KONICA MINOLTA

SECURITY
WITHOUT SACRIFICE

Konica Minolta security standards

INFORMATION
SECURITY

Giving Shape to Ideas

INDUSTRY-LEADING STANDARD SECURITY

In the digital age, we have seen global communications undergo unparalleled growth – and the potential of damaging security breaches has soared in parallel. In any enterprise environment, the day-to-day use of copying, print, scan and fax systems, as the elementary components of work processes and workflows, makes MFPs indispensable at many levels. As a consequence, it is paramount that these devices are given the protection needed to withstand the ongoing threats to security.

Konica Minolta's comprehensive range of standard security features and options form a powerful source on which professional solutions can be based: solutions to both detect and prevent security violations, and avoid knock-on financial and/or reputational damage at the corporate as well as the private individual level. Konica Minolta has pioneered this field and remains the industry's leader.

Konica Minolta devices are certified almost without exception in accordance with the Common Criteria/ ISO 15408/ IEEE 2600.1 Certification. These are the only internationally recognised standards for IT security testing for digital office products. Printers, copiers and software compliant with Common Criteria certification have all passed a strict security evaluation and are able to satisfy and deliver the kind of security levels that a prudent business operation should seek and rightfully expect.

"Security is the key element of Konica Minolta's overall strategy …

Konica Minolta has a comprehensive range of print and document security features, many of which are standard features for their bizhub range of devices. Rather than certifying optional security kits, Konica Minolta claims to have the widest range of ISO 15408 fully certified MFPs in the market."

Source: Quocirca (2011), market study "Closing the print security gap. The market landscape for print security", p. 11. This independent report was written by Quocirca Ltd., a primary research and analysis company specialising in the business impact of information technology and communications (ITC).

Common Criteria Validated

CAUSE FOR CONCERN EVERYWHERE – **SECURITY VULNERABILITY**

Generally MFPs offer a huge range of combined and single functions and choices; therefore they represent a similarly wide range of potential security loopholes. The scope of MFP security could be grouped into three main sections:

Access control/Access security

Despite the topic of security being high on the agenda in both public and corporate domains, MFPs are often ignored as being any kind of security risk. While some risks are perhaps identified, they are often simply neglected, especially where sensitive documents and information are concerned. This is especially risky for those MFPs and printers located in public areas, where they can be accessed by staff, contractors and even visitors.

Because the advanced features available on today's MFPs deliberately make it easy for information to be copied and distributed within and beyond actual and virtual corporate boundaries, the first logical step is to prevent unauthorised persons being able to operate an MFP. Preventive measures are needed to firstly control access to MFPs, and secondly to establish some kind of security policy reflecting how the devices are actually used in real life. Obviously none of these measures should restrict or limit the user-friendliness of the systems. Konica Minolta is prepared for this, offering various security features and solutions.

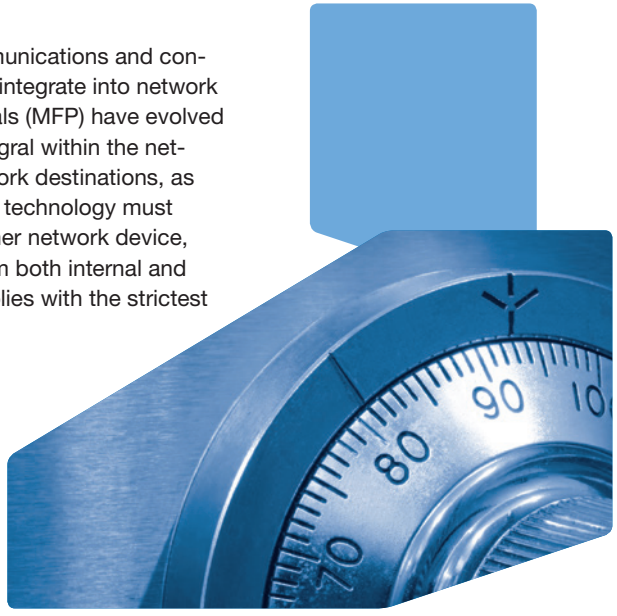
Document security/Data security

Reflecting the fact that MFPs and printers are often located in public areas, where they can be easily accessed by staff, contractors and visitors, it is necessary to implement appropriate data security policies. After all, the situation is that confidential data, for example stored on the MFP hard disk over a period of time or simply confidential documents lying in the MFP output tray as printouts, is initially unprotected and could fall into the wrong hands. Konica Minolta offers a range of tailored security measures to ensure document and data security.

