HDD Data Security

KONICA MINOLTA

bizhub Security:
Hard Disk Drive Data Protection

bizhub Office/Workgroup Product Reference Guide

COUNT ON KONICA MINOLTA

Disclaimer

This guide is intended solely for the use and information of Konica Minolta Business Solutions USA, Konica Minolta subsidiaries and distributors, and their employees. The information herein was obtained from various 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.

Introduction

Konica Minolta Security Standards

Konica Minolta realized early on the importance of security issues in the digital age, where the risk of seriously damaging security breaches rises dramatically alongside rapidly growing worldwide communication possibilities.

In response to these threats, Konica Minolta has taken a leading role in developing and implementing security-based information technology in our multifunctional products. Ever since the introduction of the first Konica Minolta MFP, Konica Minolta has strived to develop and implement technology that safeguards the confidentiality of electronic documents.

The most important IT based security standard in the world is ISO 15408, also known as Common Criteria certification. Konica Minolta has newly introduced multifunctional bizhub products validated to Common Criteria EAL3 security standards. Common Criteria (CC) is the only internationally recognized standard for IT security testing. Printers, copiers and software with the ISO 15408 certification are security evaluated, and guarantee the security levels that companies look for today. With the CC certification users can rest assured that on Konica Minolta’s multifunctional devices their confidential data remain confidential.

The Konica Minolta security standards provide protection in more than one respect, securing the network and network access, ensuring secure, authorized access to individual output devices, restricting functionalities where required, and protecting all personal user data and information content processed on the bizhub output systems.

Konica Minolta takes the security concerns of its customers seriously. This is why almost all of Konica Minolta’s comprehensive security functionality is standard on the new-generation bizhub systems. After all, users should not have to pay for capabilities that are an essential requirement for protecting customers’ sensitive information in the digital age!

This document specifically discusses the various Konica Minolta products that utilize a Hard Disk Drive within the MFP, the potential temporary or long term data stored on these drives and the built in methods of protecting and/or deleting the stored data.

HDD Best Practices

Konica Minolta Recommended HDD Best Practices

Konica Minolta bizhub MFP's offer standard, effective data protection from unauthorized access using features like HDD Encryption, HDD Lock Password, Overwrite Temporary Data, Overwrite All Data and automated box data deletion. Konica Minolta highly recommends enabling these features and functions in order to properly protect a customer's sensitive data.

HDD Encryption
The bizhub uses a standard AES 128 bit encryption algorithm to secure the entire HDD and all of its contents.

HDD Lock Password
By applying a 20 character password to the BIOS of the HDD the HDD is now protected from unauthorized access whether the drive is moved to another MFP or removed entirely.

Overwrite Temporary Data
Enabling this feature will allow for automatic deletion of all copy, print, scan and fax data immediately after the job has completed.

Overwrite All Data
At the end of life or if an MFP is moved from a secure area to a non secure area this feature will wipe or scrub **all** existing data on the HDD and reset the drive back to factory default.

Automated Box Data Deletion
The various boxes created and utilized on a bizhub MFP can be set to automatically delete any information inside the box by the MFP administrator. Boxes like User Box, Secure Print, Encrypted PDF, etc.

What's Next…

The following pages will assist in determining which Konica Minolta product utilize a hard disk drive or other non-volatile storage, what is stored on those HDD's and which security features and functions are available for securing these drives.

Konica Minolta highly recommends that each customer assess and determine their own security needs and risks before enabling the bizhub security features and functions at the Multi Function Printer (MFP).

Konica Minolta provides a Security User Manual for each bizhub model. These manuals will provide a Security Checklist, insight into each security feature/function and a step-by-step procedure to enable each feature/function.

Konica Minolta also provides Technical and Professional Services to assistance and consulting. Please contact your local Konica Minolta sales representative for more information or visit our website at http://kmbs.konicaminolta.us/content/products/subcategories/as_security.html

bizhub Model Name

bizhub C652
bizhub C652DS
bizhub C552
bizhub C552DS
bizhub C452
bizhub C452DS
bizhub C360
bizhub C280
bizhub C220

bizhub 423
bizhub 363
bizhub 283*
bizhub 223*

* HDD Optional

Explanation of Stored HDD Data and the data that is wiped from HDD

User registration data

- Deletes all user-related data that has been registered

Box registration data/file

- Deletes all User Box-related information and files saved in User Box

Secure Print ID/Password/Document

- Deletes all Secure Print Document-related information and files saved

ID & Print file

- Deletes all ID & Print files saved in ID & Print User Box

Image files:

