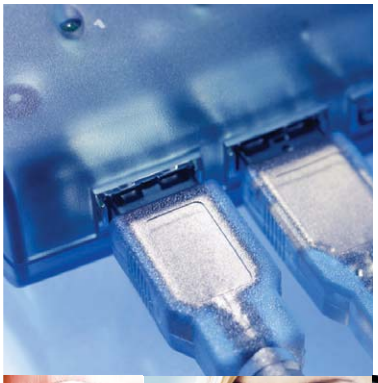
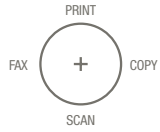
KONICA MINOLTA

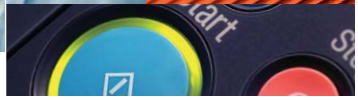
FUNDAMENTALS OF SECURITY FOR KONICA MINOLTA BIZHUB MULTIFUNCTIONAL DIGITAL OFFICE MACHINES

- ISO 15408 “Common Criteria”
- HIPAA
- Security Specifications





CONNECT_ COMMUNICATE_ CONTROL_



DO BUSINESS_BETTER

This Fundamentals of Security Guide is a "living" document – this means it is continually updated. This guide is intended solely for the use and information of **KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.**, its designated agents and their employees. The information was obtained from several different sources that are deemed reliable by all industry standards. To the best of our knowledge, this information is accurate in all respects. However, neither Konica Minolta nor any of its agents or employees shall be responsible for any inaccuracies contained herein.

Some functions may require options, which may or may not be available at time of launch.

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC., 100 Williams Drive, Ramsey, N.J. 07446

www.kmbs.konicaminolta.us

Table of Contents

NOTE:

Some of the specific security features and options described in this report may only apply to specific Konica Minolta bizhub models. It is best to refer to the documentation that is provided with every Konica Minolta bizhub MFP to verify exactly which security features are included with a specific product. It is also important to note that a specific machine may require an upgrade to achieve and/or enable some of the features discussed in this report. Please refer to your service representative for further information.

Introduction

With the dramatic increase in volume of sensitive and confidential information in electronic form, various government sponsored security regulations tie together the security and integrity of technological systems and processes. Security technology has become critically important as various organizations and businesses use their electronic systems to comply with government regulations. Recent laws and initiatives include:

- HIPAA (Health Insurance Portability and Accountability Act)
- Sarbanes-Oxley Act (Financial Accounting)
- Gramm-Leach-Bliley Act (Finance)
- Federal Information Security Management Act of 2002 (FISMA) and FDA 21 CFR Part 11 (Food and Drugs)
- ISO 15408, also known as, Common Criteria Certification

In response to these regulations, Konica Minolta has taken a lead role in developing and implementing security-based information technologies in Multi-Function office machines. Ever since the introduction of the first Konica Minolta MFP, Konica Minolta has strived to develop and implement technologies that safeguard the confidentiality of electronic documents.

With the growing popularity of connected Office Machines, people in various industries will increasingly look to MFPs as an efficient and cost effective method of distributing, storing and receiving sensitive electronic information. Security measures for Konica Minolta MFPs can easily be adopted for use in the wide range of industries where electronic document security is important. This requirement will grow more relevant as the trend towards electronic storage and maintenance of sensitive information continues. Whether installed in a small office as a workgroup device or in a large hospital as a departmental workhorse, Konica Minolta MFPs can provide you with the security, reliability and stability that security professionals demand and require. To date the only official security based certification standard for digital office products is an international standard generally known as Common Criteria. The official international designation for this security standard is ISO 15408. To date there are a number of Konica Minolta models that have achieved ISO 15408 EAL 3 (Common Criteria) certification.

Introduction

Konica Minolta ISO 15408 EAL Certified Models:

Color Multi-Functional Products

- bizhub C250
- bizhub C250P
- bizhub C252
- bizhub C252P
- bizhub C300
- bizhub C350
- bizhub C351
- bizhub C352
- bizhub C352P
- bizhub C450P
- bizhub C450P
- bizhub PRO 6500

Black & White Multi-Functional Products

- 7222/7228/7235
- 7145
- Di3510/f/2510/f/301/f/2010/f
- bizhub 750/600
- bizhub 500/420/360
- bizhub 350/250/200
- bizhub PRO 1050
- bizhub PRO 1050e
- bizhub PRO 1050eP
- bizhub PRO 1050P

In addition, there are currently several bizhub models that are “in evaluation” for the certification:

- bizhub C550
- bizhub C451
- bizhub PRO C5500

This document will discuss three important IT related security initiatives and explain how Konica Minolta MFPs comply with the various rules and regulations set forth in the following legislation and certification testing criteria:

- ISO 15408 (Common Criteria)
- Sarbanes-Oxley
- HIPAA (Health Insurance Portability and Accountability Act)

What is ISO 15408 or 'Common Criteria'

The International Common Criteria for Information Technology Security Evaluation is a relatively new program, which seeks to establish an internationally agreed-upon language for specifying security functionality, as well as an evaluation methodology to assess the strength of security implementations imbedded in various types of technologies located on the network.

This is taken from the Common Criteria web page http://niap.bahialab.com/cc-scheme/:

COMMON CRITERIA BACKGROUND

In June 1993, the sponsoring organization of the existing US, Canadian, and European criteria's started the CC Project to align their separate criteria into a single set of IT security criteria. Version 1.0 of the CC was completed in January 1996. Based on a number of trial evaluations and an extensive public review, Version 1.0 was extensively revised and CC Version 2.0 was produced in April of 1998. This became the ISO International Standard 15408 in 1999. The CC Project subsequently incorporated the minor changes that had resulted in the ISO process, producing CC version 2.1 in August 1999.

Today the international community has embraced CC through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of CC evaluations performed by other CCRA members.

COMMON CRITERIA IN THE UNITED STATES

The US is represented within the CC Project by the National Information Assurance Partnership (NIAP), a joint NIST and National Security Agency (NSA) project. NIAP, in turn, has established the Common Criteria Evaluation and Validation Scheme (CCEVS) to implement the CCRA compliant evaluation scheme within the US.

The Common Criteria Initiative has evolved into an international standard known as ISO 15408. In the US it is managed by the NIAP, which is run by the National Security Agency and the National Institute of Standards and Technology (NIST). There are seven levels of EAL (Evaluation Assurance Level) certification. Standard, "off the shelf" products can achieve only up to EAL 4 certification. Most IT related products are certified at EAL 3.

Fundamentals of Security

Up until this time Canon, Sharp, Xerox, Ricoh, Kyocera, Toshiba and Konica Minolta are the only Office Machine vendors to offer products that are certified for Common Criteria compliance. Many "security kits" are certified at EAL 2. The basis of the security kit certification, is data protection on the MFPs Hard Drive. The certification process is performed by a local testing facility. A certification lab in Japan tests Konica Minolta products. Because the Konica Minolta MFPs are certified in a Japanese testing facility, bizhub systems are not listed on the NIAP Common Criteria site. This has caused some confusion as to what is truly a NIAP approved product. As stated earlier, Common Criteria is an internationally recognized certification and as such, products tested in approved laboratories outside the US are fully recognized by NIAP here in the United States. This is the Mutual Recognition Statement published on the NIAP Common Criteria Home page:

> "Since the Common Criteria Portal is successfully up and running and in order to harmonize with other CC Schemes, the NIAP Staff is no longer posting certified products by other certificate-producing nations. The U.S. recognizes products that have been evaluated under the sponsorship of other signatories and in accordance with the International Common Criteria for Information Technology Security Evaluation Recognition Arrangement (CCRA) for EALs 1-4 only."

Konica Minolta Certifications and related documentation can be found at the following web site:

http://www.commoncriteriaportal.org/public/consumer/index.php

Here is the definition of the Konica Minolta Data Security evaluation for the bizhub PRO 1050 that is posted on the Common Criteria portal site mentioned above:

> **Product Description**
> This product (it is called "bizhub PRO 1050 control software (*1)", hereafter.) is the software installed with digital MFP (it is called "bizhub PRO 1050 series", hereafter.) manufactured by KONICA MINOLTA BUSINESS TECHNOLOGIES, INC. and for the purpose of reducing the danger to be leaked the document data stored by every user. bizhub PRO 1050 control software prevents the document data from leaking in the function to use copier and printer etc. To protect the document data, this software has "User Box" function and several control capabilities, additionally high-confidential hard disk drive (HDD) with lock system (*2) to store the document. bizhub PRO 1050 control software is provided with bizhub PRO 1050 series. (*1) "bizhub PRO 1050

zentai seigyo software" for Japan and "bizhub PRO 1050 control software" are the same product with different calling name. (*2) HDD has the password so that the hard disk cannot be removed and read in another equipment.

As you can see, by its nature Common Criteria Certification is ambiguous. Hardware and software developers submit their test parameters to a certification lab for testing. The testing lab or the certifying body does not tell the manufacturer what tests need to be performed to achieve EAL 3 certification. For example, EAL 3 does not require any specific security based function. It is up to the company submitting the product to define the parameters of the evaluation. So when a vendor submits a product (TOE - Target of Evaluation) and a ST (Security Target) the manufacturer asks the testing lab to verify the accuracy and integrity of the specific security related functions in the product. As you will see later in this document, Konica Minolta is one of the only vendors to certify the ENTIRE system and not just a kit or specific hard drive erase functionality. This is the definition of the Security Target and TOE:

Security Target (ST) — A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Target of Evaluation (TOE) — An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

http://niap.bahialab.com/cc-scheme/defining-ccevs.cfm

What is the Sarbanes-Oxley Act (SOX)?

Sarbanes-Oxley is a federal law enacted by congress in 2002. It is meant to protect shareholders from fraudulent accounting practices that occurred in the 1990's that resulted in corporate melt-downs that happened at Enron and other publicly traded companies. This is a quote from SEC Chairman William H. Donaldson:

> "Inattention to good corporate governance practices over the past decade or more is at the heart of what has gone so terribly wrong in corporate America in the past few years. If significant steps are not taken to revisit and remodel corporate governance practices, corporate America will continue to attract the anger and animosity not only of disillusioned shareholders, but also of a much broader cross-section of American society."
>
> – SEC Chairman William H. Donaldson, March 24, 2003

There are two key sections of the law that relate to digital office machines (MFPs): Section 404 and Section 409.

SECTION 404: MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

Requires each annual report of an issuer to contain an "internal control report", which shall:

1. State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
2. Contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
3. Each issuer's auditor shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this section shall be in accordance with standards for attestation engagements issued or adopted by the Board. An attestation engagement shall not be the subject of a separate engagement.
4. Directs the SEC to require each issuer to disclose whether it has adopted a code of ethics for its senior financial officers and the contents of that code.
5. Directs the SEC to revise its regulations concerning prompt disclosure on Form 8-K to require immediate disclosure "of any change in, or waiver of," an issuer's code of ethics.

What does this mean?

