Digital Imaging Systems

Security Solution

- User Authentication
- Job Tracking
- Fax Transmission via RightFax® Server
- Secure Printing Functions
- HDD/Memory Security
- Fax to Ethernet Connection
- Data Security Kit

Panasonic ideas for life

Outline

How do you protect your critical confidential data?

Security issues in today’s business:

Security in today’s networked office

With the rapid popularization of local and wide area networks, the volume of data transmitted/received, edited, and stored in the modern office is growing ever larger. Unfortunately, as information becomes more valuable and as communication becomes more efficient, the threat posed by unauthorized access or inadvertent leakage of confidential data has also become far more serious.
In today’s environment, the need for enhanced security doesn’t apply only to computer networks and individual computers, it also applies to document processing equipment — such as printers, scanners and faxes — used in the office. All of these devices handle and process important data, so more effective ways of preventing security breaches are required.

How to protect data

Even when users recognize the importance of security, they may not know how to protect their data, or may find that maintaining security interferes with normal operations. Consequently, many users tend to ignore these problems.
Protecting individual data is difficult and complicated. For example, it is very difficult to keep track of every operation, such as who copied or printed what, when they did it, and where they sent it. To manage all of this efficiently is virtually impossible. Detecting unauthorized users can also be difficult if an approved user account and password are used to access internal data. This kind of “spoofing” has to be prevented if security is to be maintained.
Rather than address these issues, many office users tend to leave things as they are until an actual security breach occurs or someone complains about the lack of security. This is why Panasonic’s multi-functional units* are provided with a powerful set of standard security features.

* Refer to the applicable models.

Panasonic helps you plug your information leaks:

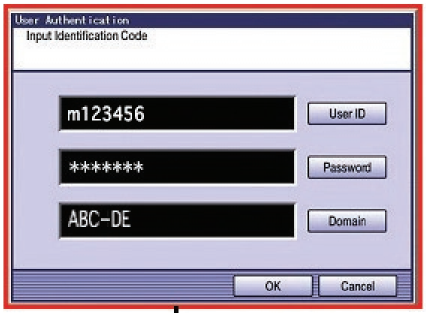
- **User Authentication**
  Job Tracking, Fax Transmission via RightFax® Server
- **Secure Printing Functions**
  Mailbox, Secure Mailbox
- **HDD/Memory Security**
  HDD Erasure (Job-by-job, Bulk)
  Image Memory Erasure
- **Data Security Kit**

User Authentication

How do you protect important data from being exposed to unauthorized users?

Preventing unauthorized access

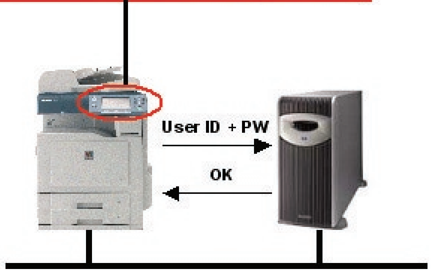
When copiers or MFPs are installed in an unmanned, “copy room”, it’s easy for unauthorized personnel or outside parties to use the equipment, increasing the likelihood that confidential data could be leaked using fax, internet fax or scan-to-email features.
To prevent unauthorized access to confidential business data, a User Authentication function that works with Windows® Active Directory database (Windows® 2000, Windows Server™ 2003) can be implemented. Users must be authenticated before they can use the machine (Copying, Faxing, Printing and/or Scanning).



User Authentication
Input Identification Code

m123456 User ID
******* Password
ABC-DE Domain

OK Cancel



Login procedure
(when using copier/fax/scanner)

When the User Authentication function is activated, users must enter their login name and password before they can use any device. Authentication is performed using the user’s Windows account.

1) User ID: Enter user name (up to 40 characters; not case-sensitive)
2) Password: Enter password (up to 40 characters; case-sensitive)
3) Domain: Selectable domain name available

Function-Independent Authentication

In addition to a universal setting, since User Authentication can be set independently for each function — Copying, Faxing, Printing and Scanning, you can use your MFP unit more flexibly according to your requirements. Also, user accounts can be managed by the system administrator using their Windows Server™.