• Image files saved other than Secure Print Documents, ID & Print files and User Box files
• Image files of jobs in job queue state
• Data files left in the data space used as image files
• Temporary data files generated during print image file processing

Destination recipient data files

- Deletes all destination recipient data including e-mail addresses and telephone numbers

Encryption Key

- Clears the currently set Encryption Key

Administrator Password

- Clears the currently set password, resetting it to the factory setting

SNMP Password

- Clears the currently set password, resetting it to the factory setting (MAC address)

WebDAV Server Password

- Clears the currently set password, resetting it to the factory setting (sysadm)

Account registration data

- Deletes all account track-related data that has been registered

S/MIME certificate data

- Deletes the currently set S/MIME certificate

SSL certificate

- Deletes the currently set SSL certificate

Network Setting

- Clears the currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting), resetting it to the factory setting

Option License Keys

Optional Loadable Drivers

bizhub Security Features

250 GB	S	HDD Capacity
Yes	S	HDD Encryption Key
Yes	S	HDD Lock Password
Yes	S	Temporary Data Overwrite
Yes	S	All Data Overwrite

S = Standard Accessory / O = Optional Accessory

These models utilize a standard Hard Disk Drive for temporary or long term image storage.

These models can encrypt the entire HDD using the standard Encryption Key feature. The data stored on the MFP HDD is encrypted using AES 128-bit key size. Once a HDD is encrypted its data cannot be read, even if the HDD is removed from the MFP.

Temporary Data Overwrite can be enabled after each MFP function Print, Scan, Copy and Fax. Depending on the job file size temporarily swapped data might be stored on the HDD. This data is immediately deleted and overwritten as soon as the data is no longer necessary to end the job in action.

- Overwrite modes are 1 time to US Navy/DoD standard or 3 times to US AirForce standard.

Overwrite All Data can be enabled when the machine is to be discarded, or is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved back to factory settings. The HDD Overwrite Method offers the choice of eight different modes, corresponding with 8 specific Government approved standards.

HDD Lock Password is a standard security feature. When enabled the MFP hard disk is automatically protected by a password. This 20 character password is stored in the hard disk BIOS and prevents access to the hard disk data.

<table>
<tr><th>bizhub Model Name</th><th>Explanation of Stored HDD Data and the data that is wiped from HDD</th><th>bizhub Security Features</th></tr>
<tr>
<td>bizhub C650
bizhub C550
bizhub C451

bizhub C353
bizhub C353P
bizhub C253
bizhub C201

bizhub 8650</td>
<td><b>User registration data</b>
• Deletes all user-related data that has been registered
<b>Box registration data/file</b>
• Deletes all User Box-related information and files saved in User Box
<b>Secure Print ID/Password/Document</b>
• Deletes all Secure Print Document-related information and files saved
<b>ID & Print file</b>
• Deletes all ID & Print files saved in ID & Print User Box
<b>Image files:</b>
• Image files saved other than Secure Print Documents, ID & Print files and User Box files
• Image files of jobs in job queue state
• Data files left in the data space used as image files
• Temporary data files generated during print image file processing

<b>Destination recipient data files</b>
• Deletes all destination recipient data including e-mail addresses and telephone numbers
<b>Encryption Key</b>
• Clears the currently set Encryption Key
<b>Administrator Password</b>
• Clears the currently set password, resetting it to the factory setting
<b>SNMP Password</b>
• Clears the currently set password, resetting it to the factory setting (MAC address)
<b>WebDAV Server Password</b>
• Clears the currently set password, resetting it to the factory setting (sysadm)
<b>Account registration data</b>
• Deletes all account track-related data that has been registered
<b>S/MIME certificate data</b>
• Deletes the currently set S/MIME certificate
<b>SSL certificate</b>
• Deletes the currently set SSL certificate
<b>Network Setting</b>
• Clears the currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting), resetting it to the factory setting

<b>HDD Lock Password</b>
• Deletes the current HDD Password

<b>Option License Keys</b>

<b>Optional Loadable Drivers</b></td>
<td><table>
<tr><td>60 GB</td><td>S</td><td>HDD Capacity</td></tr>
<tr><td>Yes</td><td>O</td><td>HDD Encryption Key</td></tr>
<tr><td>Yes</td><td>S</td><td>HDD Lock Password</td></tr>
<tr><td>Yes</td><td>S</td><td>Temporary Data Overwrite</td></tr>
<tr><td>Yes</td><td>S</td><td>All Data Overwrite</td></tr>
<tr><td colspan="3"><i>S = Standard Accessory / O = Optional Accessory</i></td></tr>
</table>
These models utilize a standard Hard Disk Drive for temporary or long term image storage.