Internal Control Reports
Each annual report must include an "internal control report" stating that management is responsible for an adequate internal control structure, and an assessment by management of the control's effectiveness. Any shortcomings in these controls must be noted.

External Auditor's Attestation (verification)
Registered external auditors must attest to the accuracy of management's assertion that internal controls are in place and are effective.

How does this relate to MFPs in the office?
Most financial documents are in the form of paper. These documents are financial evidence and need to be collected stored and managed. Purchase orders, invoices, contracts, expense reports and checks.

Sarbanes-Oxley stipulates that financial reports are accurate and verifiable. These paper-based documents can contribute to the authenticity of a company's financial status. Potentially thousands of documents may now need to be stored and retrieved in a timely and accurate manner. In addition, audit trails and document integrity may need to be verified.

Office MFPs and back-end document management applications can help an organization satisfy these requirements. Companies can use MFPs to print, store and distribute these documents

SECTION 409

Real Time Disclosure

Companies are required to disclose, "On a rapid and current basis such additional information concerning material changes in its financial condition or operations."

The SEC has not yet released a deadline for Section 409. However, the ability to provide immediate access to pertinent financial information will be a challenging task for corporate IT executives.

Sarbanes-Oxley requires public companies to have controls in place that manage the document lifecycle. This applies to paper as well as electronic documents

Konica Minolta MFPs in conjunction with document management applications can provide compliance with Sarbanes-Oxley legislation.

What is HIPAA?

HIPAA (Health Insurance Portability and Accountability Act) is a law that was passed by Congress in 1996; its intention is to protect basic personal information related to health care privacy. The law was also intended to streamline heath-care document management practices by providing a set of rules for electronic document management, related to the privacy of the patient and the accountability of the health care provider.

With the passage of HIPAA, all health-care related facilities are concerned about HIPAA regulations and how they apply to the security of MFP printing, copying and scanning functions in the office. In addition to the health care industry, many organizations are aware of this emerging trend for electronic document storage, and are concerned about security issues related to electronic document distribution.

The security regulations have just recently come into effect for large health care providers:

This white paper will review how Konica Minolta multi-functional devices offer a broad range of features supporting individual privacy and security rights. Some of the major security features offered by Konica Minolta devices are the following:

- All Konica Minolta devices (as standard factory equipment) offer the feature of account job tracking by user (accountability).

- When programmed; the device can be set up to allow copies, scans, faxes or prints only by users who have a valid Personal Identification Number (PIN) or Account number. Users who do not possess a valid PIN or Account number cannot make a copy, send a scan/fax or produce a print.

- When this function is turned on, Konica Minolta MFPs (Multi-Functional Devices) can track detailed device usage by individuals' PIN or Account numbers.

- When enabled, several Konica Minolta devices can track prints by user name, time of the print, the name of the file, how long it took to print and how many copies were produced. In addition, this detailed information can be downloaded electronically from the machine to a desktop computer and imported as a common data file into popular applications such as Microsoft Excel. This feature allows healthcare administrators to track individual usage by who printed a document, when it was printed, the name of the file, how many copies were produced, and how long it took to print the file.

- On EFI Fiery® based products, an administrator can view the actual documents that a user printed. Of course, this function is password protected.

- Some Konica Minolta devices can be programmed to submit print jobs entirely via RAM (Random Access Memory), when printed these jobs are physically erased from memory, eliminating any possible reproduction of the document from the bizhub's Random Access Memory (RAM).

- As walkup copiers, Konica Minolta MFPs offer the ability to store recently copied jobs into memory. Konica Minolta devices can be programmed to automatically reset after a fixed period of inactivity. For example, a health care worker logs into an MFP with a unique Personal Information Number, copies a file and walks away forgetting to log out of their session at the device. The MFP would detect no user activity and after 30 seconds reset itself to the PIN login state. As a security precaution, Konica Minolta has decided to eliminate the "reprint" feature from New Konica Minolta MFPs.

The final HIPAA Security Rule was published on February 20, 2003. The rule details several standard and implementation specifications for Protecting Health Information related to IT, Technology and systems that include Private Health Information. Contained in this paper is a list of these Standards and implementation specifications and how Konica Minolta MFPs comply.

The HIPAA Security regulations are applicable to Electronic Protected Health Information (ePHI) and not for traditional office communications such as facsimile or telephone. As one can imagine, the Standards and Implementation specifications are general in nature and open to interpretation. It is also important to note that many of the Security specifications are not related to Technology but to HR and other areas of compliance. For example, there is a required specification, which calls for workforce sanctions related to violations of security policies and procedures.

It is also important to know the difference between Required and Addressable specifications:

Required - Measures include workforce sanctions for violations of security policies and procedures, a data backup plan, entering into business associate agreements, unique user identification access controls, device and media disposal procedures, and person or entity authentication procedures.

Addressable - Covered entities must first assess whether each addressable specification constitutes a "reasonable and appropriate safeguard" in its environment,

based on the specification's likely contribution to protection of electronic PHI. If the entity determines that an addressable implementation specification is reasonable and appropriate, it must implement the measure. If it determines the opposite, then it must document that decision and implement an equivalent alternative measure, if reasonable and appropriate.

The Security Rule sets forth security standards that define administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic Protected Health Information ("ePHI"). Subpart C of the Security Rule sets forth eighteen security standards that must be implemented through thirteen "required" implementation specifications and twenty-two "addressable" implementation specifications. Although the majority of the Standards do not apply to Digital Office MFPs, In Appendix A, we list all of the standards and implementation specifications for the convenience of the reader.

HIPAA Security Standards that are applicable to Konica Minolta Digital Multi-Functional Machines.

Listed below are Standard features on Konica Minolta MFPs that satisfy specific HIPAA Security Specifications (the Standards and Specifications are in Blue/Italics):

ACCESS CONTROL, TECHNICAL SAFEGUARDS

The following functions satisfy the HIPAA Security Specification, Access Control Section Technical Safeguards (Section 164.312):

> *(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).*
> *(2) Implementation specifications:*
> *(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.*

LOCK JOB/SECURE PRINTING

Konica Minolta MFPs offer a standard feature called Secure Printing. This feature provides to the User sending the print job the ability to hold the Job in the memory of the system - Until that person walks up to the machine and releases the job by inputting a unique, secure, PIN/Password at the control panel of the MFP. This number is input by the User when they submit a print job from the PC workstation. This process ensures that only the sender of the job can access an electronic document that contains ePHI. In addition, those MFPs equipped with a hard drive have the ability to store electronic PHI inside the system. When these documents are stored — either by sending them from a PC or by scanning them in at the copier — users cannot retrieve the document unless a secure PIN/password is input at the copier's control panel.

Figure 1 illustrates the Secure Print feature accessed from the bizhub C450 PostScript print driver via the setup tab. From here the User inputs their unique Job ID and Secure Print Password (figure 2):

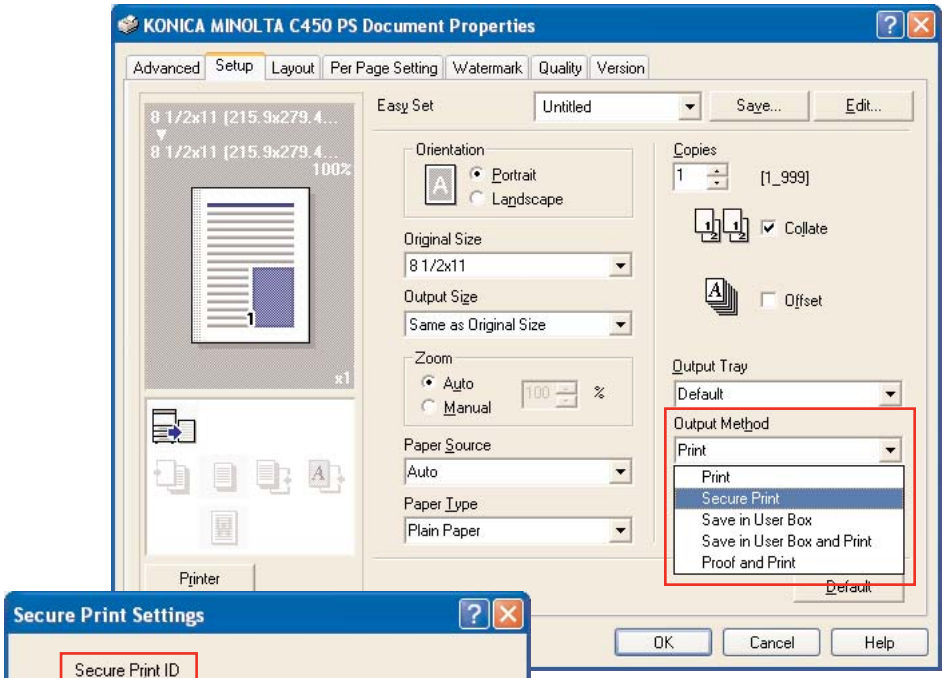


Figure 1

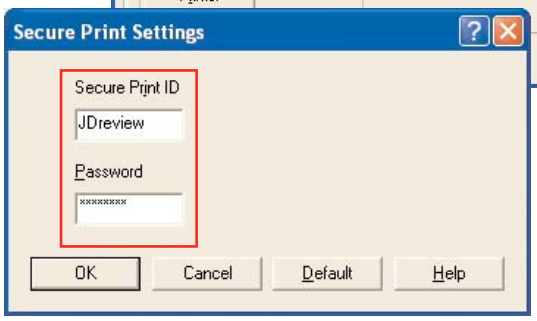
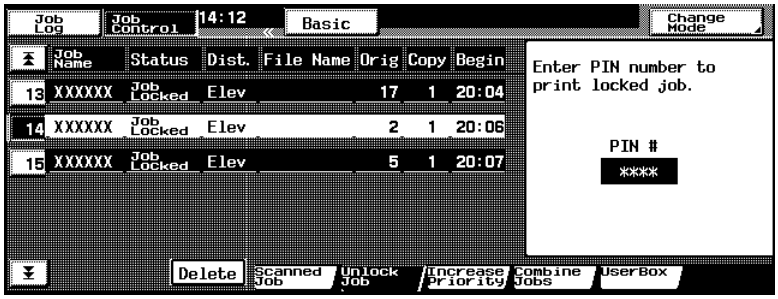


Figure 2

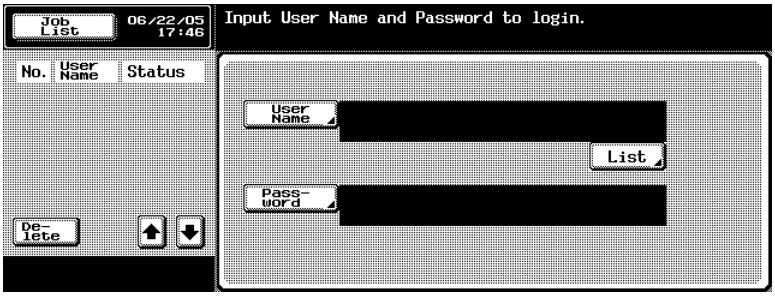
This is an example of the control Panel of the Konica Minolta bizhub C450 where there are a number of “Locked Jobs” waiting to be released:



ACCOUNT TRACKING

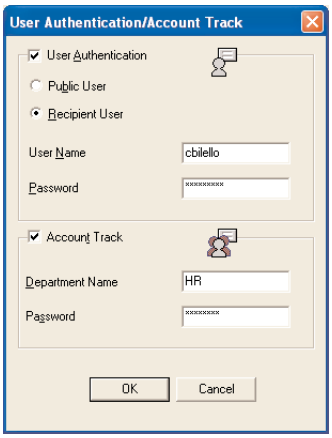
Konica Minolta bizhub MFPs come standard with the ability to enable Account Tracking. When this function is enabled, a User is required to input a 1-8 alphanumeric character password before they are granted access rights to make a copy, send a print, or perform other functions at the MFP. If a user does not submit or enter an authorized password (from the print driver), the print job submitted will not be printed. If a User does not enter an authorized password at the copier control panel, they will be denied access rights to the system. When logged in, the User’s activities are electronically recorded onto a log file inside the system. An Administrator or Key Operator can access this file. This is a very popular feature for many customers, who use this to bill departments and audit individual’s copier activities.