Supports NTLM Authentication Protocol

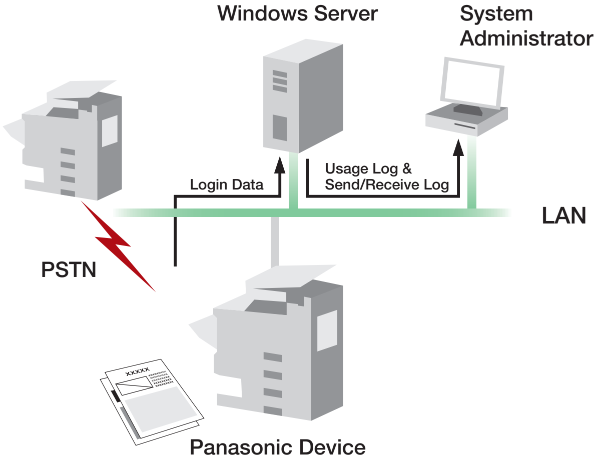
Panasonic’s User Authentication supports the NTLM v2 Authentication Protocol. The NTLM (Windows NT® LAN Manager) protocol is the standard used for network management in the Windows NT® Operating System, and its latest version, “v2”, supports Windows® 2000, Server 2003 and Windows® XP in native mode for more effective management.

Job Tracking

Does your confidential data flow outside the company or office?

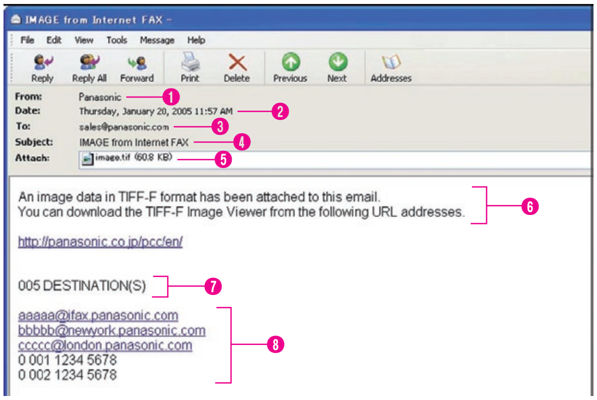
What does “Job Tracking” track?

Even though unauthorized access is prevented, you still need to keep track of who sends what data where. Otherwise, critical data could be sent to the wrong location.
The Job Tracking function can be enabled when User Authentication is used. The Job Tracking function logs fax and email transmission/reception and delivers these to the system administrator via email. When used together with User Authentication, all access to the machine can be controlled by the Windows Server, enabling the system administrator to manage login data to prevent unauthorized access and leakage of data.



Tracking log delivered to administrator

With the Job Tracking function activated, the system administrator will receive a log report via email detailing all fax transmission/reception activity and all email transmission/reception to an Internet Fax or PC. Even fax transmission/reception via the PSTN line can be logged, so the system administrator will be able to keep tabs on everything sent and received, whether via Internet or telephone line.



From: Panasonic
Date: Thursday, January 20, 2005 11:57 AM
To: sales@panasonic.com
Subject: IMAGE from Internet FAX
Attach: image.tif (60.8 KB)

An image data in TIFF-F format has been attached to this email.
You can download the TIFF-F Image Viewer from the following URL addresses.

http://panasonic.co.jp/pcc/en/

005 DESTINATION(S)

aaaaa@ifax.panasonic.com
bbbbb@newyork.panasonic.com
ccccc@london.panasonic.com
0 001 1234 5678
0 002 1234 5678

❶ Sender’s Name (or Login Name in the User Authentication)
❷ Transmitted Date and Time
❸ Sender’s Email Address (or Machine’s Email Address)
❹ Subject
❺ Transmitted Document(s)
❻ Fixed Message
❼ Number of Destination(s)
❽ Transmitted Address(es)

Job Tracking email to administrator includes:

- Name of Machine User
- Destination
- Communication Time
- Sent/Received Document Image

Note:

- When the Job Tracking function is enabled, the following functions are not available.
  - Manual reception
  - On-hook dialing
  - Fax forward

