

Continuously evolving threats require uncompromising and focused management of systems, devices, and environments. IT teams are under more pressure than ever to maintain operations, enable lines of business, and deliver user support. Outsourcing your cyber protection to a dedicated team of experts will free up your IT department to focus on core capabilities without their attention being diverted. A distracted, overwhelmed IT team invariably leads to gaps in security, with potentially disastrous outcomes.

Ricoh's expert-driven cybersecurity services and solutions can help you build a more resilient IT infrastructure, understand and manage your vulnerabilities, and enable you to grow with confidence.

Layer 3 – application security

While software is designed to accelerate efficiency and productivity, it can also pose risks. Embedded software applications, installed apps, and software running as cloud services can be potential targets for breaches. Therefore, your data must be protected.

Similar to securing your devices, your organization must also secure both your software applications and the data those applications generate. Safely managing all that data is a challenge for many organizations today.

1 Designed with security in mind

Ricoh provides various software and embedded solutions for IT systems, business process management, and multifunction devices and printers. Therefore, firmware and applications that run on Ricoh devices undergo rigorous review and must be compatibility certified and digitally signed by Ricoh in addition to many other security factors.

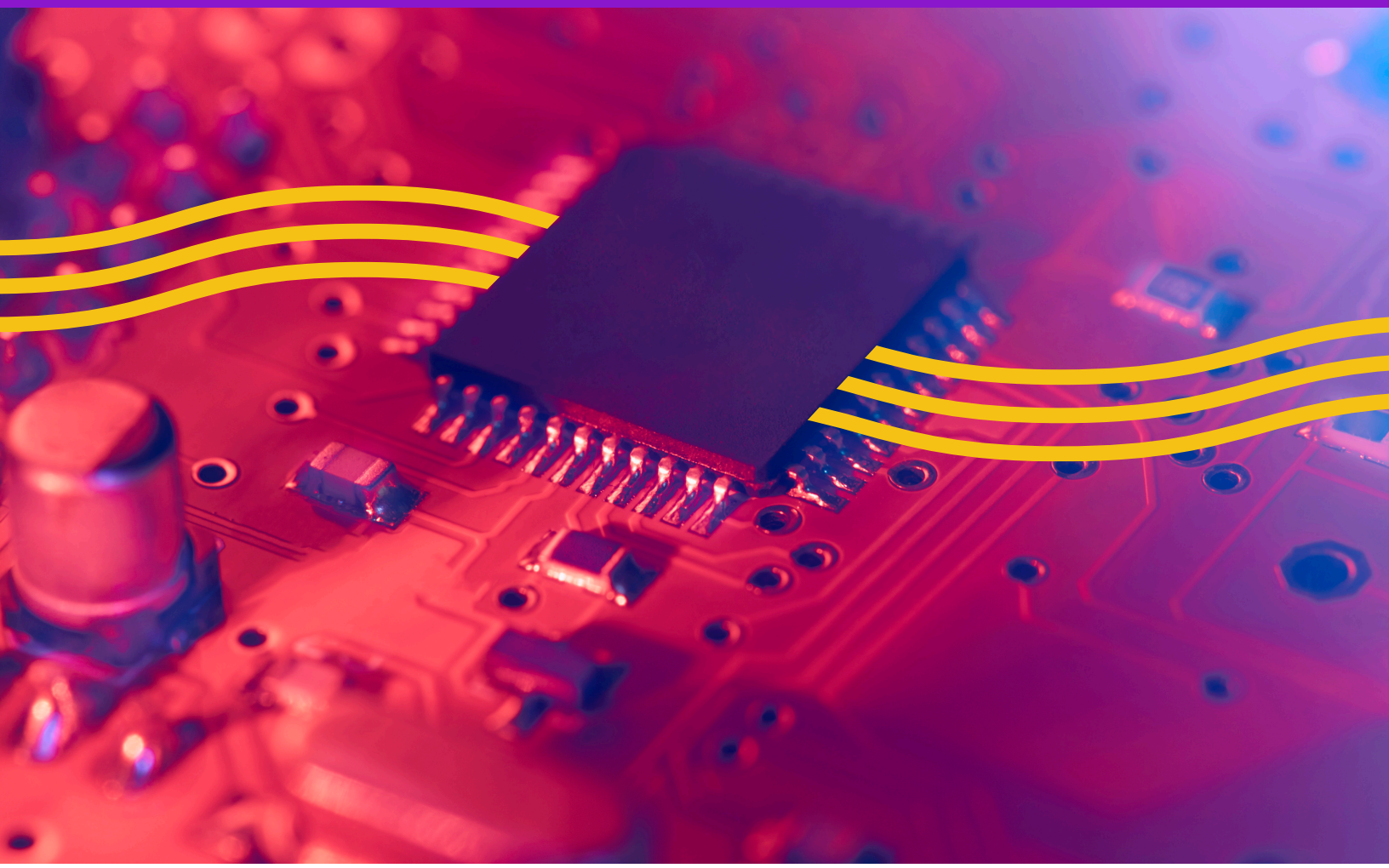
During the use of these products, we provide security functions to ensure customers' sensitive data is protected from various threats. This includes responding to persistent vulnerabilities for both multifunction copiers and printers.