This is an example of the secure access screen from the Konica Minolta bizhub C450 control panel:



Fundamentals of Security

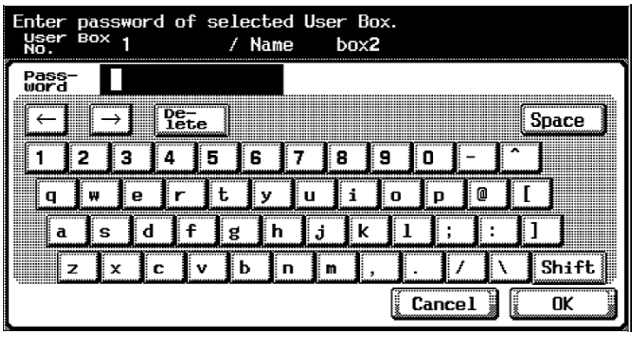
This is the User Authentication/Account Track dialog box for the Konica Minolta C352 PCL driver:



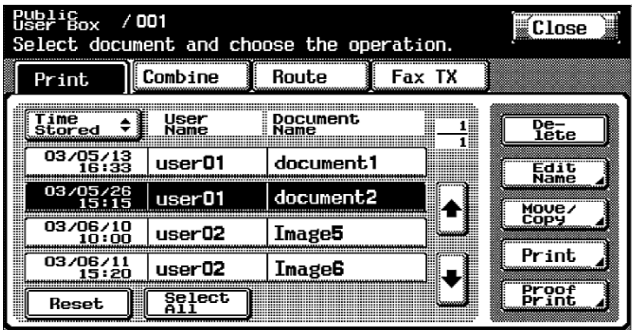
Notice that there are fields to input the User Name, Department Name and associated passwords.

When equipped with optional Hard Drives some Konica Minolta devices support walk up scanning and storage of printed documents to the MFPs internal Hard Disk Drive. This application is popular for users who would like to store frequently used jobs for later recall, distribution and printing. This function is commonly referred to as scanning or printing to a “Mailbox”. On Konica Minolta MFPs, mailboxes are password protected. A user must set up a mailbox using a unique password (PIN) in order for the user to store a job into a mailbox storage folder in the internal hard drive.

When a User wants to recall a scanned or printed job, he/she is presented with the password entry screen.



After inputting a password the User is presented with a screen requesting a job name:



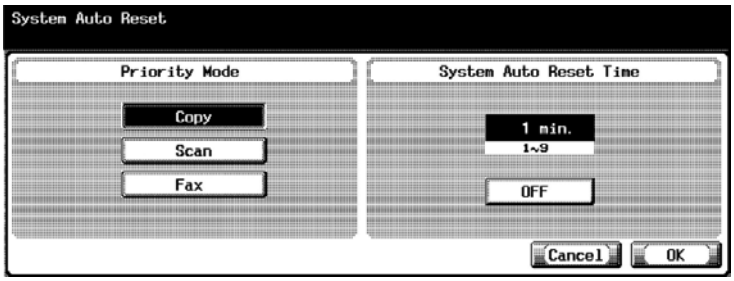
AUTOMATIC RESET/LOG-OFF

The following function satisfies the HIPAA Security Specification Section 164.312 (a)(2)(iii): Automatic Log-Off (A) - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

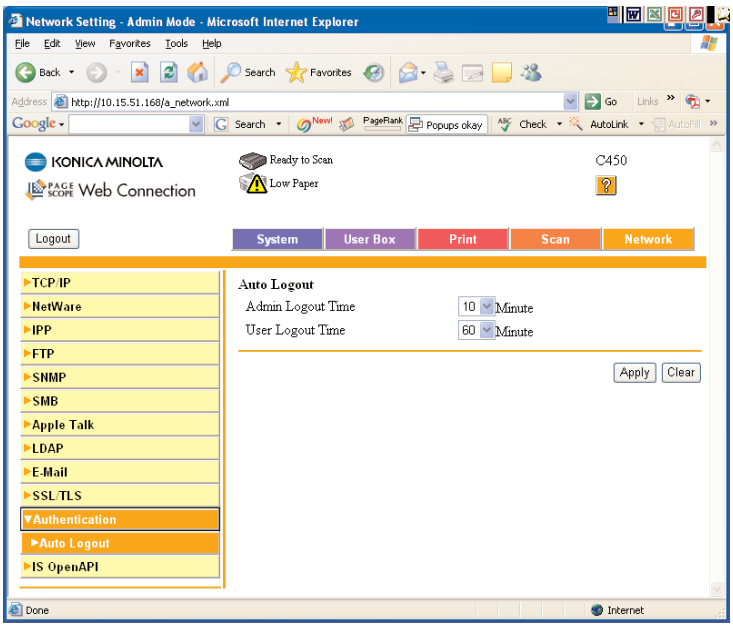
Konica Minolta MFPs can be programmed to automatically reset to a state that requires password input after a predetermined time of inactivity. This ensures that the MFP will reset to a secure state if a User forgets to logoff from an MFP when finished with their session.

Notice that the reset timer can be set from 1 to 9 minutes. Some Konica Minolta MFPs can be programmed to reset in as little as 30 seconds. If the machine has the Account Tracking function enabled the machine will enter a state (after a preprogrammed period of inactivity) that requires a User to enter a unique PIN or password. This function should satisfy most concerns about someone forgetting to log off after they are finished scanning or copying documents at the MFP.

bizhub C450 Panel Reset Setting



This Screen illustrates the Administrator and User Auto Log Off timer setting that is accessible via the MFPs remote Web Browser based interface (PageScope Web Connection).



ENCRYPTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

bizhub OP based products can encrypt scanned files in PDF format before sending them to a destination across the network. The User has the ability to encrypt a scanned file by selecting the Encryption key on the bizhub's control panel. The encryption option supports the PDF file type and will require the receiver of the scan to have the decryption code to open the file. This feature is very similar to the Adobe Acrobat encryption process where a password is utilized for encryption and opening a file as well as, for accessing the permissions area of the encryption process.

In addition Konica Minolta Business Solution offers an optional Hard Drive Encryption Kit.

If desired, electronic documents can be stored in a password protected mailbox on the hard drive. If an organization is concerned about the security of this data, there is an optional Hard Drive encryption kit available. The stored data can be encrypted using the Advanced Encryption Standard (AES) supporting 128-bit key size. Once a HDD is encrypted the data cannot be read even if the HDD is removed from the MFP.

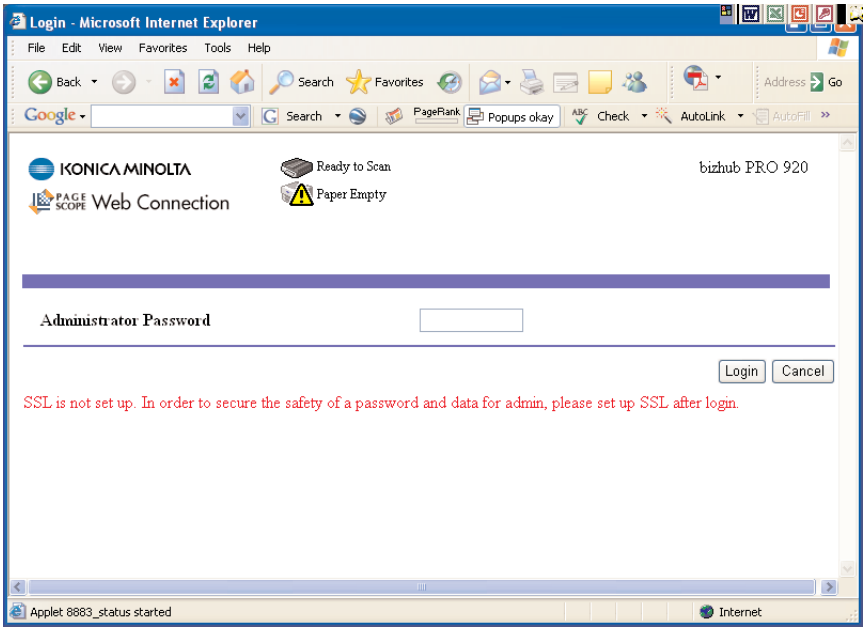
PHYSICAL SAFEGUARDS

The following function satisfies the HIPAA Security Specification Section 164.310 - Physical Safeguards. (c) Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

PASSWORD LEVELS TO ACCESS DOCUMENTS ON MFPS FROM REMOTE WORKSTATIONS

Many Konica Minolta devices offer the ability to remotely access (via Workstation) print and scanned jobs. This feature can be either disabled or Password protected using unique Personal Identification Numbers (PINs).

This is a sample login screen to a bizhub's built in Web Server showing password protection:



Notice the Administrator's Login field.