Fax Transmission via RightFax® Server

For Secure Fax Transmission

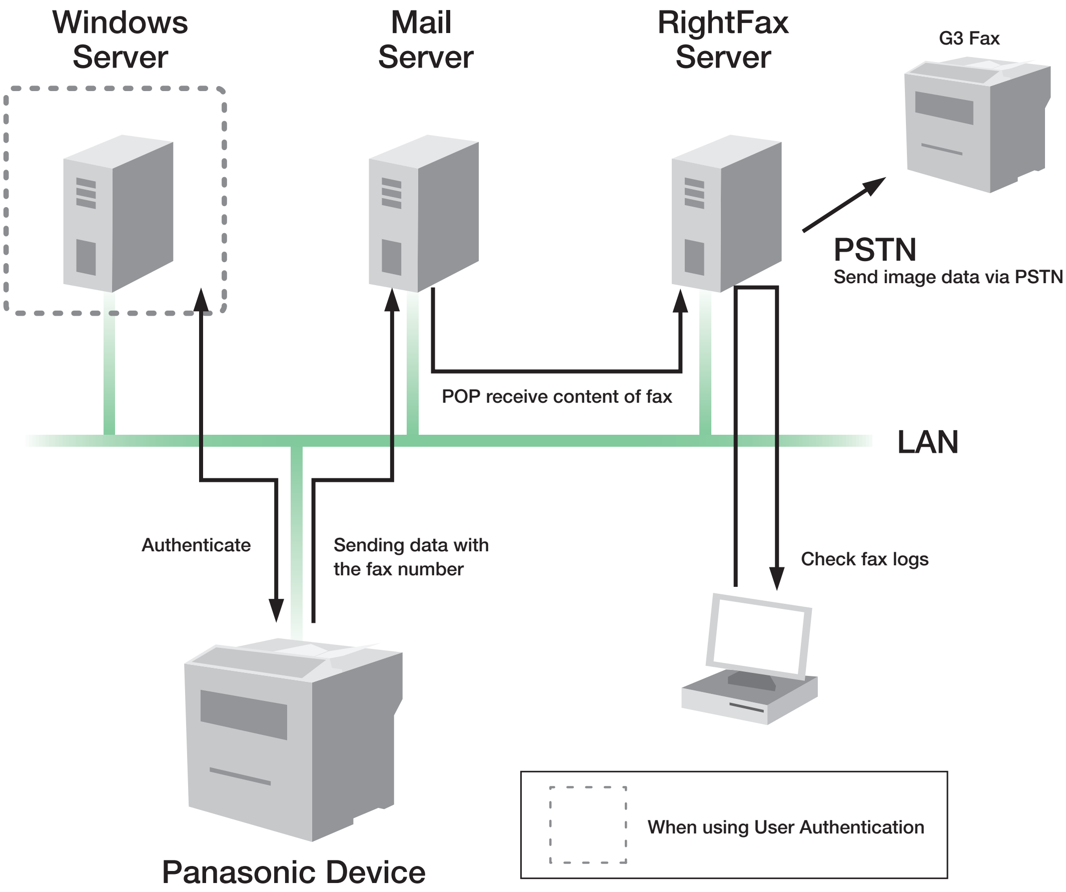
What is the benefit?

If you already use RightFax® as your fax server, Panasonic MFPs let you send hardcopy documents via your RightFax® Server as well. As all fax documents are transmitted via the RightFax® Server in the same manner as with other communication equipment, you don't have to change the way you manage your fax transmission log data.

For more security

In addition to managing fax recipients and data transmitted via the RightFax® Server, you can use User Authentication for more secure fax transmissions. With User Authentication, you can prevent unauthorized fax transmissions via RightFax® Server.

* Requires RightFax® Ver. 8.0 or later.



Secure Printing Functions

Is your confidential data left on the printer?

When is "Secure Printing" required?

When you are printing out confidential data that even other internal staffers are not supposed to see, you have to wait by the machine until the job is completed. This can be a real hassle if there are many jobs ahead of yours or if your job takes a long time. If you don't wait around, your printout could get mixed up with other printouts, it might be left for a long time on the output tray, or even get lost or picked up by someone else. To avoid this, you can use the Secure Printing function. Because you execute the print command at the machine yourself, your document will not be exposed to others, or mixed up with other printouts.