Network security

In today's corporate environment, indeed in today's business world, communications and connectivity are indispensable. Konica Minolta office devices are designed to integrate into network environments. For example, network printers and multifunctional peripherals (MFP) have evolved to the point that they act as sophisticated document processing hubs integral within the network, with the ability to print, copy and scan documents and data to network destinations, as well as send emails, for example. This scenario also means that this office technology must cope with and comply with the same security risks and policies as any other network device, and represents a risk if unprotected. In order to avoid any vulnerability from both internal and external network attacks, Konica Minolta ensures that all equipment complies with the strictest security standards. This is achieved by a number of measures.

With its comprehensive range of security features, Konica Minolta provides professional solutions for the detection and prevention of security breaks.



ALL-ROUND SECURITY – STANDARD WITH KONICA MINOLTA

The authentication path starts by setting down a policy defining and configuring users and groups of users allowed to work with an MFP device. This can include limitations to access rights; basically that some users are authorised to use various functions, such as colour printing, while others are not. The Konica Minolta approach is to provide a broad range of choice when implementing access control.

All of the access control and security functions of Konica Minolta not only offer greater security against threats which can result in financial and reputational damage, they can also be used as the basis for better governance and enhanced accountability.

Access control/Access security

- **User authentication** regulates access to copiers or printers via authentication either at the workstation or at the output device itself. On most bizhub systems, Konica Minolta offers various choices of access control.

- **Biometric finger vein authentication** employs cutting-edge technology by working with images of finger vein patterns that are captured by scanning the finger. Using an individual human feature for identification, this biometric measurement is virtually impossible to falsify. This authentication method is a lot more secure than fingerprint systems. And it's fast and simple, since there's no need to remember passwords or carry a card.

- **Authentication by non-contact ID card** is also available for most bizhub MFPs. This method is also designed for convenience and speed – it is simply a matter of placing the ID card on or near the reader interface.

- The simplest form of user authentication is to restrict access by **personal password or user code** which has to be entered at the MFP panel. This internal authentication at the machine supports up to 1,000 user accounts. Passwords are alphanumeric with up to 64 characters, can be created for administrators and users, and are maintained by an administrator.

- **Authentication information** can be stored in encrypted form on the MFPs, or existing access information can be used, e.g. from the Windows Active Directory. In addition, the authentication can be centrally managed via the PageScope Enterprise Suite Authentication Manager.

- All bizhub MFPs can be programmed to **automatically reset to require password input after a specified period of inactivity**. This ensures that the MFP will reset to a secure state if a user forgets to log off when finished. Password protection can also be used to limit access to documents on MFPs from remote workstations. Many Konica Minolta devices offer the ability to remotely access print and scan jobs. This feature can be either password-protected or disabled altogether.

- Like a cash terminal, each bizhub MFP can be programmed to **reject a user who attempts to authenticate with a wrong password**. After a specified number of wrong attempts, the machine will block access for a chosen time period. This unauthorised access lock function can also be applied to the system user box for confidential documents (secure print box).

- An advanced level of user security governs the availability of **specific MFP features, allowing or prohibiting their use**. A key operator or administrator can control these features as needed throughout an organisation of any size. The specific features are:
  - Copying from the bizhub as a walk-up function, including the restrictions of only b/w copying or only colour copying
  - Printing as a remote function via the printer driver, including the restrictions of only b/w printing or only colour printing
  - Scanning from the bizhub as a walk-up or a remote function
  - Faxing from the bizhub as a walk-up or a remote function
  - User box from the bizhub as a walk-up or a remote function
  - In addition, it is possible for various MFP functions to be limited on an individual user basis. This could be directly linked with the authentication methods mentioned above.

- **Log information** for access and usage of individual devices not only enables immediate detection of security breaches, it also facilitates accounting and cost allocation to users and departments. The administrator can individually review audits and job logs for different machine functions, including b/w and colour printing and/or copying, incoming and outgoing faxes, and scanning.
  Many print controllers on Konica Minolta systems contain electronic job logs that record all print jobs sent to the output device. In addition, Konica Minolta's PageScope Job Log Utility provides comprehensive electronic tracking logs of user activity.