Security-related threats are becoming more advanced and sophisticated each day. Ricoh continues to protect customer information assets and provide products that can be adapted to both the customer's office environment and security policy, ensuring these products can be used with confidence.

2 Application security best practices

To protect against damage resulting from malicious third parties, system administrators should consider the following:

1. Read the entire license agreement for each software and embedded solutions. In order to continue use, you must agree to the terms.
2. Confirm your operating system and/or device firmware is the most recent version before installation and operation. Install and operate software and embedded solutions on a network protected by a firewall. To avoid inherent risks, it's suggested not to connect software and embedded solutions directly to the Internet.
3. Limit access to software and embedded solution products to only authorized users and limit access to the software and embedded solution products by access control and allowing only approved IP address ranges.
4. To prevent unauthorized access by malicious third parties, change the default administrator password for the software and embedded solution products and operating system.
5. Confirm software, software operating system, embedded solutions, and multifunction printer or printer are configured correctly to meet your desired workflow and follow your company's security policy.



6. Multifunction printer and printer security settings should be appropriately set according to the details described in the multifunction copier or printer instruction manual in the “Safety Precautions” section.
7. Use encryption for all data in transit. Furthermore, certificates should be signed by either a company-hosted or public third-party Certificate Authority. Inherent risks exist if using self-signed certificates.
8. Instruction and training should be given to people who use the software and embedded solutions.
9. To limit outside threats, ensure browser security is enabled on computers used to manage software and embedded solutions. Additionally, do not use the same browser or browser session to manage/access software and embedded solutions while accessing outside network resources at the same time. Completely log off any software and embedded solutions before accessing outside network resources.
10. For software and embedded solutions that are discontinued, uninstall the software and remove any personal or sensitive data used in previous workflows. This will prevent leakage of customer-sensitive information that may remain there.

Layer 4 – device security

Security threats are no longer limited to personal computers, servers, or networks. Any device — even basic networked printers — needs countermeasures against a diverse range of threats. As multifunction printers' (MFPs) functionality has evolved, they have become core IT assets. As the computing capability of what was traditionally categorized as "printer/copiers" has grown, so have potential threats, which can include:

- Malicious access via networks
- Tapping into and alteration of information over the network
- Information leaks from storage media
- Unauthorized access via a device's operation panel
- Improper access through fax telephone lines
- Information leaks via hardcopy
- Security policy breaches due to carelessness

Simply hoping you don't get hit is not the answer. Superior technology, diligence, and knowledge are essential, requiring a deep understanding of how to tackle potential issues caused by vulnerabilities in your devices, the data they process, and the networks to which they connect.

Device authentication

Controlling access by authentication according to your security policies is necessary. Healthy, secured devices can offer another critical level of security, including remote insight into device configuration, alerts related to usage and supplies, critical service alerts, and warnings for upcoming service issues.

1 Device user authentication

The ability to track, control usage, and prevent unauthorized access is predicated on requiring users to authenticate before they can print, scan, fax, etc. Once logged in, users will only see the device functions and features they're authorized to use. Various authentication options give you the ability to control the level of capabilities granted to each user or group of users. This may include restricting the ability to change machine settings and view address book entries or granting access to scanning workflows, document servers, and other functions. In addition, the User Lock-out function — which triggers if it detects a high frequency of successful or failed login attempts — helps guard against Denial of Service attacks or brute force password cracks.

2 Network user authentication

Ricoh devices support network user authentication to limit access to authorized users. For example, Windows® authentication verifies a user's identity at the MFP by comparing login credentials (username and password, ID badge with or without PIN, or a combination of both) against the database of authorized users on the Windows network server. In the case of access to the global address book, LDAP authentication validates a user against the LDAP (Light-weight Directory Access Protocol) server — so only those with a valid username and password can search and select email addresses stored on the LDAP server.

For customers utilizing SmartCards for authentication, such as U.S. Government Common Access Cards (CAC) or Personal Identity Verification (PIV) IDs, Ricoh offers solutions for enabling this type of authentication.

Software such as RICOH Streamline NX — a modular suite that covers scan, fax, print, device management, security, and accounting processes — provides additional network authentication options. These include authenticating against the LDAP, Kerberos authentication, and an available SDK for custom integrations.

3 **Device network authentication**

Many Ricoh devices support the IEEE 802.1X authentication protocol, which is frequently part of zero-trust architecture (ZTA) network implementations. This port-based network access control allows a network administrator to restrict the use of a network until a device has been properly authenticated. This ensures secured communication between authenticated and authorized devices.

Device protection

When machines aren't performing as expected, there are not only costs associated with downtime, but it can negatively impact other user behavior, which may include less than desirable workarounds.