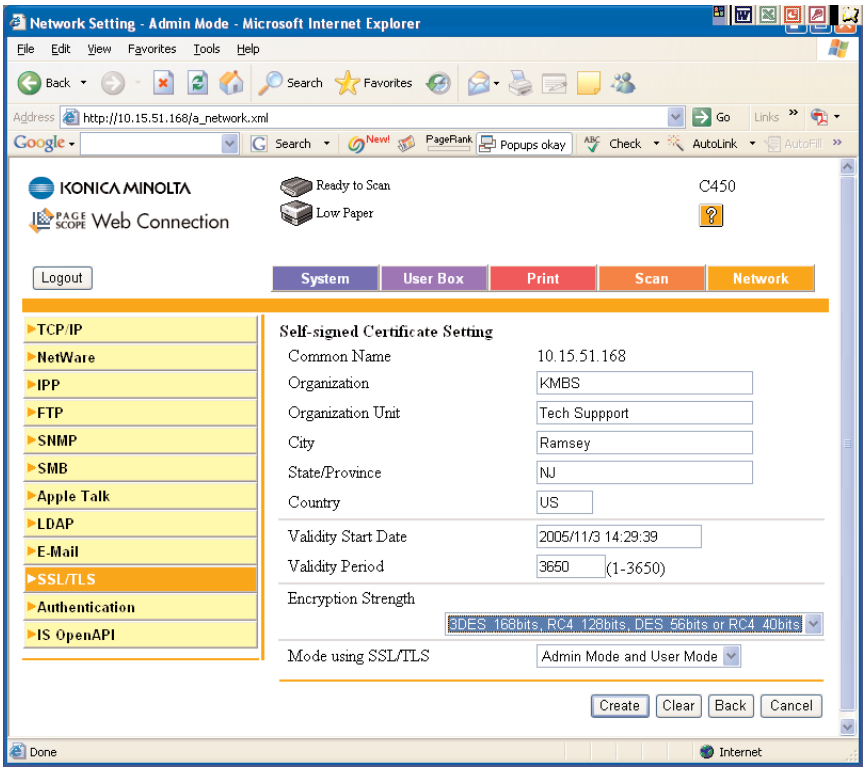
In addition, the following models offer Kerberos password protection/encryption:

- bizhub C450/C352/C351/C250
- bizhub 750, 600, 500, 420
- bizhub 350/250/200 series

The following Konica Minolta devices support SSL (Secure Socket Layer) encryption of data communication between the device and an LDAP Server, PageScope Web Connection and PageScope Data Administrator:

- bizhub C450/C352/C351/C250
- bizhub PRO 1050, PRO?920, 750, 600
- bizhub 350/250/200

This is an example of setting up SSL via PageScope Web Connection on a bizhub C450:



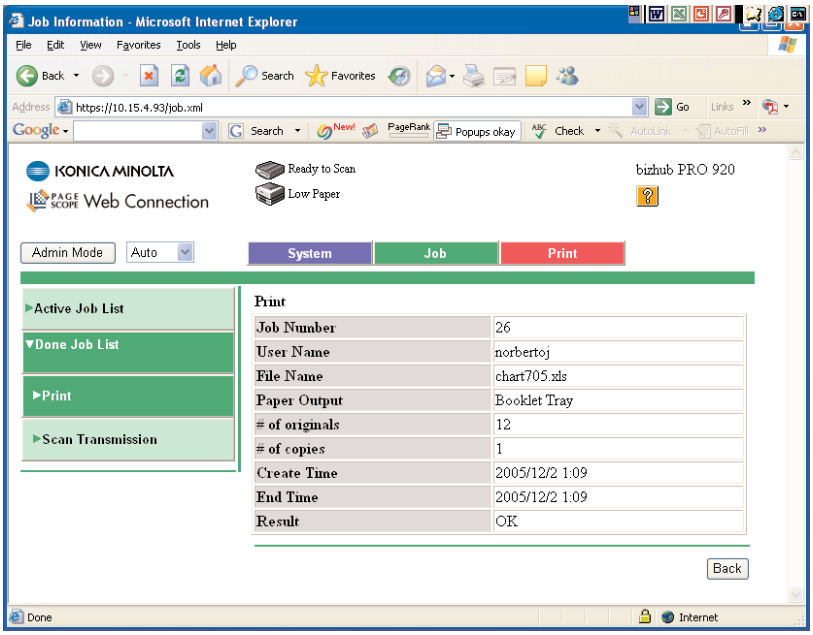
AUDIT CONTROLS

The following function satisfies the HIPAA Security Specification Section 164.312 Technical Safeguards -(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

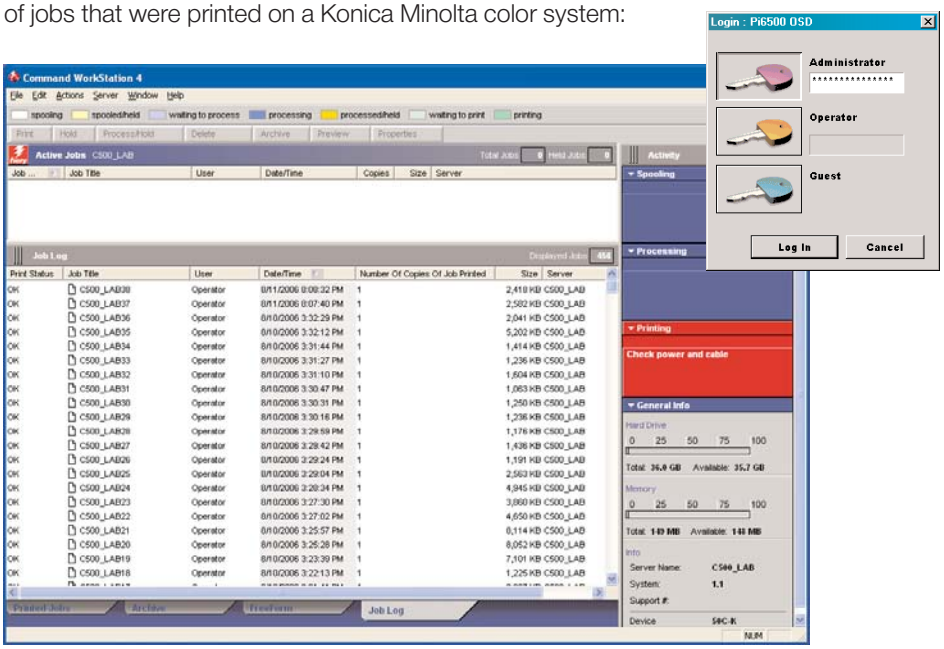
JOB LOGS

Many Konica Minolta system print controllers contain electronic job logs that record all print jobs sent to the MFP. For example, The EFI Fiery Job Log records all print jobs sent by named users. The EFI Fiery Job Log records when the job was printed, how many copies, the time it was printed etc. In addition, Konica Minolta PageScope Router and Rebus Recollect Document Management System software contain comprehensive electronic tracking logs of user activity as well.

This is a sample record from the bizhub PRO 920's job log:



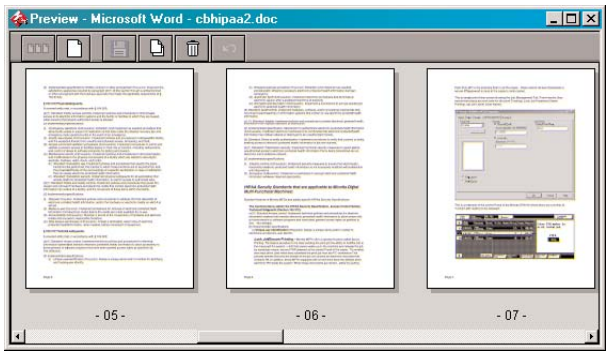
This is a sample Fiery Job Log screen showing detailed information of jobs that were printed on a Konica Minolta color system:



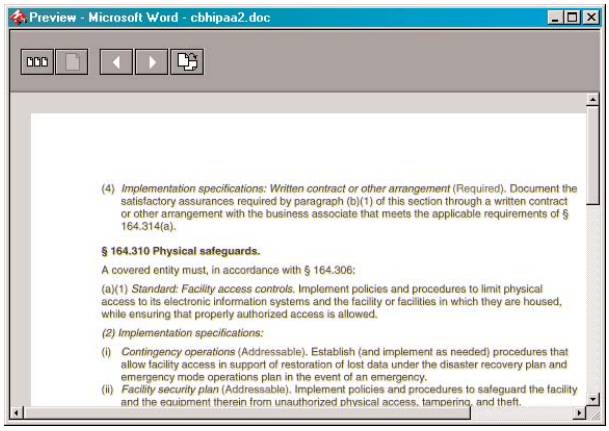
Notice the status of the print jobs. The system can be programmed to automatically print out a log of print jobs after every 55 print jobs. A copy of the Cumulative Log is held on the Hard Disk Drive indefinitely.

As mentioned earlier, the Fiery based print controllers can store from 10-99 previously printed jobs. The jobs can be reprinted using the Command WorkStation application. This feature provides the ability to examine and determine exactly what jobs were printed by whom and at what time and date. The jobs can be re-printed for examination or can be previewed using the Command WorkStation utility. This is an important function if a Health Care Security professional desires the ability to monitor and Audit print jobs that are sent to a specific system.

Here is an actual screen taken from the Command WorkStation depicting "Thumbnail Previews" of a job that was previously printed. Of course this screen is Password protected (right):



A zoom view is also available — using the zoom, documents can be examined word by word.



PHYSICAL SAFEGUARDS

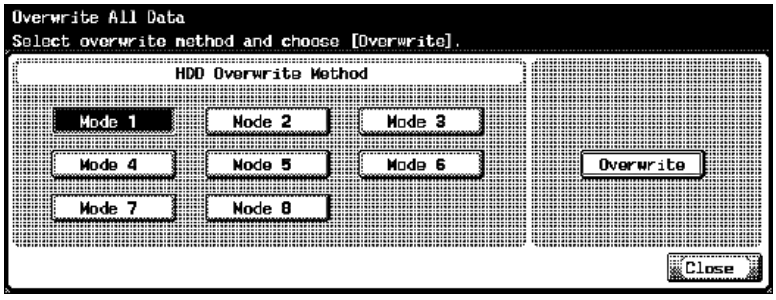
The features explained below satisfy various requirements under Physical Safeguards, Section 164.310:

Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) Implementation specifications:
(i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

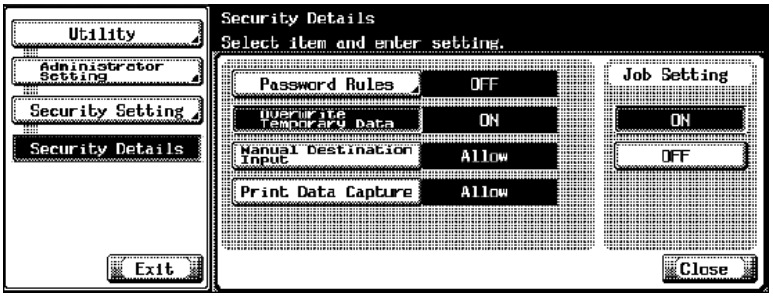
Format/Erase Hard Drives on bizhub MFPs.

When equipped with a hard disk drive (HDD), Konica Minolta MFPs can store ePHI. The data is erasable (deleted) by users who own the documents that reside inside the MFPs HDD (inside Password Protected Mailboxes). For added safety, a Key Operator, Administrator or technician can physically format (erase) the HDD if the MFP needs to be relocated. The hard drives can be overwritten (sanitized) using a number of different methods, conforming to military specifications. Please see table1, on page 33, for further details.



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 3x as well.

This configuration is from the bizhub C450's Security Mode Panel.