These models can encrypt the entire HDD using the standard Encryption Key feature. The data stored on the MFP HDD is encrypted using AES 128-bit key size. Once a HDD is encrypted its data cannot be read, even if the HDD is removed from the MFP.

Temporary Data Overwrite can be enabled after each MFP function Print, Scan, Copy and Fax. Depending on the job file size temporarily swapped data might be stored on the HDD. This data is immediately deleted and overwritten as soon as the data is no longer necessary to end the job in action.
• Overwrite modes are 1 time to US Navy/DoD standard or 3 times to US AirForce standard.

Overwrite All Data can be enabled when the machine is to be discarded, or is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved back to factory settings. The HDD Overwrite Method offers the choice of eight different modes, corresponding with 8 specific Government approved standards.

HDD Lock Password is a standard security feature. When enabled the MFP hard disk is automatically protected by a password. This 20 character password is stored in the hard disk BIOS and prevents access to the hard disk data.</td>
</tr>
</table>

bizhub Model Name	Explanation of Stored HDD Data and the data that is wiped from HDD	bizhub Security Features		
bizhub C450 bizhub C450P bizhub C352 bizhub C352P bizhub C351 bizhub C300 bizhub C252 bizhub C252P bizhub C250 bizhub C250P	**User registration data** • Deletes all user-related data that has been registered **Box registration data/file** • Deletes all User Box-related information and files saved in User Box **Secure Print ID/Password/Document** • Deletes all Secure Print Document-related information and files saved **Image files:** • Image files saved other than Secure Print Documents and User Box files • Image files of jobs in job queue state **Destination recipient data files** • Deletes all destination recipient data including e-mail addresses and telephone numbers **Encryption Key** • Clears the currently set Encryption Key **Administrator Password** • Clears the currently set password, resetting it to the factory setting **SNMP Password** • Clears the currently set password, resetting it to the factory setting (MAC address) **Network Setting** • Clears the currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting), resetting it to the factory setting **HDD Lock Password** • Deletes the current HDD Password	40 GB	S	HDD Capacity
		Yes	O	HDD Encryption Key
		Yes	S	HDD Lock Password
		Yes	S	Temporary Data Overwrite
		Yes	S	All Data Overwrite
		S = Standard Accessory / O = Optional Accessory		
		These models utilize a standard Hard Disk Drive for temporary or long term image storage. These models can encrypt the entire HDD using the standard Encryption Key feature. The data stored on the MFP HDD is encrypted using AES 128-bit key size. Once a HDD is encrypted its data cannot be read, even if the HDD is removed from the MFP. Temporary Data Overwrite can be enabled after each MFP function Print, Scan, Copy and Fax. Depending on the job file size temporarily swapped data might be stored on the HDD. This data is immediately deleted and overwritten as soon as the data is no longer necessary to end the job in action. • Overwrite modes are 1 time to US Navy/DoD standard or 3 times to US AirForce standard. Overwrite All Data can be enabled when the machine is to be discarded, or is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved back to factory settings. The HDD Overwrite Method offers the choice of eight different modes, corresponding with 8 specific Government approved standards. HDD Lock Password is a standard security feature. When enabled the MFP hard disk is automatically protected by a password. This 20 character password is stored in the hard disk BIOS and prevents access to the hard disk data.		

<table>
<tr><th>bizhub Model Name</th><th>Explanation of Stored HDD Data and the data that is wiped from HDD</th><th>bizhub Security Features</th></tr>
<tr>
<td><b>bizhub 501</b>
<b>bizhub 421</b>
<b>bizhub 361</b>
*120GB HDD

<b>bizhub 500</b>
<b>bizhub 420</b>
<b>bizhub 360</b>
*40GB HDD</td>
<td><b>User registration data</b>
• Deletes all user-related data that has been registered
<b>Box registration data/file</b>
• Deletes all User Box-related information and files saved in User Box
<b>Secure Print ID/Password/Document</b>
• Deletes all Secure Print Document-related information and files saved
<b>ID &amp; Print file</b>
• Deletes all ID & Print files saved in ID & Print User Box
<b>Image files:</b>
• Image files saved other than Secure Print Documents, ID & Print files and User Box files
• Image files of jobs in job queue state