Keeping device firmware updated can be accomplished remotely and in batches, and updates can be set to your schedule.

1 **Firmware and driver management**

Working with your service provider, organizations can maintain a line of defense by ensuring current firmware on your devices through proactive remote management. You can prevent printer device firmware from becoming outdated via a remote cloud portal. A device's firmware can be remotely checked, and an update can be immediately pushed. Or, updates can be performed automatically on a scheduled basis.

Refreshing firmware for large numbers of devices or across an entire fleet can be handled as a batch upgrade in moments. Drivers can also be pre-configured and pushed to devices remotely. You can package drivers with the appropriate defaults according to your print and security policies — and control who has access to different driver packages.

2 **Digitally signed firmware**

If an MFP or printer's built-in software — also known as firmware — is altered or compromised, that device can then be used as a method of intrusion into the corporate network to damage the device or platform for other malicious purposes. Ricoh-designed devices are built using a Trusted Platform Module (TPM) and are designed to not boot up if the firmware has been compromised. Ricoh's TPM is a hardware security module that validates the controller core programs, Operating System, BIOS, boot loader, and application firmware.

Ricoh MFPs and printers use a digital signature to judge firmware validity. The public key used for this verification is stored in an overwrite-protected, non-volatile region of the TPM. A root

encryption key and cryptographic functions are also contained within the TPM and cannot be altered from the outside. Ricoh uses a Trusted Boot procedure that employs two methods to verify the validity of programs/firmware:

- Detection of alterations
- Validation of digital signatures

Ricoh devices are designed to boot up only when firmware and applications are verified to be authentic and safe for users.

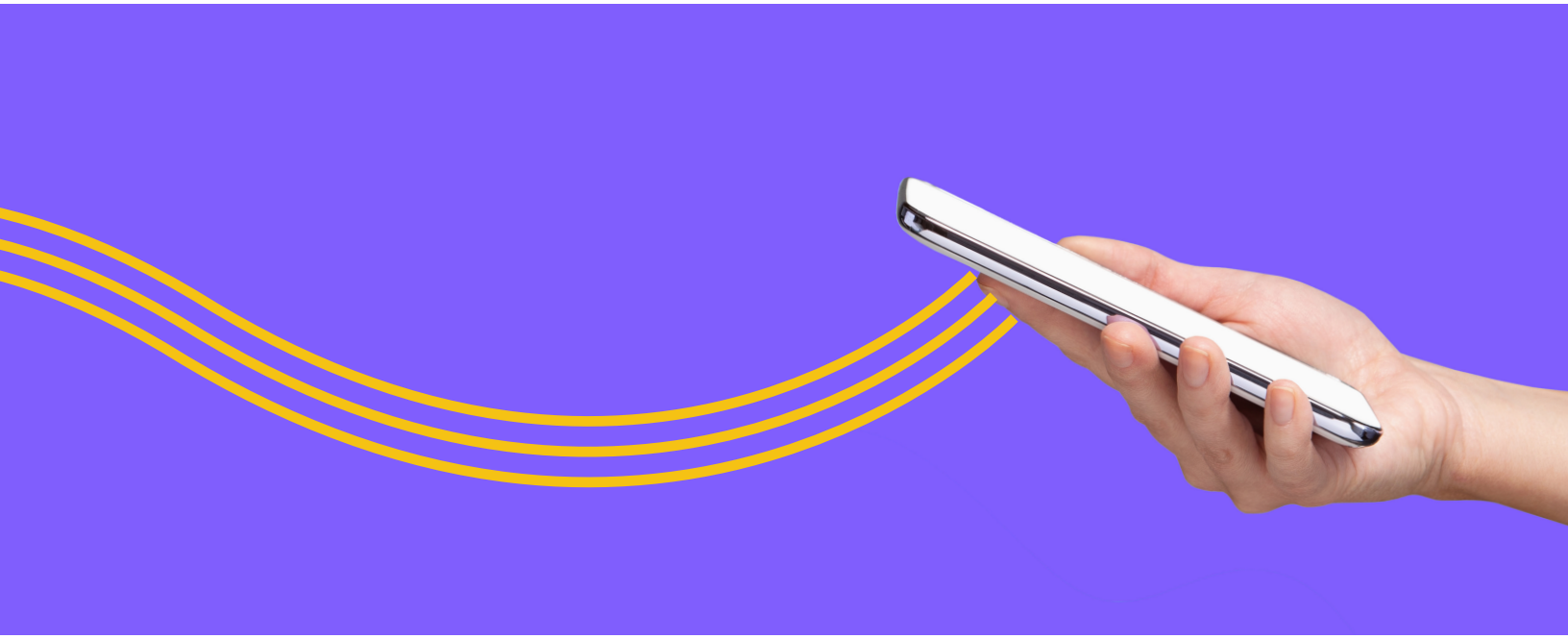
3 Disable unused protocols and services

To make it easy to add network devices, many vendors' network-enabled systems are routinely shipped to the customer with all network protocols and services set to "enabled or active" — but unused services on network devices pose a security risk. Compromised ports can lead to various threats, including the destruction or falsification of stored data, Denial of Service (DoS) attacks and viruses or malware entering the network.

