Manual abstract:

1 Ver. @@@@@@@@1-6 Roles and Requirements of the Administrator.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.1-6 Password Usage Requirements .....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..1-6 Network Connection Requirements for the Machine .....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.1-6 Security function operation setting operating requirements ....

.....

.....

.....

.....

.....

.....

.....

.....

.....

....1-6 Operation and control of the machine.

.....

.....

.....

.....

.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....4-13 <From the PC> .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
4-13 8650 x-3 Contents 8650 x-4 1 Security Security 1 Security Introduction Thank you for purchasing our product. This User's Guide contains the operating procedures and precautions to be used when using the security functions offered by the magicolor 8650 machine. To ensure the best possible performance and effective use of the machine, read this manual thoroughly before using the security functions. The Administrator of the machine should keep this manual for ready reference. The manual should be of great help in finding solutions to operating problems and questions.
This User's Guide (Ver. 1.00) describes magicolor 8650 Multi Function Peripheral Control Software (MFP Controller: A02E0Y0-0100-GP0-12). Compliance with the ISO15408 Standard When the EnhancedSecurity on this machine is set to [ON], more enhanced security functions are available. The security functions offered by the magicolor 8650 machine comply with ISO/IEC15408 (level: EAL3).
Operating Precautions The Administrator of the machine should make sure that each individual general user exits from the current mode to return to the basic screen whenever the access to that mode is completed or if the user leaves the machine with the mode screen left displayed. The Administrator of the machine should exit from the current mode to return to the basic screen whenever the access to that mode is completed or if he or she leaves the machine with the mode screen left displayed. The PageScope Web Connection functions can be used only if the setting is made to accept "Cookie." 1 1.1 8650 1-2 Security INSTALLATION CHECKLIST 1 This Installation Checklist contains items that are to be check by the Service Engineer installing this machine. The Service Engineer should check the following items, then explain each checked item to the Administrator of the machine. To Service Engineer Make sure that each of these items is properly carried out by checking the box on the right of each item. 1. Perform the following steps before installing this machine. Check with the Administrator to determine if the security functions of this machine should be enhanced.

If the functions should be enhanced, check the following. If the security functions are not to be enhanced, quit the operation without checking the following. I swear that I would never disclose information as it relates to the settings of this machine to anybody, or perform malicious or intentional act during setup and service procedures for the machine. When giving the User's Guide Security Operations to the Administrator of the machine, check that the User's Guide is the security-compatible version and explain to the Administrator that it is security-compatible. 2. After this machine is installed, refer to the Service Manual and perform the following steps. Check that the Firmware version (MFP Controller, CheckSum) checked with the Service Manual matches the Firmware version

values indicated on the report output. If there is a mismatch in the Firmware version number, explain to the Administrator of the machine that upgrading of the Firmware is necessary and perform upgrading of the Firmware. Set the Service Password (CE Password) that meets the requirements of the Password Rules. Check that CS Remote Care is set to RAM Clear Set, HDD Installation to Installed, and AuthDeviceSetting to Not Installed.

3. After this machine is installed, refer to this User's Guide and perform the following steps. Check that the Administrator Password has been set by the Administrator of the machine. Check that data has been backed up by the Administrator of the machine using the HDD Backup Utility. Check that the HDD Lock Password or Encryption Key, or both, have been set by the Administrator of the machine.

Check that the self-signed certificate for SSL communications has been registered by the Administrator of the machine. Check that data has been restored by the Administrator of the machine using the HDD Backup Utility. Let the Administrator of the machine set EnhancedSecurity to [ON]. The languages, in which the contents of the User's Guide Security Operations have been evaluated, are Japanese and English. Explain the way how to get the manual in the language, in which it is evaluated.