Mailbox & Secure Mailbox

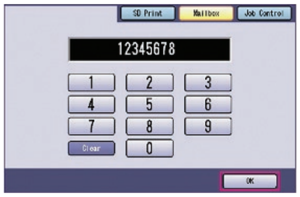
Two types of mailbox printing are available – **Mailbox** and **Secure Mailbox.**
Mailbox is useful when you want to store print data in the device's internal HDD. Once you store the data in the Mailbox, you can recall the stored data and print it out anytime you want. This can be very useful when the printer is busy.
Secure Mailbox provides further security. Once the data is stored in the Secure Mailbox, you have to enter a multi-digit user ID and password to print it. This is especially useful for sensitive documents.

(1) Mailbox data printing

Data stored in the Mailbox storage area can be printed out by entering your Mailbox ID number. Once you've stored print data in the Mailbox, you can leave it there and print it out anytime you need it.

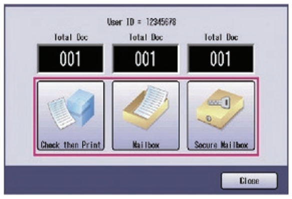
How to print out Mailbox data

❶ Enter the 8-digit Mailbox ID number
❷ Select the Mailbox
❸ Select the job you want printed and press OK



12345678

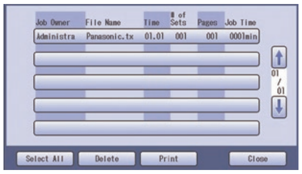
❶



User ID = 12345678

Total Doc	Total Doc	Total Doc
001	001	001

❷



Job Owner	File Name	Time	# of Sets	Pages	Job Time
Administra	Panasonic.tx	01.01	001	001	0001min

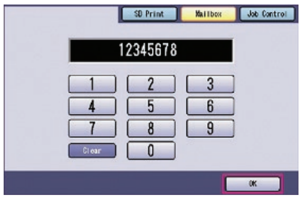
❸

(2) Secure Mailbox data printing

Data stored in a Secure Mailbox can be printed out by entering the 8-digit ID number of the Mailbox and a 4-digit password. To ensure maximum security, data stored in the Secure Mailbox cannot be retrieved without a password.

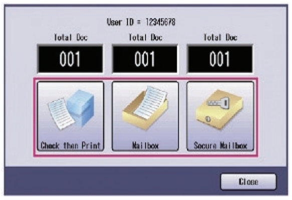
How to print out Secure Mailbox data

❶ Enter the 8-digit Mailbox ID number
❷ Select the Secure Mailbox
❸ Select the job you want printed
❹ Enter the 4-digit password



12345678

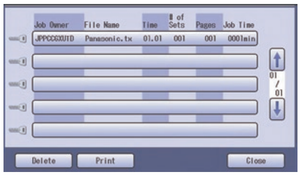
❶



User ID = 12345678

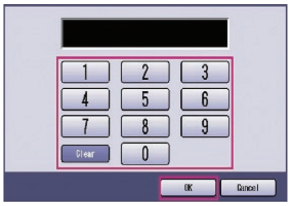
Total Doc	Total Doc	Total Doc
001	001	001

❷



Job Owner	File Name	Time	# of Sets	Pages	Job Time
JPPCCGXUID	Panasonic.tx	01.01	001	001	0001min

❸



❹

Mailbox: Requires 8-digit User ID number
Secure Mailbox: Requires 8-digit User ID & 4-digit Password

HDD/Memory Security

Is your data stolen without you even knowing?

Protect your data from unauthorized remote retrieval

Connecting your MFP to your local area network (LAN) is a great way to enhance productivity and streamline workflow. Unfortunately, it also makes your confidential data vulnerable. Data sent from a PC to the MFP is temporarily stored in the machine's built-in storage (memory or HDD). These days, people worry about an intruder accessing this data via the network or by removing the HDD. To help you avoid this, an HDD/Memory Security function is standard feature provided with Panasonic MFP products*.

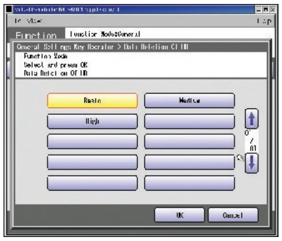
* Refer to the applicable models.