BYPASSING HARD DISK DRIVES WHEN PRINTING

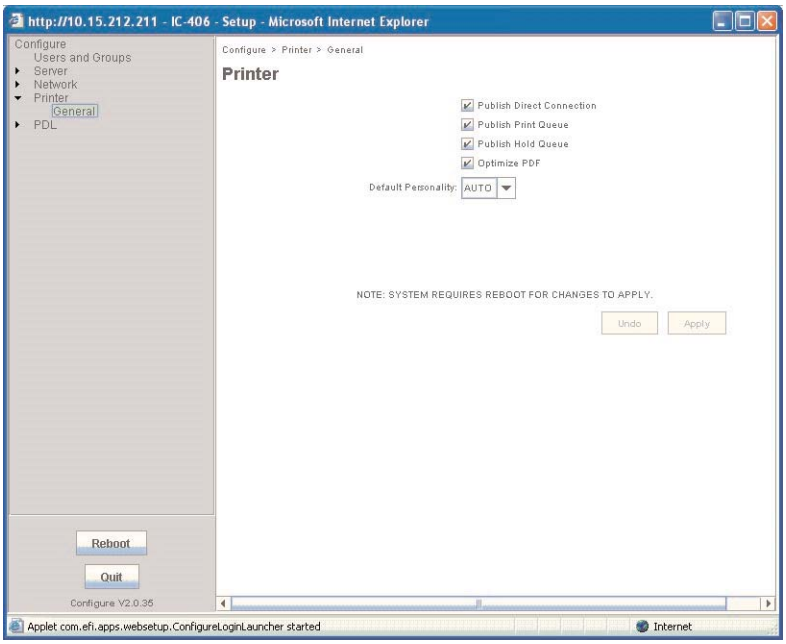
When equipped with Hard Disk Drives, Konica Minolta Fiery based print controllers can store ePHI that is printed from end-user workstations and PCs. This data can remain on the Print controller HDD – An IT administrator can set up the connection from end-user PCs that bypass the print controller hard drive and send the document to be printed via system RAM. Once the job is printed it is completely erased from system memory. This eliminates any risk of unauthorized access of any ePHI that was printed on the system.

In addition, many Konica Minolta bizhub MFPs offer an **optional** hard drive. If the customer is overly concerned about sensitive data, the recommendation is not to install the Hard Drive in the bizhub product.

The following machines offer an optional hard drive:

- bizhub C250
- bizhub 750
- bizhub 600
- bizhub 500
- bizhub 420
- bizhub 350
- bizhub 250
- bizhub 200

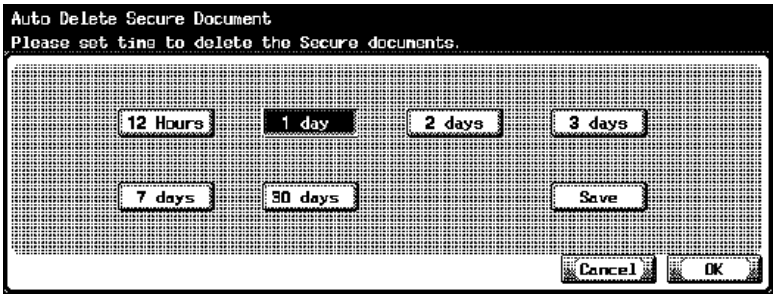
Below is a screen capture from a Fiery based controller showing the disabling of all Queues except the Direct Queue. This is where the setting can be made to disable the Fiery's hard drive based queue. When this setting is made, users can only send print jobs to the RAM of the print controller. After a job is printed it is completely erased from memory, making access physically impossible.



AUTOMATIC DELETION OF SECURE DOCUMENTS KONICA MINOLTA bizhub MFPS

Many (CE) Covered Entities Security professionals are concerned about scanned ePHI residing on the MFP. Most people wish to use the Secure Print functionality of the MFP, however, they are concerned about the risks. As mentioned before, ALL confidential print jobs can be password protected. In addition, the bizhub MFPs can be programmed to automatically delete Secure Jobs residing in memory at pre-determined intervals.

This is the setting to automatically delete Secure Documents on a Konica Minolta bizhub C450.



DEVICE AND MEDIA CONTROLS, ACCOUNTABILITY AND DATA BACKUP AND STORAGE

Konica Minolta Document management software solutions can assist a Covered Health Care Entity comply with the following standards:

(d)(1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
(2) Implementation specifications:
(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

KONICA MINOLTA SOLUTIONS FOR BACKUP STORAGE, ARCHIVAL AND RETRIEVAL OF ELECTRONIC PROTECTED HEALTH INFORMATION

Konica Minolta markets and sells Rebus Technology's Recollect® Software that has been developed to work together with Konica Minolta MFP scanning functions. This system electronically archives documents by using a Konica Minolta bizhub MFP and Recollect software. Konica Minolta's bizhub products scans the hard copy documents and automatically delivers them to Recollect, which transforms almost all paper-based documents into an electronic archive that is accessible simply by typing in the words that you are looking for.

Konica Minolta Business Solutions and Rebus Technology Inc. have entered into a strategic partnership to offer the best Document Management solution in the marketplace. Rebus Technology Inc. has worked closely with Konica Minolta's Solutions Research and Development Team in tailoring Recollect software to work seamlessly with Konica Minolta's MFPs, Micrographic equipment and Book Scanners.

When installed in a Health Care environment Recollect can satisfy an important HIPAA requirement under the Device and Media Controls section – Data backup and storage. Recollect provides extensive backup, storage and retrieval of ePHI. Some of the advanced storage and retrieval functions include powerful document compression — use less storage space with multiple file-compression options like CCITT-Group IV, CCITT Group III, JPEG.

Unlimited storage capacity — access unlimited storage space by moving documents to any Windows or network operating system storage device—such as ZIP, CD-ROM, DVD Jukebox and JAZ drives. These features provide an easy way to backup and restore systems even during emergencies. Document can be stored on DVDs and secured in remote safe locations.

Recollect Provides Portable, Unlimited Document Storage

- Patented Portable Document Indexing
- Supports removable storage devices
- Search across multiple drives concurrently – DVD, CD-ROM, ZIP, Local hard drives and other storage devices
- Search multiple CD-ROMs without shuffling all the CD-ROMs

One-Step-Retrieval

Recollect builds an index of every significant word on every page, so finding any document Is simple. Just type in a search word or two, and in seconds, Recollect displays a prioritized list of all the documents which meet your criteria, along with a thumbnail view of each. Open the one you want and Recollect brings you to the page you need and highlights the word on the page for you. Recollect's powerful and patented Fuzzy Search technology even compensates for OCR errors, finding documents that contain misspelled or fragmented words.

Familiar Storage System

Recollect takes the familiar Windows Explorer look-and-feel and turns it into a powerhouse of functionality. Documents are stored in the same style hierarchy, and the familiar icons for folders, file names, and drives are all there in Recollect. Recollect allows users to Include or Exclude entire drawers as desired from any storage media.

Portable, Unlimited Document Storage

Recollect performs index updates on the fly, offering incredible speed when copying, moving or renaming documents. Now you can share information over a networked Recollect Server, reorganize all your documents, or back everything up to removable media with drag-and-drop ease. And because Recollect supports any Windows-compatible storage device you never have to worry about running out of disk space, in the office, the enterprise or on the road.

Activity Log

- Recollect has the ability to track activity as it relates to:
- Document searches
- Document changes such as adding pages, reorganizing pages or deleting pages
- Renaming documents
- Moving documents between folders and drawers
- Page level changes such as adding a note or highlight text
- User level searches and access of the documents, including print and mail activities
- Electronic drawers and folders activity including adding, moving, changing, renaming and deleting of the electronic filing hierarchy
- This activity log can be printed for each and every electronic drawer managed by Recollect

Security Level Access

Recollect Enterprise inherits security rights from the base Novell or Windows Network Operating System. A registered Novell or Windows network user can be added to the Recollect system and given rights to read only or to read and modify the contents of the electronic filing system. A non-registered Novell or Windows identity cannot access the Recollect Enterprise System.

HIPAA CONCLUSION

With the dramatic increase in volume of protected health information in electronic form, HIPAA privacy requirements tie together the security and integrity of technological systems and processes. Technology security has become critically important as covered entities use their electronic systems to comply with HIPAA regulations. With the growing popularity of connected Office Machines, people in the health care industry will increasingly look to MFPs as an efficient and cost effective method of distributing, storing and receiving ePHI. Security measures for Konica Minolta MFPs can easily be adopted for use in the health care industry and will grow more relevant as the trend towards electronic storage and maintenance of protected health care information continues.

Whether installed in a small office as workgroup device or in a large hospital as a departmental workhorse, Konica Minolta MFPs can provide you with the security, reliability and stability that health care professionals demand and require.

Legal Disclaimer: This paper is for general informational purposes only and does not represent legal advice or a legal opinion. Because of its generality, it may not be applicable to your specific situation. For legal advice, you should consult with legal counsel or Health Care Security Officer regarding your own particular legal needs. This paper is current as of October 1, 2006.

NOTE:

Some of the specific security features and options described in this report may only apply to certain Konica Minolta machines. It is best to refer to the documentation that is provided with every Konica Minolta machine to verify exactly which security features are included with a specific machine. It is also important to note that a specific machine may require an upgrade to achieve and/or enable some of the features discussed in this report. Please refer to your service representative for further information.

ISO 15408 or 'Common Criteria' Standards that are applicable to Konica Minolta Digital Multi-Functional Machines.

As stated earlier, the industry standard certification for computer security is ISO 15408, also known as 'Common Criteria'. ISO, or International Organization for Standardization, is a network of the national standards institutes from 156 countries. This network is made up of one member from each country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization: its members are not, as is the case in the United Nations system, delegations of national governments.

The ISO occupies a special position between the public and private sectors. This is because, on the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

Therefore, ISO is able to act as a bridging organization in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users.

Because "International Organization for Standardization" would have different abbreviations in different languages (IOS, OIN), it was decided at the outset to use a word derived from the Greek isos, meaning, "equal", hence ISO.

Within the ISO 15408 standard there are seven categories dedicated to security levels, they are described as Evaluation Assurance Levels or EAL. EAL3 or level 3 is the industry standard for digital MFPs.

ISO 15408 CERTIFICATION OVERVIEW

For Konica Minolta, the Target of Evaluation regarding ISO 15408 certification is the 'Total System'. Many of the current manufacturers have achieved an ISO 15408 certification for a specific Data Security Kit, Data Protection Kit, Software package or an MFS + Image Overwrite feature. These certifications are for the Security option only, not the entire system. Konica Minolta's total system certification applies to:

Machine	Certification
bizhub 7145	EAL 3 Certified
bizhub 7235/7228/7222	EAL 3 Certified
bizhub Di3510/3010/2510/2010 series	EAL 3 Certified
bizhub C350	EAL 3 Certified
bizhub PRO 920	EAL 3 Certified
bizhub PRO 1050	EAL 3 Certified
bizhub PRO 1050P	EAL 3 Certified
bizhub 350/250/200	EAL 3 Certified
bizhub C250	Currently in evaluation for EAL 3
bizhub C450/C351/C352	Currently in evaluation for EAL 3
bizhub 500/420	Currently in evaluation for EAL 3
bizhub 750/600	Currently in evaluation for EAL 3

HDD AND RAM SECURITY

Data theft is the leading concern by end-users, corporations/business, government and manufacturers alike. One particular fear is that critical data can be stolen from the MFPs Hard Disk Drive (HDD) or RAM, either by accessing the MFP remotely or removing the HDD or RAM and extracting the data after the MFP has been discarded. These concerns have been addressed for each technology; HDD and RAM.