Explain to the administrator that the settings for the security functions for this machine have been specified. Completed If the Security Kit SC-503 is to be mounted, data must first be backed up using the HDD Backup Utility before the SC-503 is mounted. When the above steps have been properly carried out, the Service Engineer should make a copy of this page and give the original of this page to the Administrator of the machine. The copy should be kept at the corresponding Service Representative for filing. Product Name Customer Service Representative Company Name User Division Name Person in charge 8650 1-3 Security 1 Security Functions Setting the EnhancedSecurity to [ON] will validate the security function of this machine. For details of the settings of different security functions to be changed by turning [ON] the EnhancedSecurity, see "Enhancing the Security Function" on page 2-6. Setting the EnhancedSecurity to [ON] will enhance the authentication function. Access control is then provided through password authentication for any access to the Admin. Settings, Public User Box, a Public User Box data file, and a Secure Print Document file. Access is thereby granted only to the authenticated user.

A password that can be set must meet the requirements of the Password Rules. The machine does not accept setting of an easily decipherable password. For details of the Password Rules, see "Password Rules" on page 1-8. If a wrong password is entered, during password authentication, a predetermined number of times (once to three times) set by the Administrator of the machine or more, the machine determines that it is unauthorized access through Prohibited Functions When Authentication Error, prohibiting any further entry of the password. By prohibiting the password entry operation, the machine prevents unauthorized use or removal of data, thereby ensuring secured used of the machine. To cancel the password entry operation prohibited condition, the Administrator must perform the Release Setting. When the Administrator performs the Release Setting for the operation prohibited condition, a sound operation control in utmost security is achieved under the control of the Administrator. Setting the HDD Lock Password provides the following security function. That is, even if the HDD is illegally replaced with another, the HDD authentication function prohibits access to the HDD, when the HDD Lock Password is yet to be set or there is a mismatch in the passwords. In addition, should the HDD be removed unawares, the HDD Lock Password locks the HDD protecting data contained in the HDD.

Furthermore, by mounting the optional Security Kit SC-503 and setting the Encryption Key, the data stored in the HDD is encrypted, thereby protecting the data in the HDD. Note, however, that the HDD Lock Password and Encryption Key do not prevent the HDD from being physically removed. Make sure of a good operation control. When the machine is to be discarded, or use of a leased machine is terminated at the end of the leasing contract, the Overwrite All Area function overwrites and erases all data stored in all spaces of the HDD. The function also resets all passwords saved in the NVRAM to factory settings, preventing leak of data.

For details of items to be cleared by Overwrite All Area function, see "Types of Data Cleared by Overwrite All Area Function" on page 1-10. 1.2 1.2.1 Check Count Clear Conditions The following are the conditions for clearing or resetting the check count of the number of wrong entries at the time of authentication by the EnhancedSecurity.

<Admin. Settings> Authentication of Admin. Settings is successful. <Secure Print Document> Authentication of Secure Print Document is successful. Release of Prohibited Functions When Authentication Error is executed. <Public User Box> Authentication of Public User Box is successful. Authentication for execution of change of Public User Box Name and User Box Password is successful. Release of Prohibited Functions When Authentication Error is executed. <SNMP Password (auth-password, priv-password)> Authentication of SNMP is successful. Release of Prohibited Functions When Authentication Error is executed.

8650 1-4 Security 1 Data to be Protected The underlying concept of this machine toward security is "to protect data that can be disclosed against the intention of users." The following types of image files that have been stored in the machine and made available for use by its users are protected while the machine is being used. Image files stored by Secure Print Image files stored in Public User Box The following types of data stored in the HDD are protected when use of a leased machine is terminated at the end of the leasing contract, the machine is to be discarded, or when the HDD is stolen. Image files stored by Secure Print Image files stored in Public User Box Image files of a job in the queue Image files other than Secure Print file and Public User Box file Data files left in the data space used as image files Temporary data files generated during print image file processing This machine offers specific functions as data protection method: the SSL function that ensures confidentiality of images transmitted and received over the network. When transmitting and receiving highly confidential image data among different pieces of IT equipment within an office LAN, the machine carries out communications with the correct destination via encrypted and reliable paths, assuming an office environment that responds to most stringent security requirements. 1.3 8650 1-5 Security 1 Precautions for Operation Control This machine and the data handled by this machine should be used in an office environment that meets the following conditions. Roles and Requirements of the Administrator The Administrator should take full responsibility for controlling the machine, thereby ensuring that no improper operations are performed. <To Achieve Effective Security> A person who is capable of taking full responsibility for controlling the machine should be appointed as the Administrator to make sure that no improper operations are performed.