There is a simple but often overlooked solution for this particular risk source: disable all unrequired services. Ricoh device administrators can easily lock down unneeded services, helping to make devices less susceptible to hacking. In addition, specific protocols — such as SNMP or FTP — can be completely disabled to close off the risk of them being exploited.

4 Fax line security

Enabling a device's fax feature may mean connecting it to the outside via a telephone line — which means that blocking potential unauthorized access via the analog fax line is critical. Ricoh embedded software is designed to only process appropriate types of data (i.e., fax data) and send that data directly to the proper functions within the device. Because only fax data can be received from the fax line, the potential for unauthorized access from the fax line to the network or to programs inside the device is eliminated.



The Facsimile Control Unit (FCU) in Ricoh fax-enabled devices supports only G3 FAX protocols. Therefore, even if an initial connection is established with a terminal that does not use these protocols, the MFP will view this as a communication failure and terminate the connection. This prevents access to internal networks via telecommunication lines and ensures that no illegal data can be introduced via these lines.

5 Simplify managing devices

Managing devices can be time-consuming, and security gaps can emerge unintentionally when aspects of proper device management go unattended. Ricoh device management software, such as Streamline NX, gives IT managers a central control point to monitor and manage their fleet of network-connected print devices — whether spread across multiple servers or geographic regions — from a single management console.

Here's how Ricoh does it:

- SNMPv3-encrypted communications between devices and servers
- Central controls allow administrators to control access, monitor security settings, and manage device certificates
- Automated firmware update tasks reduce exposure from outdated firmware
- Deploy customer-approved firmware versions, or use the latest firmware available from Ricoh
- The Security Analyst add-on for Streamline NX provides an at-a-glance dashboard for assessing device security policy compliance and offers a best practices checklist for whether devices are in policy

6 Meters and alerts

When an early warning enables teams to resolve a problem before it causes downtime, it helps reduce the risk of unexpected user behavior, such as unsanctioned workarounds. If machines are not operating as expected, users may choose a different, unsecured course of action. They may print or scan from a local device with no ability to audit activity or protect the data being moved.

Using monitoring and management software with devices lets you collect information and keep your device healthy with timely alerts. This includes automatic collection of meter data based on your set schedule, low/replace toner alerts, critical service alerts, and upcoming critical service issues.

7 @Remote.NET

Ricoh's @Remote Connector NX enhancement for Streamline NX collects approaching critical service alerts and communicates them directly to your service provider. Your provider can schedule remote firmware updates and push critical updates immediately. The @Remote Connector also collects device meters and makes them available on a pre-defined schedule — along with notifications of consumables levels — to maintain uptime and reduce administrative burden. The collected data is available via the @Remote.NET web portal.

Types of encryption

1 Drive encryption

If the drive is physically removed from a Ricoh machine, the encrypted data cannot be read. Once enabled, the drive encryption function can help protect an MFP's drive against data theft while helping organizations comply with corporate security policies. Encryption includes data stored in a system's address book — reducing the danger of an organization's employees, customers, or vendors having their information misappropriated.

The following types of data — which are stored in non-volatile memory or on the drive of MFPs — can be encrypted:

- Address book
- User authentication data
- Stored documents
- Temporarily stored documents
- Logs
- Network interface settings
- Configuration info

2 Device data in transit encryption

As information moves through the network, it is possible for a knowledgeable hacker to intercept raw data streams, files, and passwords. Without protection, unencrypted information can be stolen, modified, or falsified and re-inserted back into the network with malicious intent. To combat this, Ricoh uses encryption and robust network security protocols that can also be configured according to customers' needs. For example, the Transport Layer Security (TLS) protocol is used to help maintain the confidentiality and integrity of data being communicated between two endpoints.

3 Print stream encryption

Data sent in a print stream can be exploited if unencrypted and captured in transit. Ricoh enables the encryption of print data by means of Secure Sockets Layer/Transport Layer Security (SSL/TLS) via Internet Printing Protocol (IPP) — encrypting data from workstations to network devices or MFPs. Because this is a protocol that helps maintain data confidentiality, attempts to intercept encrypted print data streams in transit would only produce data that is indecipherable. Data sent to printers could be misused or attacked if it is not encrypted.

4 End-to-end driver-based encryption

Concerns about a malicious attack on print job data can be addressed using the Ricoh Universal Print Driver for end-to-end encryption of print data between the user's system and the Ricoh MFP. End-to-end encryption can be enabled in the print dialog so a user can set an encryption password. To release the print job, the user enters the encryption password at the Ricoh device, which then decrypts the data and prints the job. This method of print data encryption utilizes AES-256 encryption.