RAM Security – Random Access Memory, there are 3 types of RAM currently being used by bizhub products:

- Volatile RAM
- Non-Volatile RAM
- Flash Memory

Volatile RAM – Typically Volatile RAM would be:

- File Memory – electronic sorting
- Work Memory – storing program parameters, temporary data and image conversion of controller
- Fax Memory – working RAM for fax

Data that written to Volatile RAM is held while the power is 'ON'. The data held in this type of RAM is overwritten by the next page or job being printed. Once the job is printed the data is deleted from RAM. Also, if the power is turned 'OFF' the data in Volatile RAM is deleted. Volatile RAM is secure, if RAM is removed after an engine is powered OFF all the data on that RAM chip would have already been deleted. It would be impossible to remove the RAM while the engine power is ON. The only other way to possibly extract data would be an indirect route or a security hole. These access points have been evaluated and tested by 3rd party security consultants before the KMBS products were sent for ISO 15408 certification. There are no indirect routes or security holes present in bizhub MFPs.

Non-Volatile RAM (NV_RAM) – Typically Non-Volatile RAM would be:

- Counter Data
- Job Settings
- Utility Settings

The data written to Non-Volatile RAM is not image or document data, meaning the data is not confidential or private. This data is not cleared when the power is turned 'OFF' unlike Volatile RAM. It is important to note that when the HDD is formatted the User/Account data, data in NV-RAM will be deleted and set back to factory default.

Flash Memory Stores – Typically Flash memory is utilized with:

- Machine Firmware
- Control Panel Data
- Printer Resident Fonts
- Copy Protect Watermarks

Flash Memory is embedded on an MFP circuit board and cannot be erased. The data stored in Flash Memory is not critical, confidential or private.

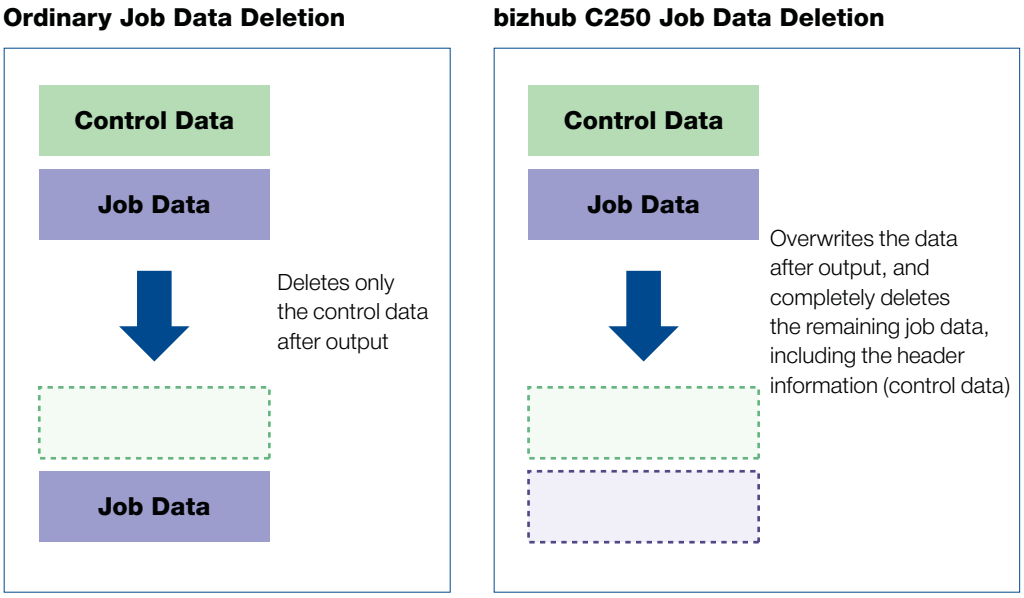
HDD SECURITY

The current line of bizhub products ship with or offer an optional 20, 40 or 80 GB HDD. The HDD is protected from data theft with the use of the security technologies listed below. An Administrator can control the use of each of these functions individually or in combination.

- Job Overwrite (Temporary Data Overwrite)
- HDD Encryption (option)
- HDD Lock Password
- HDD Overwrite or HDD Sanitizing

Automatic HDD Job Overwrite (Temporary Data Overwrite)

As mentioned earlier, an administrator can set the bizhub to automatically overwrite any residual image data from the Hard Drive.



There are two Job Overwrite Modes to choose from:

Overwrite Method		Compliance
Mode 1:	Overwrite with 0x00	US Navy NAVSO P-5239-26 & Department of Defense DoD 5220.22-M
Mode 2:	3 times overwrite: – Overwrite with 0x00 – Overwrite with 0xff – Overwrite with A (Dx61) – Verify	US Air Force AFSSI5020

Job data can be overwritten automatically when a job is printed or after a job is deleted from the User Box.

HDD Encryption

If desired, electronic documents can be stored in a password protected mailbox on the hard drive. If an organization is concerned about the security of this data there is an optional Hard Drive encryption kit available. The stored data can be encrypted using the Advanced Encryption Standard (AES) supporting 128-bit key size. Once a HDD is encrypted the data cannot be read even if the HDD is removed from the MFP.

The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector. (Encryption for the US military and other classified communications is handled by separate, secret algorithms.). AES is a Federal Information Processing Standard (FIPS) and is outlined in FIPS Publication 197.

In January of 1997, a process was initiated by the National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department, to find a more robust replacement for the Data Encryption Standard (DES) and to a lesser degree Triple DES. The specification called for a symmetric algorithm (same key for encryption and decryption) using block encryption (see block cipher) of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next 20 to 30 years. It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques.

HDD Lock Password

The bizhub's hard disk drive can be locked using a passcode of 20 alphanumeric characters. The data stored on this HDD is protected. Even if the HDD is removed from the MFP and installed into a different MFP or PC, the data cannot be read.

HDD Overwriting or HDD Sanitizing

At the time of decommissioning, relocation or with the replacement of a bizhub, the entire HDD can be overwritten so that all of the data is completely removed. This can be achieved using one of the 8 following Modes and corresponding Overwrite Methods (see table 1).

TABLE 1

Mode	Overwrite Method	Compliance
Mode 1	Overwrite with 0x00	Japan Electronic & Information Technology Association Russian Standard (GOST)
Mode 2	Overwrite with random 1 byte numbers	Current National Security Agency (NSA) standard Overwrite with random 1 byte numbers Overwrite with 0x00
Mode 3	Overwrite with 0x00 Overwrite with 0xff Overwrite with random 1 byte numbers Verified	National Computer Security Center (NCSC-TG-025) US Navy (NAVSO P-5239-26) Department of Defense (DoD 5220.22-M)
Mode 4	Overwrite with random 1 byte numbers Overwrite with 0x00 Overwrite with 0xff	Army Regulations (AR380-19)
Mode 5	Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff	Former NSA Standard
Mode 6	Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 512 bytes of specified data	NASA Standard
Mode 7	Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0xaa	German Standard (VISTR)
Mode 8	Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0xaa Verified	US Air Force (AFSSI5020)

NETWORK SECURITY

User Authentication

User Authentication is a function that will protect unauthorized users from accessing the network or machine. This feature requires a User ID and a Password and can be configured to authenticate to the network or locally at the machine.

Network

Supported external servers like Active Directory, Novell NDS, NTML v.1 and NTLM v.2. Up to 64 characters, maximum, can be utilized. Active Directory can support up to 20 Domains.

Machine

Internal authentication at the machine can support up to 1000 user accounts. Passwords can be up to 8 alphanumeric characters.

Virus Protection

Konica Minolta MFPs contain an embedded operating system called VxWorks, which is far less susceptible to attack by viruses or worms that target traditional applications, and their OS Services because it provides a very small base “common” functionality. The viruses do not affect it, and worms typically found on the networks and the Internet are not written for the VxWorks platform. In practice, this makes it extremely difficult for an attacker to write a virus targeted at generic VxWorks implementations.

Password Protection

Passwords can be created for administrators and users and can be up alphanumeric up to 8 characters. An administrator can maintain passwords. Passwords are protected by the Kerberos system or SSL.

Allow/Prohibit Functions by User

An advanced level of user security allows or prohibits the use and availability of specific machine features. A user and/or administrator can control these features as needed throughout an organization or any size. The specific features affected are:

- Scanning from the bizhub as a walk up function or a remote function.
- User Box from the bizhub as a walk up function or a remote function.
- Copying from the bizhub as a walk up function where there can be a restriction of just B&W copying or just Color copying or neither B&W nor Color copying.
- Faxing from the bizhub as a walk up function or a remote function.
- Printing as a remote function, via the Print Driver, where there can be a restriction to allow just B&W printing but not color printing or vice versa.

Network Vulnerabilities

- Open Ports and Protocols can be opened, closed or enabled and disabled through the Administration Mode at the machine or remotely via PageScope Web Connection or PageScope Net Care.
- The Following ports can be opened or closed.

Port 20 – FTP	Port 123 – NTP	Port 110 – POP3
Port 21 – FTP	Port 161 – SNMP	Port 636 – LDAP for TLS/SSL
Port 25 – SMTP	Port 389 – LDAP	Port 9100 – PDL
Port 80 – HTTP	Port 631 – IPP	

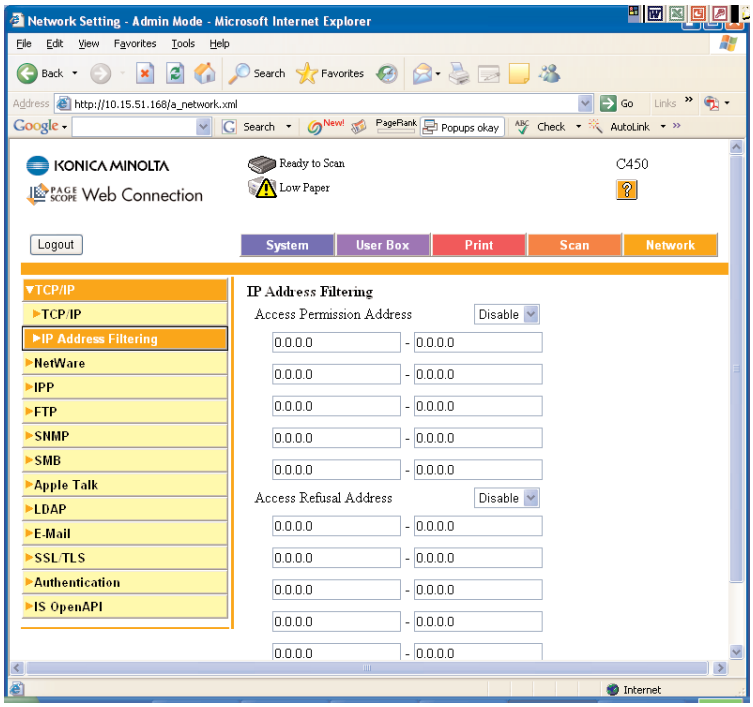
- The Following protocols can be enabled or disabled

  SNMP, SMB, POP, FTP, SMTP, IPP, Telnet, LDAP, HTTP

- IP Address Filtering can be set at the machine where the network interface card of the MFP can be programmed to prohibit access to the device by specific IP address ranges of client PCs (Figure 3).

