



KONICA MINOLTA

**Konica Minolta Business Solutions U.S.A., Inc.
magicolor 8650 Color Printer
Security Report**



Introduction

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.

The magicolor 8650 has EAL3 ISO 15408 Common Criteria Certification for the entire system.

HDD and RAM Security

Data theft is the leading concern by end-users, corporations/business' and manufacturers alike. One particular fear is that critical data can be stolen from the printer Hard Drive (HDD) or RAM, either by accessing the PRINTER or removing the HDD or RAM and extracting the data after the PRINTER 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 magicolor printers:

- 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 is 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 module 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 Konica Minolta products were sent for ISO 15408 certification. There are no indirect routes or security holes.

Non-Volatile RAM (NV_RAM)

Typically Non-Volatile RAM would be:

- Counter Data
- Service Settings
- Utility Settings

The data written to Non-Volatile RAM is non-critical 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
- OP Panel Data
- Printer Resident Fonts
- Copy Protect Watermarks

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

HDD Security

The magicolor 8650 offers a standard 60 GB Hard Disk Drive. . The hard drive is protected from data theft by implementing the following security technologies. An Administrator can control the use of each of these functions individually or in combination:

- Job Overwrite (Temporary Data Overwrite)
- HDD Encryption
- HDD Lock Password

- HDD Overwrite or HDD Sanitizing

Automatic Job Overwrite (Temporary Data Overwrite)

The magicolor 8650 supports automatic erase of any temporary image data that might remain on the hard drive after a job is completed.

There are two Job Overwrite Modes to choose from:

Mode	Overwrite method	Compliance
Mode 1	Overwrite with 0x00	<ul style="list-style-type: none"> • U.S. Navy NAVSO P-5239-26 • Dept. of Defense DoD 5220.22-M
Mode 2	3 times overwrite: <ul style="list-style-type: none"> • Overwrite with 0x00 • Overwrite with 0xff • Overwrite with A (Dx61) • Verify 	U.S. 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

The magicolor 8650 hard drive supports factory equipped encryption. HDD data can be encrypted using the Advanced Encryption Standard (AES). Any files temporarily written or stored at rest are encrypted using the AES 128 bit encryption algorithm. Once a Hard Disk Drive is encrypted the data cannot be read even if the HDD is removed from the printer.

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.)

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

An HDD can be locked using a password of 20 alphanumeric characters. The data stored on this HDD is protected even if the HDD is removed from the printer and installed into a different printer or PC, the data cannot be read.

HDD Overwriting or HDD Sanitizing

At the time of disposal of a printer or with the replacement of a printer HDD, the entire HDD can be overwritten so that all of the data is completely removed. This can be achieved by using any of the 8 following modes and Overwrite Methods:

Mode	Overwrite method	Compliance
Mode 1	Overwrite with 0x00	<ul style="list-style-type: none">• Japan Electronic & Information Technology Association• Russian Standard (GOST)
Mode 2	<ul style="list-style-type: none">• Overwrite with random 1 byte numbers• Overwrite with random 1 byte numbers• Overwrite with 0x00	Current National Security Agency (NSA) standard
Mode 3	<ul style="list-style-type: none">• Overwrite with 0x00• Overwrite with 0xff• Overwrite with random 1-byte numbers• Verify	<ul style="list-style-type: none">• National Computer Security Center (NCSC-TG-025)• US Navy (NAVSO P-5239-26)• Department of Defense (DoD 5220.22-M)
Mode 4	<ul style="list-style-type: none">• Overwrite with random 1-byte numbers• Overwrite with 0x00• Overwrite with 0xff	Army Regulations (AR380-19)
Mode 5	<ul style="list-style-type: none">• Overwrite with 0x00• Overwrite with 0xff• Overwrite with 0x00• Overwrite with 0xff	Former NSA Standard
Mode 6	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Overwrite with 0x00 • Overwrite with 0xff • Overwrite with 0x00 • Overwrite with 0xff • Overwrite with 0x00 • Overwrite with 0xff • Overwrite with 0xaa • Verified 	U.S. Air Force (AFSSI5020)

This material is copyrighted by Konica Minolta Business Solutions U.S.A., Inc. and is the sole property of Konica Minolta Business Solutions U.S.A., Inc. Duplication of this proprietary report or excerpts from this report, in any manner, whether printed or electronic (including and not limited to, copying, faxing, scanning or use on a fax-back system), is illegal and strictly forbidden without written permission from Konica Minolta Business Solutions U.S.A., Inc. Violators will be prosecuted to the fullest extent of the law.

Konica Minolta Business Solutions U.S.A., Inc.

100 Williams Drive
 Ramsey, NJ 07446
www.CountOnKonicaMinolta.com