- **Account tracking** requires a user login at the output device and provides efficient monitoring at user level, group level and/or departmental level. Monochrome and colour copies, scans, faxes, b/w and colour printing can all be tracked locally at the machine or remotely via Konica Minolta software such as PageScope Web Connection, PageScope Net Care Device Manager and Page Scope Enterprise Suite Account Manager.
  When logged in, the user's activities are electronically recorded onto a log file inside the system, which can be accessed by the administrator or key operator. This feature provides efficient support, e.g. for invoicing departments or to audit employees' copier activities.

CONFIDENTIAL DATA AND INFORMATION – **SECURE WITH KONICA MINOLTA**

Designed to protect confidential information content as well as private user and corporate network data, Konica Minolta's comprehensive security functionality secures user details and output content, helping to prevent sensitive corporate information from falling into the wrong hands.

Document security/Data security

– Output devices are considered a security risk, a risk which should not be underestimated: at the simplest level, documents lying in the output tray can be seen and read even by passers-by. There is no simpler way for unauthorised persons to gain access to confidential information.
The **secure print** functionality keeps documents confidential by requiring the author of the print job to set a password as a security lock prior to printing. Protected documents cannot be printed until the password set in the driver is entered directly at the output device. This guarantees that such documents are available only to those intended to read them. Each password connected to a confidential print job is encrypted. As further protection, the bizhub systems can be configured to delete all unopened secure print jobs after a designated time period.

– Secure printing is also available via the convenient **Touch & Print** or **ID & Print** functionality. Touch & Print is based on authentication via finger vein scanner or ID card reader, while ID & Print requires the user's authentication via ID and password. With these features, no additional secure print ID and password are required; instead the user authentication data is used to identify a stored secure print job and release the job immediately after authentication at the device.

– Alternatively, print jobs can be protected by secure printing to the user box. The **user box** functionality on bizhub systems enables users to store their documents in personal boxes that are only visible after authentication and only accessible with an additional individual user password. To access such print jobs for outputting or forwarding via fax or email, the user will have to enter both the correct user ID and the password. At the same time the protected user boxes also enable confidential fax receipt.

- The content of PDFs can be encrypted by standard 40- or 128-bit encryption. **Encrypted PDFs** are protected by a user password that can have up to 32 characters. As part of the encryption, it is possible to specify permissions to print or copy the PDF or even edit its contents.

- PDF data that is attached to an email or sent to an FTP or SMB folder can by encrypted by **Digital ID**. Such PDF encryption makes the interception of PDF information impossible. Digital ID encryption is based on the S/MIME encryption and requires a public key for encryption plus a private key for decryption.

- To prevent tampering with PDFs created on a bizhub MFP, a digital signature can be added to the PDF. This monitors any changes made to the PDF after writing it. The **digital signature** clearly indicates all changes in the PDF security information. In addition to preventing documents from being tampered with, the digital signature provides details on the document source, helping to recognise if this is unsafe.

- With **copy protection**, which is available on certain bizhub models, a concealed security watermark is placed on the original document during printing. The security watermark can consist of several phrases and/or patterns. When a protected document such as this is copied on any other MFP, the security watermark will appear, indicating to the recipient that this document has been copied and/or distributed without authorisation.

- The optional **Copy Guard/Password Copy** feature adds a concealed security watermark to the original during printing to prevent the copying of documents. While barely visible on the protected original document, it is not possible to copy this document again. The device is blocked for this operation. The password copy feature can override the copy guard and allows copies to be made when the correct password is entered at the MFP panel.

- Most printers and MFPs have access to **hard disks and memory** which can retain many gigabytes of confidential data, over long periods. Dependable safeguards must therefore be in place to ensure the safekeeping of sensitive corporate information. At Konica Minolta a number of overlapping and intermeshing features provide this assurance.
  Konica Minolta offers **HDD encryption** for most of the MFPs. This is of interest to companies that are concerned about the security of documents stored as electronic data in password-protected boxes on the system's hard drive. The stored data can be encrypted using the Advanced Encryption Standard (AES) supporting 128-bit key size. Once an HDD is encrypted, its data cannot be read even if the HDD is removed from the MFP.
  For additional protection of the data on the HDD, this can be secured by a TPM (Trusted Platform Module) chip that stores an encryption key to protect the hard disk data encryption. This hardware chip allows for confidential information storage, such as certificates and MFP passwords.

- An **auto-delete function** erases data stored on the internal hard disk after a set time. This format/erase hard drive feature protects the sensitive electronic information stored on the hard disk drives of Konica Minolta MFPs. The stored data can be deleted by the users who first stored the documents.