Figure 3 illustrates PageScope Web Connection's Administrator access into a bizhub C450. Here an administrator can allow access permission or refusal of a specific IP address ranges.

Figure 3



FILE TRANSMISSION SECURITY

Confidential Print

There are two ways to send a print to the bizhub MFP that will be held until the sender releases it at the bizhub control panel.

Secure Print (Lock Job)

Secure print is supported on all models. The standard hard drive is required for the bizhub color products. The optional Hard Drive is required on monochrome bizhub OP products (420, 500, 600, 750). The user inputs the secure password (up to 8 alphanumeric characters) in the driver and inputs the same password at the MFPs panel. The machine verifies the password and releases the secure document. The password connected to the confidential print job is encrypted. The system can be set to delete all unopened secure print jobs after a designated time period.

Secure Mailbox Print

A print job will be stored in the Secure Print User Box where a User ID and Password will have to be entered for that print job to be accessed for printing or forwarding via fax or email. The User ID consists of a maximum 8 or 16 character ID (depending on the machine) AND an 8 character Password. The Print can only be accessed when both the User ID and Password are entered correctly.

Scan/PDF Encryption

The User has the ability to encrypt a scanned file by selecting the Encryption key on the bizhub's control panel (figure 4). The encryption option supports the PDF file type and will require the receiver of the scan to have the decryption code to open the file. This feature is very similar to the Adobe Acrobat encryption process where a password is utilized for encryption and opening a file, as well as for accessing the permissions area of the encryption configuration.

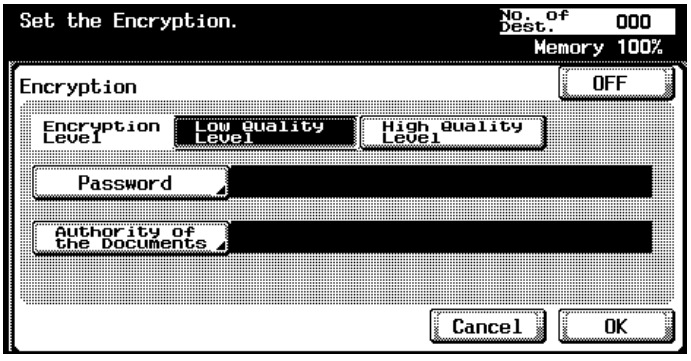


Figure 4.

Copy Protection (bizhub C352/C300/C250 only)
A concealed Security Watermark is placed on the original document being printed. The Security Watermark can consist of several phrases and/or patterns. When this document is copied by ANY other MFP the Security Watermark will appear notifying anyone who reads this newly copied document that it has been copied and/or distributed without authorization.

Advanced Email Security

- LDAP Search supports up to five LDAP Servers and LDAP Referral Function (Global LDAP) is supported.
- SMTP Authentication (Simple Mail Transfer Protocol), when enabled this will authorize a machine to send email. For those customers who do not host their email services the use of an ISP mail server can be utilized and supported by the machine. SMTP authentication is required by AOL and in the prevention of SPAM.
- POP3 before SMTP
- APOP Authentication
- Restriction from altering the 'From' address. When User Authentication is enabled and the 'Changing From Address' function is enabled the, 'from address of a scan-to-email job will always be the logged-in user's email address. This feature allows the machine to prevent spoofing and provide audit trails for administrators.
- Restriction of 'Manual Destination Input' will prohibit the ad hoc 'Direct Input' of an email address or any scan destination.

Advanced Fax Line Security

- Communication via the bizhub's fax connection uses **only** the fax protocol. It does not support any other communication protocols. Konica Minolta products block any intrusion attempts as threats. This would include intrusions of a different protocol over public telephone lines as well as transmitted data that cannot be decompressed as fax data.
- Routing Incoming Faxes, any incoming fax can be routed to any destination within the bizhub's internal Address Book. This would include; email address, FTP server, SMB folder and the User Box via the machine's HDD.
- Storing Incoming Faxes to Memory RX User Box. Instead of routing a fax to an email address or desktop, a user can store the incoming faxes to the Memory RX User Box. A user via Konica Minolta's Box Operator application can preview faxes stored in this manner. A user or administrator can pick and choose which faxes to print or not to print.

Fundamentals of Security

KONICA MINOLTA SECURITY LAYERS

Option or Feature		Security Layer
PageScope Web Connection		SSL
PageScope Box Operator		SSL
PageScope Data Administrator		SSL
Active Directory		Kerberos
Novell NDS		Novell
NT 4.0 Domain (SMB)		NTLM V.1, NTLM V.2
LDAP Server		SSL
Via a workstation	Secure Print PW	Encrypted
	Authentication PW	Encrypted

KONICA MINOLTA USER ID AND PASSWORD SECURITY

Function	User ID and/ or Password	Maximum Characters	Minimum Characters
User Authentication	User ID	64	1
User Password	32 or 64*	None	
Account Track	Account Name	8	1
Password	8	None	
Secure Print	ID	8 or 16*	1
Password	8	None	
User Box	Password	8	None
Memory RX	Password	8*	1*
Confidential RX	Password	8*	1*
Password	20 # digits*	None*	

* depending on specific Konica Minolta Model

ACCESS HISTORY

Account Tracking

Account tracking can be monitored at the User level, Group level and/or the departmental level. Monochrome and color copies, Scans, Faxes, Pure Black and Color printing can all be tracked locally at the machine or remotely via Konica Minolta software like PageScope Web Connection or PageScope Net Care.

Audit and Job Logs

- Audits and job logs can be reviewed for the following machine functions;
- Black & White and Color Prints
- Incoming and out-going faxes
- Scanning
- Black & White and Color Printing

Summary

Konica Minolta has invested a tremendous amount of engineering resources developing security related features for bizhub MFPs. Konica Minolta's forward thinking development processes provide our customers with the technology required in today's security conscious environments. Whether a customer is concerned about network intrusion, data theft or compliance, Konica Minolta bizhub technology can offer our customers a sense of security demanded by internal clients or federal legislation.

In summary, the following important points should be remembered:

- Konica Minolta uses a security consultant to evaluate the technology
- Konica Minolta certifies the entire system for ISO 15408 (Common Criteria) compliance
- Konica Minolta can help a health related facility satisfy HIPAA technical requirements
- There is no HIPAA certification for a device or product
- Konica Minolta can help a finance related facility satisfy Sarbanes-Oxley (SOX) technical requirements

HIPAA Security Final Rule — Appendix A to Subpart C of Part 164 — Security Standards: Matrix

§ 164.306 Security standards: General rules.

(a) General requirements. Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach.

(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) Standards. A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312,

§ 164.314, and § 164.316 with respect to all electronic protected health information.

(d) Implementation specifications. In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word ''Required'' appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word ''Addressable'' appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.

(1) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must —

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

(ii) As applicable to the entity—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate —

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) Maintenance. Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.

§ 164.308 Administrative safeguards.

(a) A covered entity must, in accordance with § 164.306:

(1) (i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

(3) (i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) Implementation specifications:

(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4) (i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) Implementation specifications:

(A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5) (i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

(ii) Implementation specifications. Implement:

(A) Security reminders (Addressable). Periodic security updates.

(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6) (i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.

(ii) Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

(7) (i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) Standard: Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

(b)(1) Standard: Business associate contracts and other arrangements. A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory

assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

(2) This standard does not apply with respect to —

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)©, when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)© are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

(4) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

§ 164.310 Physical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) Implementation specifications:

(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d) (1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) Implementation specifications:

(i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§ 164.312 Technical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/ or number for identifying and tracking user identity.

(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c) (1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) Implementation specifications:

(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(i) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Glossary of Security Terms and Acronyms

Shown below are terms and acronyms frequently used in discussions about Common Criteria and IT Security.

A

Accreditation Body An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Accredited Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

AES Advanced Encryption Standard. In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It is expected to be used worldwide and analysed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) in November 26, 2001 after a 5-year standardization process (see Advanced Encryption Standard process for more details). It became effective as a standard May 26, 2002. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography

Anti-Virus An Anti-Virus application provides protection against viruses coming into the workstation from network connections and/or removable media, and is considered sufficient protection for environments where the likelihood of an attempted compromise is low.

AOL America On Line

Approval Policy A part of the essential documentation of the Common Criteria Evaluation and Validation Scheme, setting out the procedures for making an application to be approved as a CCTL and placed on the NIAP Approved Laboratories List and for the processing of such applications and of the requirements which an applicant must fulfill in order to qualify.

Approved Lab List The list of approved CCTLs authorized by the NIAP Validation Body to conduct IT security evaluations within the Common Criteria Evaluation and Validation Scheme.

Approved Test Method List The list of approved test methods maintained by the NIAP Validation Body which can be selected by a CCTL in choosing its scope of accreditation, i.e., the types of IT security evaluations that it will be authorized to conduct using NIAP-approved test methods.

APOP Authenticated post Office Protocol

B

Biometrics Provide stronger user authentication to facilities or workstations by adding the "something you are" to the "something you know or have" protection of passwords/tokens. The Biometric capability may involve fingerprints, whole hand geometry, facial recognition, or retina scanning devices.

C

CC Common Criteria. The Common Criteria (CC) is an international standard (ISO/IEC 15408) for computer security. Unlike standards such as FIPS 140, Common Criteria does not provide a list of product security requirements or features that products must contain. Instead, it describes a framework in which computer system users can specify their security requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

CC Certificate A brief public document issued by the NIAP Validation Body under the authority of NIST and NSA which confirms that an IT product or protection profile has successfully completed evaluation by a CCTL. A Common Criteria certificate always has associated with it, a validation report.

CCEVS Common Criteria Evaluation and Validation Scheme

CCRA Common Criteria Recognition Arrangement

CCTL Common Criteria Testing Laboratory

CEM Common Evaluation Methodology

Certificate Management Technology used to manage the ordering, generation, distribution, and compromise recovery of public key certificates for users of cryptographic systems.