5 Locked print

Printed documents sitting on the paper tray or left out in the open can be picked up by anyone. This puts the document's information at risk, and the potential impact grows dramatically when printing confidential documents. Ricoh locked print capabilities can hold encrypted documents on the device's hard drive until the document's owner arrives and enters the correct PIN code or network credentials. For even more capability, software such SLNX can provide full-featured secure document release — giving users options over their secure print queue while letting administrators maintain control.

6 Copy data security

Ricoh offers functions to thwart unauthorized copying of hardcopy documents — helping prevent possible information leaks. The copy guard function prints and copies documents with special invisible patterns embedded across the background. If the printed or copied document is photocopied again, the embedded patterns will become visible on the copies.

The unauthorized copy control function protects against unauthorized copying in two ways. Masked Type for Copying embeds a masking pattern and message within the original printout, safeguarding the information. If unauthorized copies are made, the embedded message appears on the copy. This might include the document author's name or a warning message. When the Ricoh device detects the masking pattern, the printed data is obscured by a gray box that covers all but a 4mm margin of the masking pattern.

7 Mandatory secure information print

Stamping documents with key identifying information can achieve greater accountability and management control. Mandatory security information print is a feature that forces key information — including who printed a document, when it was printed, and from which device — to be printed with a document. This feature can be enabled for copy, print, fax, and document server functions.

Administrators can select the print position and which types of information will be automatically printed on the output, which may include:

- Date and time the job was printed
- Name or login user ID of who printed the job
- IP address and/or serial number of the device used

8 Temporary data removal

When a document is scanned or when data is received from a PC, some may be stored temporarily on the hard disk drive or memory device. This can include scan/print/copy image data, user-entered data, and device configuration. This temporary data represents a potential security vulnerability.

The DataOverwriteSecurity System, built into most Ricoh devices, addresses this vulnerability, destroying temporary data stored on the MFP's hard disk drive by overwriting it with random sequences of 1 and 0. Temporary data is actively overwritten and thereby erased each time a job is successfully completed. The DataOverwriteSecurity System can also:

- Include options for National Security Agency (NSA) and Department of Defense (DoD) recommendations for handling classified information
- Make it virtually impossible to access latent data from copy/print/scan jobs once the overwrite process is complete (overwrite process can be selected from 1 to 9 times)
- Assist customers in their compliance with HIPAA, GLBA, FERPA, and other regulations
- Provide visual feedback regarding the overwrite process (i.e. Completed or In-Process) with a simple display panel icon

Independent security standards and certifications

Common Criteria is used internationally for the evaluation of information technology security. It is used for measuring whether security functions are appropriately developed for IT products. The Common Criteria Certification is a standard recognized by more than 25 nations of the world. Domestic and overseas multifunction copier vendors are eager to obtain authentication for digital multifunction copiers.

The Common Criteria Certification process verifies protection provided by multiple security technologies against various security threats. The certification covers, for example, system validity verification at the start, access control and logging, data protection by encryption and data deletion at machine disposal. Therefore, it helps protect our products from various threats — such as software alteration, invalid access, and information leakage.

1 **Protection Profile for Hardcopy Devices (PP_HCD_V10)**

PP_HCD_V10 is a U.S. government approved protection profile for hardcopy devices such as digital MFPs. It was developed by the Multifunction Printers Technical Community with representatives from industry (including Ricoh), U.S. and Japanese government agencies, Common Criteria Test Laboratories, and international Common Criteria schemes. The purpose of this Protection Profile (PP) is to facilitate efficient procurement of Commercial Off-The-Shelf (COTS) Hardcopy Devices (HCDs) using the Common Criteria (CC) methodology for information technology security evaluation.

50+ | **Products with Common Criteria (ISO/IEC 15408)**

The following areas — which have been identified as among the most important for security protections — have been validated in most Ricoh devices to the PP_HCD_V10 standard and can be enabled:

- User identification and authentication systems
- Data encryption technology available for multifunction printers
- Validation of the system's firmware
- Separation of the analog fax line and the copy/print/scan controller
- Validation of data encryption algorithms
- Data protection

At Ricoh, our product line is constantly being enhanced to meet our customers' and regulators' changing requirements.