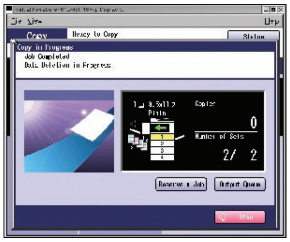
(1) Job-by-Job Erasure

Each time the machine is used for a new copying, scanning or printing job, existing data on the HDD is erased. Three security levels are available: Basic, Medium, and High.
When the Basic level is selected, the HDD's header information, which includes the data size and layout information, is erased. As special data compression is used, the original data cannot be recovered if the header information is lost.
If the Medium or High level is selected, the HDD data is additionally overwritten by zeros and/or random data. This completely destroys the previous data and makes recovery impossible.

For Job-by-Job Erasure function, these three security levels are available depending on your requirements. The security level can be defined by the system administrator.

Basic: Deletes header information in the control area of the HDD
Medium: Overwrites with zeros
High: Overwrites with random data and zeros on the HDD


Function Mode/General
General Settings Key Operator > Data Deletion ON Off
Function Mode
Select and press OK
Data Deletion ON Off


Ready to Copy
Copy in Progress
Job Completed
Data Deletion in Progress

(2) Bulk Erasure

One of the most common ways for critical data to find its way into the wrong hands is through improper disposal or replacement. Before replacing or disposing of a device, the built-in HDD should be thoroughly erased, as data on any HDD can still be accessed even if the machine itself no longer functions. To destroy critical data before disposal, the most effective way is to delete all the data on the HDD, and overwrite the entire disk with random data to make it impossible for any information to be accessed or restored.

Format: Initializes the sector information on the HDD
Medium: Overwrites with zeros
High: Overwrites with random data and zeros on the HDD

(3) Image Memory Erasure

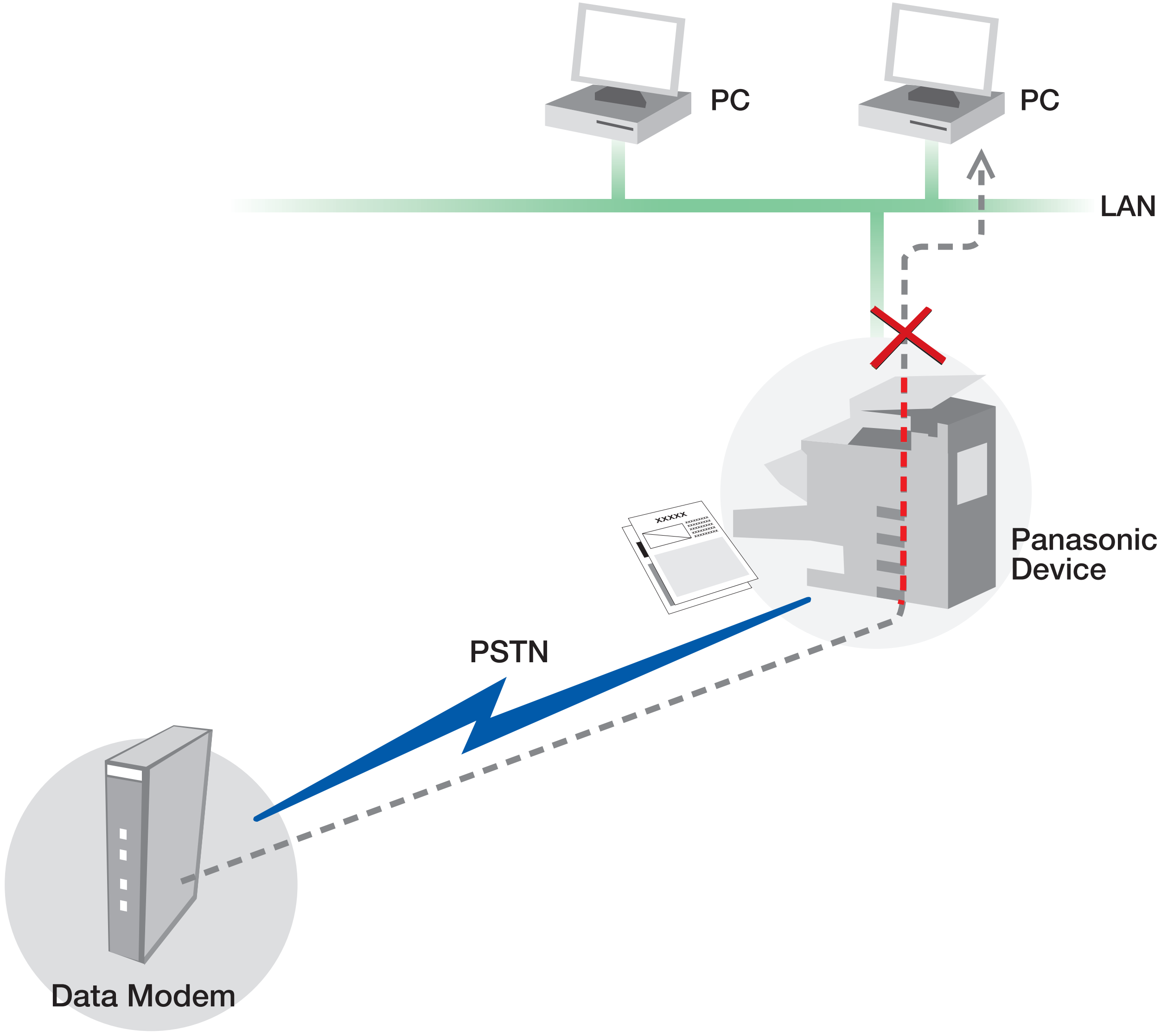
Thanks to today's continuing innovations in technology, today's faxes and Internet faxes feature large image memories capable of storing significant amounts of data. While this enhanced memory capacity is convenient, it also makes confidential data more vulnerable to unauthorized access. To eliminate this problem and assure your peace of mind, the Image Memory Erasure function automatically erases all fax data after each transmission. Once deleted, it cannot be restored.