- For added safety, a key operator, administrator or technician can physically format (erase) the HDD, for example if the MFP needs to be relocated. The **hard drives can be overwritten** (sanitised) using a number of different methods conforming to various (e.g. military) specifications. In addition, administrators can program the bizhub to automatically erase any temporary data remaining on the HDD on a per job basis. If the automatic overwrite is set to 'on', then jobs manually deleted from a user box will be overwritten three times as well.

- **Password protection of the internal HDD** prevents its unauthorised removal; this password is linked with the device so that data is not accessible if the hard disk is removed.

NETWORK COMMUNICATION – SAFE WITH KONICA MINOLTA

Konica Minolta's office devices are based on a concept of communication and connectivity. This complies with strict security standards concerning user access, encryption of data and protocols used for information transmission.

Network security

– Besides governing access to output devices, **user authentication** also prevents unauthorised users from accessing the network. With this feature, which can be configured to authenticate to the network or locally at the machine, every authorised user has a unique user ID and password.

– **SSL and TLS encryption** protects communication to and from output devices, covering online administration tools, the PageScope Enterprise Server and Active Directory transmissions, for example.

– bizhub devices also support **IPsec** for the complete encryption of any network data transmitted to and from the MFP. The IP security protocol encrypts the whole network communication between the local intranet (server, client PC) and the device itself.

– An internal basic firewall provides **IP address filtering** and control of protocol and port access. IP address filtering can be set at the machine: the network interface card of the MFP can be programmed to only grant access to the device to specific IP address ranges from client PCs.

– **Open ports and protocols can be opened, closed, enabled and disabled** via the administration mode at the machine or remotely via PageScope Web Connection or PageScope Net Care Device Manager. As protection against unauthorised tampering with machine and network settings, the administrator mode itself is accessed by an 8-digit alphanumeric password, which can only be changed by the service engineer or from within the administrator area.

– Where required, a web interface closing functionality allows the **disabling of the web interface**, i.e. PageScope Web Connection, for all users. This limits web access to administrators, providing reliable protection against unauthorised persons tampering with settings, configurations, etc.

- **SMTP Authentication** (Simple Mail Transfer Protocol) provides advanced email security. When activated, SMTP will authorise a machine to send email. For those customers who do not host their email services, the use of an ISP mail server is possible and is supported by the machine. SMTP authentication is required by AOL and for the prevention of spam. For secure communication it is also possible to combine POP before SMTP, APOP, SMTP authentication or encryption using SSL/TLS.

- To secure email communication from the MFP to certain recipients, the MFP supports **S/MIME** (Secure/Multipurpose Internet Mail Extensions). S/MIME encrypts the email message and content with a security certificate. S/MIME certificates or encryption keys (public key) can be registered for email addresses stored in the MFP address book. S/MIME encrypted emails can only be opened by the owner of the decryption key (private key).

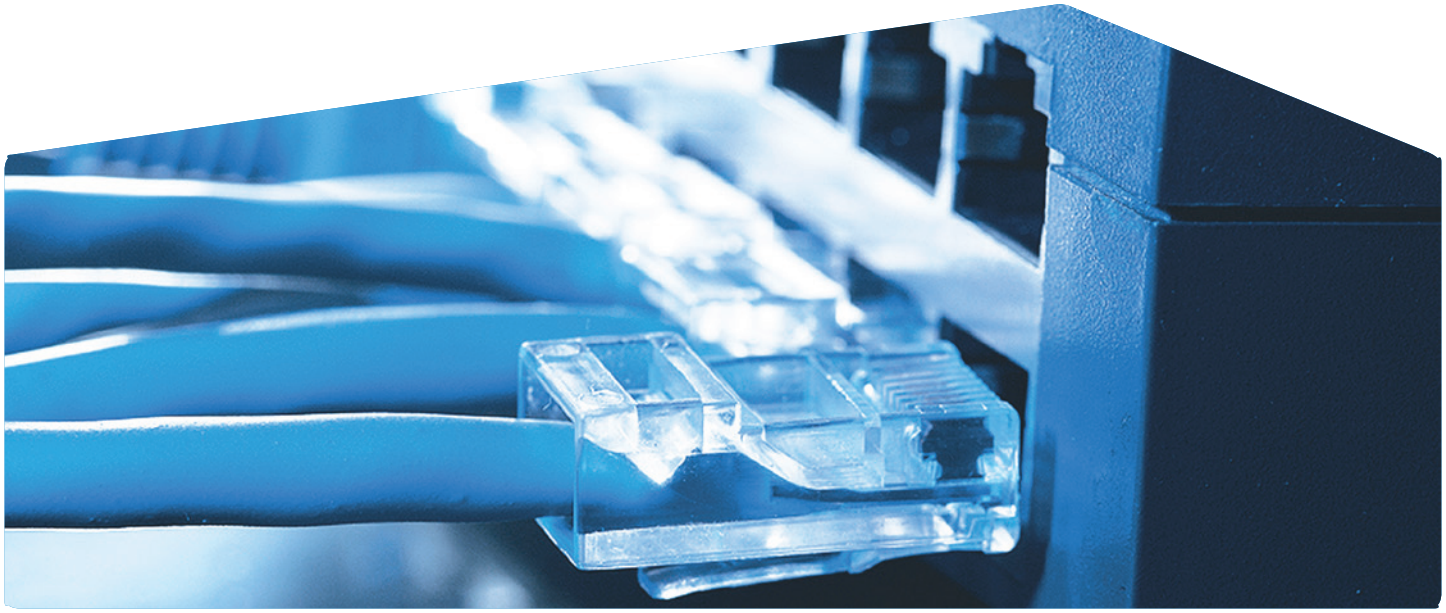
- **When user authentication is activated, it is not possible to change the 'From' address.** Despite the 'Changing From Address' function being enabled, the 'From' address of a scan-to-email job will always be the logged-in user's email address. This feature prevents spoofing and provides audit trails for administrators.