2 IEEE 2600.2

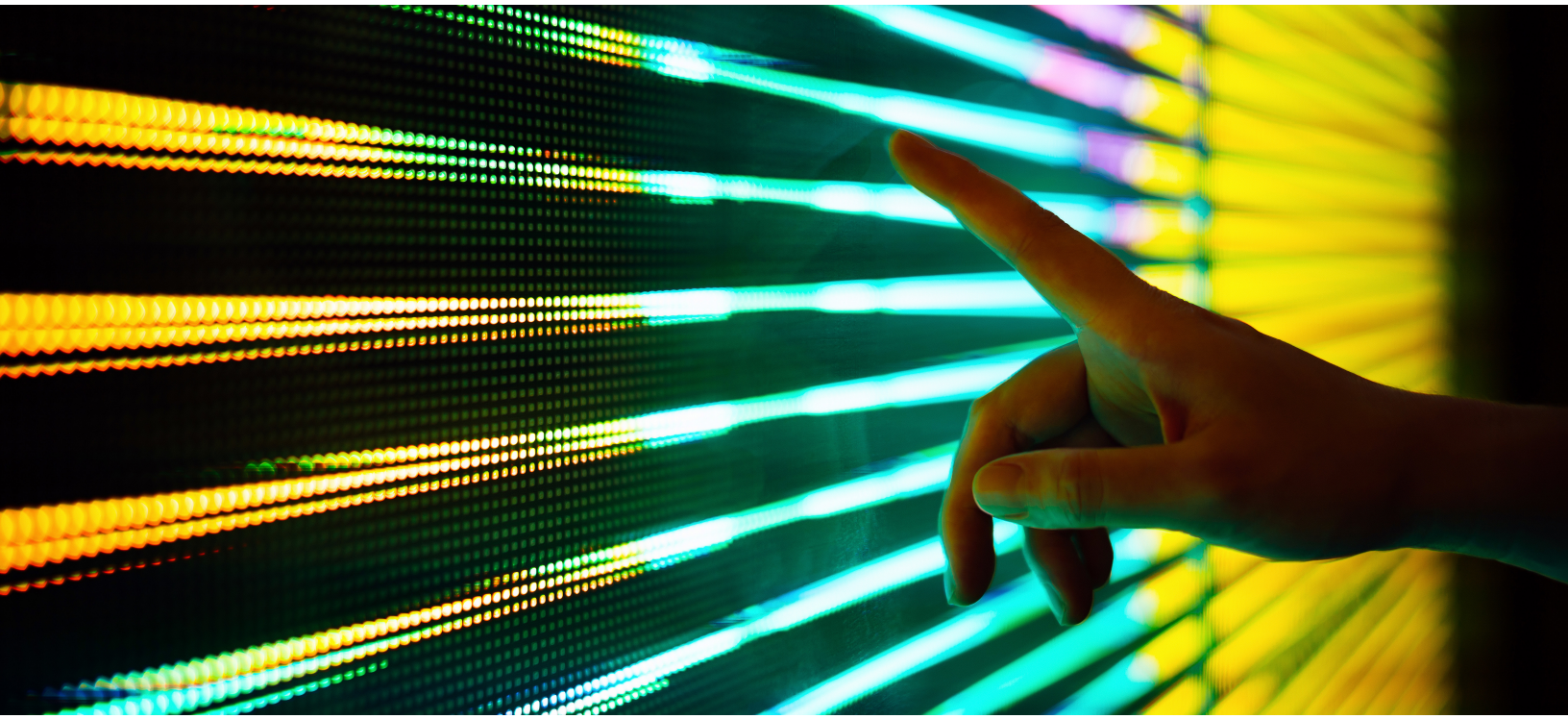
The IEEE 2600.2 security standard pertains to hardcopy devices operating in a commercial information processing environment — with required levels of document security, network security and security assurance. It establishes a common baseline of security expectations for MFPs. To ensure that a device demonstrates conformance with the established standard, independent third-party laboratory tests provide verification of the manufacturer's security features. Ricoh offers a broad line of MFPs that have been certified as conforming to the IEEE 2600.2 security standard.

200 Listed in Top 200 Federal government contractors

3 FIPS 140-2/3

The Federal Information Processing Standard (FIPS) 140-2/3 is a U.S. government security standard for validating cryptographic modules through the National Institute of Standards and Technology's (NIST) Cryptographic Module Validation Program (CMVP). Many cryptographic modules in Ricoh devices use algorithms that are recommended or approved by NIST, including algorithms validated under NIST's Cryptographic Algorithm Validation Program (CAVP). CAVP validation is a prerequisite for CMVP validation.

Customers can upgrade certain devices to a CMVP validated drive* and a soon-to-be-released MFP firmware upgrade that will incorporate CMVP validated modules elsewhere within the MFP**. Firmware upgraded devices will implement certain device hardening measures — including turning off less secured ports, protocols, and limiting some application use.



* The FIPS 140-2 CMVP validated hard drive is available now in limited supply for many of our products.
** Firmware upgrade available as a planned future release. May not be suitable for all devices.

Layer 5 – data security

Data is your organization's most valuable currency, and with the quantity and diversity of data threats we all face, business leaders must prioritize data protection and mandate governance to support those efforts.

Threats come from a variety of external and internal sources, including cyber attacks, ransomware attacks, insider threats, technology failure, natural disasters, phishing, and human error. A resilient organization requires protective strategies that serve to prevent data breaches as well as strategies to mitigate damage in the event an attack occurs.

1 **Encryption**

As mentioned in previous sections of this document, data encryption should be applied to documents, files, messages, or any other form of communication over a network. Ricoh ensures all its devices, software, and storage solutions deliver end-to-end encryption.