Fax to Ethernet Connection

Can someone 'hack' into the network via the PSTN connection to the machine?

PSTN line security

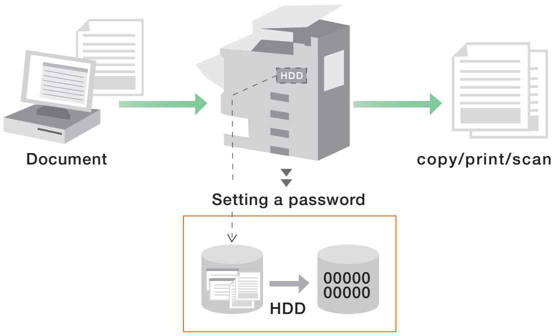
The fax modem control software incorporated in Panasonic devices is used exclusively for fax transmission/reception and does not incorporate the communication protocols used by a data modem. This means that is not possible to connect to the Panasonic device via the PSTN line and make a connection to the network. If an attempt is made to connect to the Panasonic device from a data modem via the PSTN line, the device will immediately terminate the connection to interrupt the communication.



Data Security Kit

A simple “add-on” security solution for your existing devices

Overview of security functions



Document data that is temporarily stored on the hard disk when using the copier/printer/scanner functions is deleted immediately after completion of the operation. However, when data is deleted from the hard disk, typically only the data management information that controls access to the data is deleted. The actual data itself remains intact. As a result, the document data remains on the hard disk, and can possibly be recovered and read by a computer or a utility tool if the hard disk drive is stolen, replaced or disposed of.

To protect your document data, the **Data Security Kit** provides the following security functions.

(1) Document data deletion

Automatically deletes the data regions on the hard disk drive by overwriting the data when outputting the document. Two levels of overwriting security are available:

Medium: Deletes all data by zeroing out all of the document’s data sectors in three passes.

High: Assigns random values to the document’s data sectors in the first two passes, then zeroes out all the data in the third pass.

Before replacing or disposing of the device, it is strongly recommended that the hard disk be initialized and that all data sectors be overwritten in such a way that the data cannot be restored. This can be done utilizing the Data Security Kit’s built-in initialization function.

(2) Hard disk drive lock management

Setting a password for the hard disk drive helps prevent unauthorized use of the data it contains, even if the hard disk drive is removed. Attempting to use a ‘locked’ hard disk drive in another device without the correct password will result in the drive’s data being overwritten.

(3) Security setting protection

Security settings on the device can only be made or changed by the key operator, and only after entering a user-defined, 8-character password.