- With the **'Manual Destination Prohibit'** function, the direct input of an email address or scan destination is impossible. If this function is activated, only registered destinations from the internal MFP address book or LDAP can be used.

- Advanced **fax line security** is ensured by the bizhub fax connection using only the fax protocol for communication – no other communication protocols are supported. Konica Minolta products block any intrusion attempts as threats, including intrusions of a different protocol over public telephone lines, as well as any attempt to transmit data that cannot be decompressed as fax data.

- **Fax rerouting** allows automatic forwarding of incoming faxes to any destination within the internal bizhub address book, including for example email addresses, or to the user boxes on the bizhub's internal HDD. Storing incoming faxes in a user box is considerably safer, as there are no printed faxes to be seen in the output tray. This rerouting can also make the communication faster, as faxes reach their recipients sooner. Last but not least, it also helps save paper – recipients can decide whether printing a fax is really necessary.

- Most Konica Minolta devices support the **IEE802.11x standard** for network access control to WANs and LANs. These standards ensure a secure network by shutting down any network communications (e.g. DHCP or HTTP) to unauthorised devices, with the exception of authentication requests.



THE EVERYDAY CHALLENGE OF PROTECTING AGAINST SECURITY RISKS

It is important to remain aware of the fact that today no company or organisation is immune to security risks – security breaches happen everywhere, all the time! But prudent businesses look ahead and take the necessary precautions before it's too late. They ensure that the confidential data held by the hard disk and memory of digital printers, copiers and all-in-one equipment cannot be accessed in the first place, let alone tampered with.

Security-conscious company owners and managers ensure that their network is protected and that unauthorised access to information on the company's intranet is barred. Conscientious managers are also aware that the printers and copiers installed throughout the company can easily constitute the most serious of security gaps.

If left unattended in the output tray, confidential information might get into the wrong hands and could easily leave the company, for example via scan to email or fax transmissions. But prudent managers and IT specialists guard against these risks by reliably limiting access to devices to those authorised and by guarding against the unattended output of any kind of prints.

Konica Minolta supports its customers' efforts to protect against security risks by allocating extensive engineering resources to the advanced development of security-related features for bizhub MFPs and printers. Konica Minolta thus provides customers with the technology required in today's security-conscious environments.

Whether a customer is concerned about network intrusion, data theft or compliance with regulations, or whether the issue centres around limiting access to devices or functionalities, Konica Minolta bizhub technology offers professional solutions for the detection and the prevention of security breaches. This is the level of comprehensive protection that customers from all industries and public authorities now expect.

KONICA MINOLTA

Common Criteria Validated

Your Konica Minolta Business Solutions Partner:

Konica Minolta
Business Solutions Europe GmbH
Europaallee 17
30855 Langenhagen ◆ Germany
Tel.: +49 (0) 511 74 04-0
Fax: +49 (0) 511 74 10 50
www.konicaminolta.eu

10/2017