While data security should be a top priority for all staff, you cannot rely on them to know when or how data should be encrypted. When developing your organization's encryption policy, you'll first want to get an accurate picture of where all your data resides, how much of it is confidential or valuable (a potential target for malicious actors), and the risks it presents to your organization. Cleaning up unstructured data and conducting a data protection impact assessment will enable you to develop a comprehensive data security strategy.

2 **Cloud hosting**

Bringing your distributed data and infrastructure into one cloud environment allows for holistic, end-to-end monitoring and management, closing security gaps and enabling more rigorous, centralized management. Public, private, and hybrid cloud models allow for varying levels of security suited to the needs of your organization.

Microsoft 365 and Azure are the industry's top public cloud platforms because of Microsoft's many layers of security features, add-ons, and integrations, ranging from unified data governance to secured file sharing to user authentication and identity management.

3 **Ransomware security**

There are two critical layers to ransomware security — prevention and mitigation. Preventative solutions detect ransomware signatures and behaviors, stopping them from getting past the perimeter, whereas ransomware containment stops outbreaks of malicious encryption if it breaks through safeguards. The software focuses on the outcome of ransomware, rapid illegitimate encryption. It stops encryption at the source or root file, isolating and containing it to prevent further spread.

Ransomware containment is a critical last line of defense to an organization's security infrastructure, filling the perilous gap between devices and file shares where organizations often lack the essential defenses.

4 Secured data backups and recovery

An essential element of data security is planning for the unexpected; whether it is a cyber attack or a system malfunction, to maintain operations you need to know your data can be reliably and quickly restored.

The most secured and failsafe backup solutions involve a combination of advanced cloud technologies and expert management, which is why many organizations outsource to a trusted services provider. From implementation to configuration, regular testing, and recovery, you can rest assured your data is protected and accessible in any scenario.

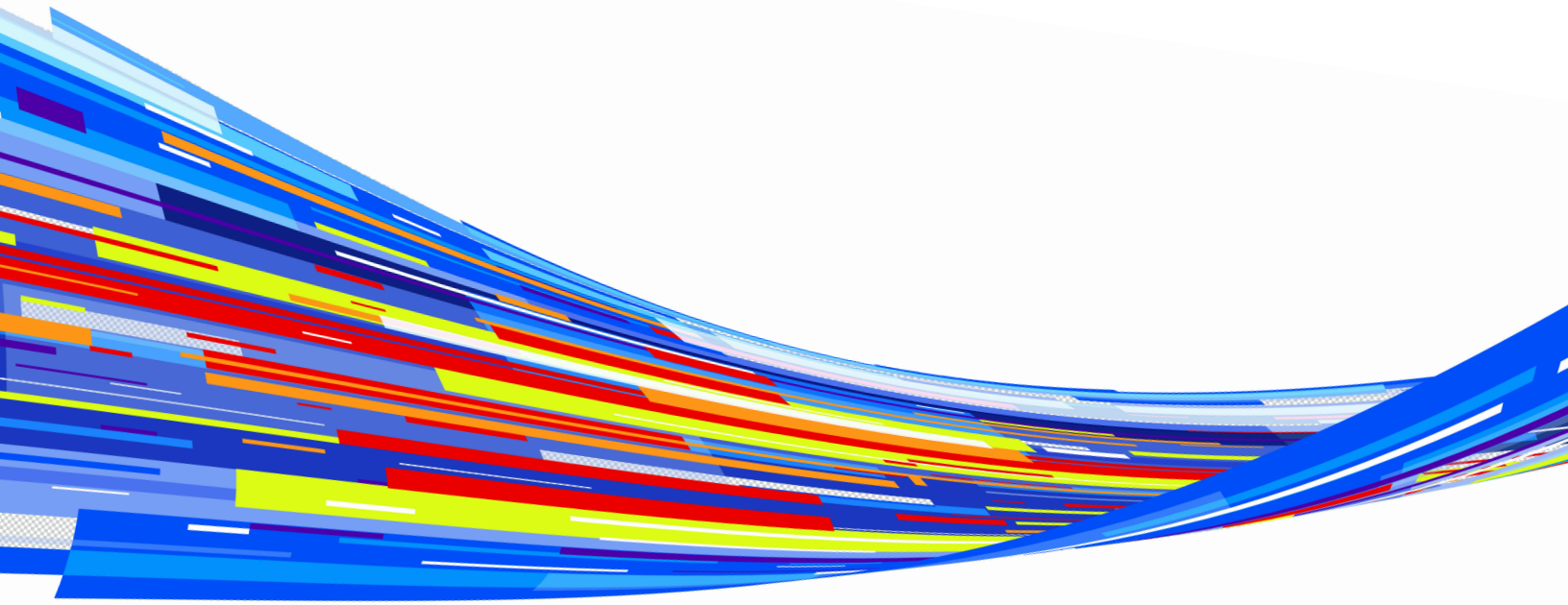
5 Compliance assessments

Organizations subject to PCI DSS, PII, HIPAA, FINRA, FERPA, GDPR, CCPA, or FFIEC mandates — or needing to meet compliance requirements that adhere to the HITRUST framework or meet other corporate security policies — should consider compliance-centric professional IT services.