The DA-SC01 and DA-SC03 Data Security Kits have been approved as EAL2 certified system products.

Common Criteria Validated EAL2
Data Security Kit DA-SC01 V1.01 and DA-SC03 V1.01
The certification obtained for this product regarding information security indicates that, as a result of evaluation based on given evaluation criteria and evaluation method, the target of evaluation used for such evaluation has been determined to conform to the security assurance requirements.

What is “Common Criteria”?

Common Criteria is an international standard defined as ISO15408, which is used to evaluate an information system or the hardware and software that comprises the information system, based on the targeted security assurance level.

What is “EAL”?

EAL stands for Evaluation Assurance Level, which indicates the strictness of the evaluation level, and not the level of security. The EAL is defined in seven levels as shown in the table on the right.

Assurance Levels

Level	Outline
EAL 1	Functionally Tested
EAL 2	Structurally Tested
EAL 3	Methodically Tested and Checked
EAL 4	Methodically Designed, Tested and Reviewed
EAL 5	Semi-formally Designed and Tested
EAL 6	Semi-formally Verified Design and Tested
EAL 7	Formally Verified Design and Tested

System Requirements

Applicable Models

▶ User Authentication:

DP-C406/C306/C266/C405/C305/C265/C354/C264/C323/C263/C213/C322/C262/8060/8045/8035/8032/8025/3030/2330/8020E/8020P/8016P/1820E/190, UF-9000/8000/7000/8200/7200

▶ Job Tracking:

DP-C406/C306/C266/C405/C305/C265/C354/C264/C323/C263/C213/C322/C262/8060/8045/8035/8032/8025/3030/2330/8020E/8020P/8016P/1820E/1820P/190, UF-9000/8000/7000/8200/7200

- Internet Fax/Email/Network Scanner Module is required for the UF-8000/7000/8200-AUG/7200.
- Fax Communication Board and Internet Fax Module are required for the DP-C354/C264/C323/C263/C213/1820E/1820P.
- Fax Communication Board is required for the DP-C406/C306/C266/C405/C305/C265.

▶ Fax Transmission via RightFax® Server:

DP-C406/C306/C266/C405/C305/C265/C354/C264/C323/C263/C213/C322/C262/8060/8045/8035/3030/2330/8020E/8020P/1820E/1820P/190, UF-9000/8000/7000/8200/7200.

- Internet Fax/Email/Network Scanner Module is required for the UF-8000/7000/8200-AUG/7200.
- Internet Fax/E-Mail Module is required for the DP-1820E/1820P.

▶ Secure Printing Functions:

DP-C406/C306/C266/C405/C305/C265/C354/C264/C323/C263/C213/C322/C262/8060/8045/8035/8032/8025/8020E/8020P/8016P/6030/4530/3530/6020/4520/3520/6010/4510/3510/3030/2330/3010/2310/1820E/1820P/1520P/190/180, UF-9000/8000/7000/8200/7200.

- Hard Disk Drive Unit and Image Memory are required for above models except DP-C406/C306/C266/C405/C305/C265/C354/C264/8060/8045/8035, UF-8000/7000/8200/7200.
- SD Memory Card is required for the UF-8000/7000/8200/7200.

▶ HDD/Memory Security:

Job-by-Job Erasure:
DP-C406/C306/C266/C405/C305/C265/C354/C264/C323/C263/C213/C322/C262/8060/8045/8035/8032/8025/8020E/8020P/6030/4530/3530/6020/4520/3520/3030/2330

HDD Deletion:
DP-C406/C306/C266/C405/C305/C265/C354/C264/C323/C263/C213/C322/C262/8060/8045/8035/8032/8025/8020E/8020P/8016P/6030/4530/3530/3030/2330/190, UF-9000

- HDD is required for above models except DP-C406/C306/C266/C405/C305/C265/C354/C264/8060/8045/8035.

▶ Data Security Kit:

DP-C405/C305/C265/8060/8045/8035/8032/8025/3030/2330

- HDD and Image Memory are required for the DP-8032/8025/3030/2330.

Panasonic®
Panasonic System Networks Company of America
One Panasonic Way, Secaucus, NJ 07094
For a local dealer, please call 1-800-742-8086
panasonic.com/office