<b>Destination recipient data files</b>
• Deletes all destination recipient data including e-mail addresses and telephone numbers
<b>Encryption Key</b>
• Clears the currently set Encryption Key
<b>Administrator Password</b>
• Clears the currently set password, resetting it to the factory setting
<b>SNMP Password</b>
• Clears the currently set password, resetting it to the factory setting (MAC address)
<b>WebDAV Server Password</b>
• Clears the currently set password, resetting it to the factory setting (sysadm)
<b>Account registration data</b>
• Deletes all account track-related data that has been registered
<b>S/MIME certificate data</b>
• Deletes the currently set S/MIME certificate
<b>SSL certificate</b>
• Deletes the currently set SSL certificate
<b>Network Setting</b>
• Clears the currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting), resetting it to the factory setting
<b>HDD Lock Password</b>
• Deletes the current HDD Password

<b>Option License Keys</b>

<b>Optional Loadable Drivers</b>

<b>Flash Memory Lock Password</b>
• Clears the currently set password</td>
<td>
<table>
<tr><td>40/120GB</td><td>O</td><td>HDD Capacity</td></tr>
<tr><td>Yes</td><td>O</td><td>HDD Encryption Key</td></tr>
<tr><td>Yes</td><td>S</td><td>HDD Lock Password</td></tr>
<tr><td>Yes</td><td>S</td><td>Temporary Data Overwrite</td></tr>
<tr><td>Yes</td><td>S</td><td>All Data Overwrite</td></tr>
<tr><td colspan="3"><i>S = Standard Accessory / O = Optional Accessory</i></td></tr>
</table>
These models utilize a optional Hard Disk Drive for temporary or long term image storage.

These models can encrypt the entire HDD using the standard Encryption Key feature. The data stored on the MFP HDD is encrypted using AES 128-bit key size. Once a HDD is encrypted its data cannot be read, even if the HDD is removed from the MFP.

Temporary Data Overwrite can be enabled after each MFP function Print, Scan, Copy and Fax. Depending on the job file size temporarily swapped data might be stored on the HDD. This data is immediately deleted and overwritten as soon as the data is no longer necessary to end the job in action.
• Overwrite modes are 1 time to US Navy/DoD standard or 3 times to US AirForce standard.

Overwrite All Data can be enabled when the machine is to be discarded, or is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved back to factory settings.
The HDD Overwrite Method offers the choice of eight different modes, corresponding with 8 specific Government approved standards.

HDD Lock Password is a standard security feature. When enabled the MFP hard disk is automatically protected by a password. This 20 character password is stored in the hard disk BIOS and prevents access to the hard disk data.
</td>
</tr>
</table>

<table>
<tr><th>bizhub Model Name</th><th>Explanation of Stored HDD Data and the data that is wiped from HDD</th><th>bizhub Security Features</th></tr>
<tr>
<td><b>bizhub 751</b>
<b>bizhub 601</b>
*80GB HDD

<b>bizhub 750</b>
<b>bizhub 600</b>
*40GB HDD</td>
<td><b>User registration data</b>
• Deletes all user-related data that has been registered
<b>Box registration data/file</b>
• Deletes all User Box-related information and files saved in User Box
<b>Secure Print ID/Password/Document</b>
• Deletes all Secure Print Document-related information and files saved
<b>ID &amp; Print file</b>
• Deletes all ID & Print files saved in ID & Print User Box
<b>Image files:</b>
• Image files saved other than Secure Print Documents, ID & Print files and User Box files
• Image files of jobs in job queue state

<b>Destination recipient data files</b>
• Deletes all destination recipient data including e-mail addresses and telephone numbers
<b>Encryption Key</b>
• Clears the currently set Encryption Key
<b>Administrator Password</b>
• Clears the currently set password, resetting it to the factory setting
<b>SNMP Password</b>
• Clears the currently set password, resetting it to the factory setting (MAC address)
<b>WebDAV Server Password</b>
• Clears the currently set password, resetting it to the factory setting (sysadm)
<b>Account registration data</b>
• Deletes all account track-related data that has been registered
<b>S/MIME certificate data</b>
• Deletes the currently set S/MIME certificate
<b>SSL certificate</b>
• Deletes the currently set SSL certificate
<b>Network Setting</b>
• Clears the currently set network settings (DNS Server setting, IP Address setting, SMTP Server setting, NetWare Setting, NetBIOS setting and AppleTalk Printer Name setting), resetting it to the factory setting
<b>HDD Lock Password</b>
• Deletes the current HDD Password