These focused services assist customers in achieving compliance with a variety of federal, state, and industry regulations including Federal Rules of Civil Procedure (FRCP), Open Meeting Laws, Freedom of Information Act "Sunshine Laws", SEC 17A-4 and NASD 3010, SEC Investment Advisers Act of 1940, Sarbanes-Oxley Act of 2002 (SOX), HIPAA (Health Insurance Portability & Accountability Act), and GLBA (Gramm-Leach Bliley Act).

Compliance-centric measures include:

- Automated data capture, tagging, and archiving of all emails and attachments
- Original email format preservation
- Rapid random sampling of requested data to regulatory bodies
- Automated user offboarding
- Mobile device management
- Enforced separation of duties
- Isolating systems for sensitive information
- Linked access rights and audit to user identities



Strategic guidance and support

Security consultations

Shift your IT strategy from one that merely supports day-to-day business to one that plays an integral part in building and supporting secure and strategic business initiatives.

Ricoh's virtual technology consultants and security specialists can help you build a comprehensive security strategy that's assessed, tested, and retested before disaster strikes. Our approach, based on governance, risk, and compliance best practices, quickly identifies vulnerabilities for security breaches, gaps that can result in cyberattacks, and other internal technology exposures before they impact your business.

Information governance consulting

Many organizations struggle with several aspects of information management, such as security and protection, retention and disposition, legal and regulatory compliance, reliability, and authenticity. Ricoh's Information Governance (IG) consultants address these aspects, helping organizations break down silos and establish long-term, sustainable programs. We look at information as both the problem and the solution and take a proactive approach to your information challenges, setting your organization up for success to make sound business decisions.

Nationwide and global technical support

Ricoh has established Technology Centers in every region to provide technical support to our customers around the globe, responding to their needs quickly and efficiently. The Ricoh Global Services team provides standardized, consistent, end-to-end solutions. With coverage in about 200 countries and territories worldwide, Ricoh employs over 9,000 service delivery and technician professionals. Our unrivaled direct sales and dealer partner support network has the capability to do business with 60% of Fortune 1000 companies — which means that you can rely on one partner for all your global needs. By having offices and service delivery professionals in so many countries worldwide, we can respond quickly to customer requests.

60%

Fortune 1000 companies do business with us

Security support documentation

Ricoh provides technical documentation to support our customers' information security requirements — including Common Criteria Validation Reports and Certificates for select product offerings. This documentation provides independent third-party validation of security claims and can be provided upon request. In addition, security white papers covering device and network settings and the Device Security Administrators Guide required by Common Criteria are also available to customers. These guides provide detailed information about how Ricoh equipment communicates data inside of the device and how the device interacts with the network. Click here to see more documentation.

End user and administrator training

Maintaining a high degree of vigilance and adhering to security best practices involves more than just technology — it involves people. Ricoh offers training on our devices — and third-party partner vendors — aimed at both end users and administrators. With the right knowledge at their fingertips, your team can understand available security capabilities and learn how their appropriate use can help your organization protect its information and comply with regulations.

Ricoh's security commitment

Security is ingrained in our values — a commitment we do not take lightly. Whether you're stuck in a data deluge, work in a highly regulated industry, lack resources or experience, or want the assurance of utilizing highly secured services, software, and devices, we aim to gain your trust by having the highest security standards in the industry. Our goal is to stay ahead of cyber criminals — and if they do encroach into our systems, we have a plan and systems in place to mitigate a breach.

Our pledge to every customer is to adhere to current security standards and guidelines in our products and services, work diligently to protect our customers' data, and enable them to protect themselves. We commit to always evaluate, learn, and innovate with every initiative, looking towards the best future for our customers and partners.

Information security threats are becoming more advanced and stealthier every day. Ricoh is committed to offering secured products that protect your information assets and harmonize with your office environment and security policies. Ensuring security requires correct settings and implementation in your specific environment.

Our depth of experience and multi-layered approach can be leveraged across your organization from strategy, devices, software, services, support, training, and more. Let us help you in your digital information services journey.

RICOH
imagine. change.

Ricoh, a trusted partner

At Ricoh, we're empowering our customers to respond to our changing world with actionable insights. We believe having access to the right information translates to better business agility, more human experiences, and the ability to thrive in today's age of hybrid and borderless work. Through our people, experience, and solutions, we create a competitive advantage every day for over 1.4 million businesses around the globe. To us, there's no such thing as too much information.

Have questions? Visit ricoh-usa.com or contact a Ricoh security expert today.

Ricoh USA, Inc. 300 Eagleview Boulevard, Exton, PA 19341 | 1-800-63-RICOH

RICOH
imagine. change.