Glossary of Security Terms and Acronyms

Common Access Card The Common Access Card (CAC) is a United States Department of Defense (DoD) smartcard issued to standard identification for active duty military personnel, selected reserve personnel, civilian employees, and eligible contractor personnel. The CAC is used as a general identification card as well as for authentication to enable access to DoD computers, networks, and certain DoD facilities. The CAC enables encrypting and crytographically signing email, facilitating the use of PKI authentication tools, and establishes an authoritative process for the use of identity credentials.

Common Criteria Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Criteria Evaluation and Validation Scheme The program developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP) establishing an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles.

Common Criteria Testing Laboratory Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.

Common Evaluation Methodology Common Methodology for Information Technology Security Evaluations - a technical document that describes a set of IT security evaluation methods.

Confidentiality The prevention of unauthorized disclosure of information.

D

Database Management System (DBMS) A trusted software system that facilitates the creation and maintenance of a database or databases, and the execution of computer programs using the database or databases. A Database is defined as a set of data that is required for a specific purpose or is fundamental to a system, project, or enterprise.

Denial of Service attack In computer security, a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers where the attack is aiming to cause the hosted web pages to be unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB).

DES The Data Encryption Standard (DES) is a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. The algorithm was initially controversial, with classified design elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor. DES consequently came under intense academic scrutiny, and motivated the modern understanding of block ciphers and their cryptanalysis.

E

EAL Evaluation Assurance Level

EAP Evaluation Acceptance Package

ETR Evaluation Technical Report

ePHI Electronic Personal Health Information

Encryption In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge. While encryption has been used to protect communications for centuries, only organizations and individuals with an extraordinary need for secrecy had made use of it. In the mid-1970s, strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now employed in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines.

Evaluation The assessment of an IT product against the Common Criteria using the Common Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

Evaluation Acceptance Package A set of documentation from the CCTL consisting of a complete security target for the Target of Evaluation (TOE) and a complete evaluation work plan detailing the inputs, actions and timelines for the conduct of the evaluation; and the identification of points of contact for both the CCTL and the sponsor of the evaluation.

Evaluation Technical Report A report giving the details of the findings of an evaluation, submitted by the CCTL to the CCEVS Validation Body as the principal basis for the validation report.

Evaluation Work Plan A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

F

FIPS Federal Information processing Standard. The Federal Information Processing Standard 140 (FIPS) are series of publications numbered 140, which are a U.S. government computer security standards that specify requirements for cryptography modules.

FTP File Transfer Protocol

Firewall Deployed at enclave boundaries or on local hosts/servers to control access and restrict vulnerable services in support of an organization's security policy.

H

HDD Hard Disk Drive

HIPAA Health Insurance Portability and Accountability Act

HR Human Resources Department

http HyperText Transfer Protocol

https HyperText Transfer Protocol - https is not a separate protocol, but refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) transport mechanism

G

Guards Used to protect connections from a classified network. Analogous to high assurance firewalls, but with additional protection against leakage of high side data.

I

IEC International Electro-technical Commission

IPP Internet Printing Protocol

ISO International Organization for Standards

IT Information Technology

Integrity The prevention of unauthorized modification of information.

Intrusion Detection System/Intrusion Prevention System Devices generally deployed on networks or user hosts to monitor traffic and look for evidence of unauthorized intrusions or network attacks.

K

Kerberos Protocol Kerberos is a computer network authentication protocol which allows individuals communicating over an insecure network to prove their identity to one another in a secure manner. Kerberos prevents eavesdropping or replay attacks, and ensures the integrity of the data. Its designers aimed primarily at a client-server model, and it provides mutual authentication — both the user and the server verify each other's identity

Key (cryptography) A key is a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions (also known as MACs), often used for authentication.

L

LDAP Lightweight Directory Access Protocol

M

MFD Multi Function Device

MR Memorandum of Record

MSR Monthly Summary Report

Mobile Code Technology that enforces security policy restrictions on mobile code. These restrictions may be implemented within boundary protection solutions or may be enforced on user hosts or servers.

N

NIAP National Information Assurance Partnership. The National Information Assurance Partnership (NIAP) is a United States government initiative to meet the security testing needs of both information technology consumers and producers which is operated by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST).

NIAP Validation Body A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the CCEVS.

NIST National Institute of Standards and Technology. The National Institute of Standards and Technology (NIST, formerly known as The National Bureau of Standards) is a non-regulatory agency of the United States Department of Commerce's Technology Administration. The institute's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

Glossary of Security Terms and Acronyms

NSA The National Security Agency/Central Security Service (NSA/CSS) is the United States's cryptologic organization. Officially established on November 4, 1952, it is believed to be the largest U.S. government intelligence gathering agency. Responsible for the collection and analysis of foreign communications, it coordinates, directs, and performs highly specialized activities to produce foreign signals intelligence information, which involves a significant amount of cryptanalysis. It is also responsible for protecting U.S. government communications from similar agencies elsewhere, which involves a significant amount of cryptography.

A component of the Department of Defense, the NSA has always been directed by a three-star flag or general officer. NSA is a key component of the United States Intelligence Community headed by the Director of National Intelligence.

NVLAP National Voluntary Laboratory Accreditation Program the U.S. accreditation authority for CCTLs operating within the NIAP CCEVS.

NV-RAM Non-Volatile RAM

Network Management Technology that helps to protect networks against malicious attacks that might deny access or use of the network. For example, the technology used to control access to network management centers and to protect network management transactions from various kinds of attacks.

O

OD Observation Decision

ODRB Observation Decision Review Board

OR Observation Report

Observation Decision A response to an Observation Report (OR). The observation decision (OD) is the formal documented response from the Validation Body that provides clarification/guidance to the CCTL on a submitted OR.

Observation Report A report issued to the NIAP Validation Body by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

Operating System Operating systems, which offer security mechanisms such as authentication, access control, data separation, and auditing to enforce security policies, set by the system administrators or users.

P

Peripheral Switch A trusted electronic or physical device that allows a user to share a single peripheral (e.g. a monitor or keyboard) across two workstations operating on different system high networks. The switch must prevent leakage or sharing of data across the two networks.

PIN Personal Identification Number

POP Post Office Protocol

Protection Profile An implementation independent set of security requirements for a category of IT products, which meet specific consumer needs.

Public Key Infrastructure (PKI)/Key Management Infrastructure Refers to the collection of technologies, facilities, people and processes used to manage the provisioning of public key and traditional key management services to users of cryptographic products.

R

RAM Random Access Memory

RX Abbreviation for Receive

S

SEC Securities and Exchange Commission

SF Security Function

SFR Security Functional Requirement

SMB Server Message Block

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

SNMP v3 SNMP Version 3 (SNMPv3) adds security and remote configuration capabilities to the previous versions. The SNMPv3 architecture introduces the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. The architecture supports the concurrent use of different security, access control, and message processing models.

SOX The Sarbanes–Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX or SarBox; July 30, 2002) is a United States federal law passed in response to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, and WorldCom (now MCI).

SPAM Slang for unsolicited commercial, junk or bulk Email

SSL Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are cryptographic protocols which provide secure communications on the Internet for such things as web browsing, Email, Internet faxing, and other data transfers.

SSL provides endpoint authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; mutual authentication requires public key infrastructure (PKI) deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery.

Secure Messaging Messaging applications that offer authentication, signature, and encryption mechanisms to provide privacy and integrity for user data. These services are usually enabled by the use of public keying techniques.

Security Management Security management is a set of pervasive security mechanisms, which support the security services by direct and supervisory administration, automated processes, and by the activities of all information users.

Security Target (ST) A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the CC. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Sensitive Data Protection The implementation of administrative, technical, or physical measures to guard against the unauthorized access to data.

Single Level Web Server Web servers that provide access control, audit, and authentication and data encryption services appropriate for use on system high networks.

Smart Cards Small user tokens generally used to securely store user authentication credentials (e.g. the private portion of public key material) and to control access and use of these credentials.

Sponsor The person or organization that requests a security evaluation of an IT product or protection profile.

Spoofing Attack In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage.

System Access Control A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device. Limiting access to information system resources only to authorized users, programs, processes, or other systems.

T

TOE Target of Evaluation - An IT product or group of IT products configured as an IT System and associated documentation that is the subject of a security evaluation under the CC. Also, a protection profile that is the subject of a security evaluation under the CC.

TX Abbreviation for Transmit

Test Method An evaluation assurance package from the CC, the associated evaluation methodology for that assurance package from the CEM, and any technology-specific derived testing requirements.

V

VPL A publicly available document issued periodically by the NIAP Validation Body giving brief particulars of every IT product or protection profile which holds a currently valid CC certificate awarded by that body and every product or profile validated or certified under the authority of another Party for which the certificate has been recognized.

Validation The process carried out by the NIAP Validation Body leading to the issue of a CC certificate.

Validation Report A publicly available document issued by the NIAP Validation Body which summarizes the results of an evaluation and confirms the overall results, (i.e., that the evaluation has been properly carried out, that the CC, the Common Evaluation Methodology, and scheme-specific procedures have been correctly applied; and that the conclusions of the Evaluation Technical Report are consistent with the evidence adduced).

Glossary of Security Terms and Acronyms

Virtual Private Network (VPN) A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. The idea of the VPN is to ensure that the right people can access your network resources.

VxWorks VxWorks is a Unix-like real-time operating system made and sold by Wind River Systems of Alameda, California, USA.

Like most RTOSes, VxWorks includes a multitasking kernel with pre-emptive scheduling and fast interrupt response, extensive inter-process communications and synchronization facilities, and a file system. Newer versions of VxWorks now support pSOS system calls since Wind River now owns both RTOSes.

Major distinguishing features of VxWorks include efficient POSIX-compliant memory management, multiprocessor facilities, a shell for user interface, symbolic and source level debugging capabilities, and performance monitoring.

VxWorks is generally used in embedded systems. Unlike "native" systems such as UNIX and Forth, VxWorks development is done on a "host" machine running UNIX or Windows, cross-compiling target software to run on various "target" CPU architectures as well as on the "host" by means of VxSim.

W

Wireless LAN (WLAN) WLANs provide wireless network communication over short distances using radio signals instead of traditional network cabling. A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access system, to the edge of the wired network. Clients communicate with the access system using a wireless network adapter similar in function to a traditional Ethernet adapter.

Notes

Notes

Notes

bizhub

Office imagery courtesy of Knoll, Inc.

Design & specifications are subject to change without notice. NOTE: Some of the specific security features and options described in this White Paper may only apply to certain Konica Minolta bizhub products. It is best to refer to the documentation that is provided with every bizhub product to verify exactly which security features are included with a specific bizhub product. It is also important to note that a specific bizhub product may require an upgrade to achieve and/or enable some of the features discussed in this White Paper. Please refer to your Konica Minolta Service Representative for further information.

KONICA MINOLTA

KONICA MINOLTA
BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive
Ramsey, NJ 07446
www.kmbs.konicaminolta.us