<b>Option License Keys</b>

<b>Optional Loadable Drivers</b>

<b>Flash Memory Lock Password</b>
• Clears the currently set password</td>
<td><table>
<tr><td>40/80GB</td><td>O</td><td>HDD Capacity</td></tr>
<tr><td>Yes</td><td>O</td><td>HDD Encryption Key</td></tr>
<tr><td>Yes</td><td>S</td><td>HDD Lock Password</td></tr>
<tr><td>Yes</td><td>S</td><td>Temporary Data Overwrite</td></tr>
<tr><td>Yes</td><td>S</td><td>All Data Overwrite</td></tr>
<tr><td colspan="3"><i>S = Standard Accessory / O = Optional Accessory</i></td></tr>
</table>
These models utilize a optional Hard Disk Drive for temporary or long term image storage.

These models can encrypt the entire HDD using the standard Encryption Key feature. The data stored on the MFP HDD is encrypted using AES 128-bit key size. Once a HDD is encrypted its data cannot be read, even if the HDD is removed from the MFP.

Temporary Data Overwrite can be enabled after each MFP function Print, Scan, Copy and Fax. Depending on the job file size temporarily swapped data might be stored on the HDD. This data is immediately deleted and overwritten as soon as the data is no longer necessary to end the job in action.
• Overwrite modes are 1 time to US Navy/DoD standard or 3 times to US AirForce standard.

Overwrite All Data can be enabled when the machine is to be discarded, or is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved back to factory settings.
The HDD Overwrite Method offers the choice of eight different modes, corresponding with 8 specific Government approved standards.

HDD Lock Password is a standard security feature. When enabled the MFP hard disk is automatically protected by a password. This 20 character password is stored in the hard disk BIOS and prevents access to the hard disk data.</td>
</tr>
</table>

<table>
<tr><th>bizhub Model Name</th><th>Explanation of Stored HDD Data and the data that is wiped from HDD</th><th colspan="3">bizhub Security Features</th></tr>
<tr><td rowspan="7">bizhub 362
bizhub 282
bizhub 222

bizhub 350
bizhub 250
bizhub 200</td><td rowspan="7">**Enhance Security function**
• Clears the current settings, resetting them to the default ones.

User Box Password/file
• Deletes the User Box Password and all files saved in the user box.

Swap data
• Deletes all swap data generated in a copy, PC print, or Secure Print Document that is too large in size to fit in the RAM space, representing part of the image files stored in the HDD.

Image files
• Deletes overlay image files and all image files stored in the HDD.

Destination recipient data files
• Deletes all destination recipient data including e-mail addresses and telephone numbers

HDD Lock Password
• Clears the currently set password.

Encryption Key
• Clears the currently set Encryption Key.

Administrator Code (Administrator Password)
• Clears the currently set password, resetting it to the factory setting</td><td>40 GB</td><td>O</td><td>HDD Capacity</td></tr>
<tr><td>Yes</td><td>O</td><td>HDD Encryption Key</td></tr>
<tr><td>Yes</td><td>S</td><td>HDD Lock Password</td></tr>
<tr><td>Yes</td><td>S</td><td>Temporary Data Overwrite</td></tr>
<tr><td>Yes</td><td>S</td><td>All Data Overwrite</td></tr>
<tr><td colspan="3">*S = Standard Accessory / O = Optional Accessory*</td></tr>
<tr><td colspan="3">These models utilize an optional Hard Disk Drive for temporary or long term image storage.

These models can encrypt the entire HDD using the standard Encryption Key feature. The data stored on the MFP HDD is encrypted using AES 128-bit key size. Once a HDD is encrypted its data cannot be read, even if the HDD is removed from the MFP.

Temporary Data Overwriting: Delete by overwriting data and temporary files that are saved in the HDD and memory, but that are no longer necessary. Overwrites with 0x00 → 0x00 → 0x00.

Overwrite All Data can be enabled when the machine is to be discarded, or is terminated at the end of the leasing contract, the Overwrite All Data function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved back to factory settings.
The HDD Overwrite Method offers one mode; Government approved - US Air Force (AFSSI5020).

HDD Lock Password is a standard security feature. When enabled the MFP hard disk is automatically protected by a password. This 20 character password is stored in the hard disk BIOS and prevents access to the hard disk data.</td></tr>
</table>

Konica Minolta
Business Solutions U.S.A., INC.
100 Williams Drive
Ramsey, NJ 07446
www.kmbs.konicaminolta.us
www.kmbs.konicaminolta.us/solutions