Password Usage Requirements The Administrator must control the Administrator Password, HDD Lock Password, Encryption Key, Authpassword, and Priv-password appropriately so that they may not be leaked.

These passwords should not be ones that can be easily guessed. The user, on the other hand, should control the Secure Print Password appropriately so that they may not be leaked. Again, these passwords should not be ones that can be easily guessed. For the Public User Box shared among a number of users, the User Box Password should be appropriately controlled so that it may not be leaked to anyone who is not the user of the Public User Box. <To Achieve Effective Security> Make absolutely sure that only the Administrator knows the Administrator Password, HDD Lock Password, Encryption Key, Auth-password, and Priv-password.

The Administrator must change the Administrator Password, HDD Lock Password, Encryption Key, Auth-password, and Priv-password at regular intervals. The Administrator should make sure that any number that can easily be guessed from birthdays, employee identification numbers, and the like is not set for the Administrator Password, HDD Lock Password, Encryption Key, Auth-password, and Priv-password. If a Public User Box Password has been changed, the Administrator should have the corresponding user change the password as soon as possible. If the Administrator Password has been changed by the Service Engineer, the Administrator should change the Administrator Password as soon as possible. The Administrator should have users ensure that the Secure Print Document is known only by the user concerned.

The Administrator should make sure that only the users who share a Public User Box know the password set for it. The Administrator should have users change the passwords set for the Public User Box at regular intervals. The Administrator should make sure that any user does not set any number that can easily be guessed from birthdays, employee identification numbers, and the like for the passwords set for the Secure Print Document, and Public User Box. Network Connection Requirements for the Machine Packets being transmitted over the LAN installed in the office, in which the machine is installed, should be protected from unauthorized manipulation. If the LAN is to be connected to an outside network, no unauthorized attempt to establish connection from the external network should be permitted. <To Achieve Effective Security> If the LAN, in which the machine is installed, is connected to an outside network, install a firewall or similar network device to block any access to the machine from the outside network and make the necessary settings. Configure the LAN installed in the office, in which the machine is installed, by using a switching hub and other devices to ensure that the packets are protected from unauthorized manipulation. Provide an appropriate network control at all times to make sure that no other copying machine or printer is connected without prior notice to the office LAN to which this machine is connected. Security function operation setting operating requirements The Administrator should make sure of correct operation control so that the machine is used with the EnhancedSecurity set to [ON]. 1.

4 8650 1-6 Security Operation and control of the machine 1 The Administrator of the machine should perform the following operation control. The Administrator of the machine should log off from the Admin. Settings whenever the operation in the Admin. Settings is completed. The Administrator of the machine should also make sure that each individual user makes it a rule to quit each session whenever it is completed, including those of the Secure Document file, Public User Box, and Public User Box file. The Administrator of the machine should set the HDD Lock Password according to the environment, in which this machine is used. If the machine is mounted with the optional Security Kit SC-503, the Administrator should also set either the HDD Lock Password or Encryption Key, or both. Machine Maintenance Control The Administrator of the machine should perform the following maintenance control activities. Provide adequate control over the machine to ensure that only the Service Engineer is able to perform physical service operations on the machine. Provide adequate control over the machine to ensure that any physical service operations performed on the machine by the Service Engineer are overseen by the Administrator of the machine.

*8650 1-7 Security 1 Miscellaneous Password Rules According to certain Password Rules, registration of a password consisting of a string of a single character or change of a password to one consisting of a string of a single character is rejected for the Administrator Password, Public User Box Password, Secure Print Password, HDD Lock Password, and Encryption Key. For the Administrator Password, HDD Lock Password, and Encryption Key, the same password as that currently set is not accepted. Study the following table for more details of the number of digits and characters that can be used for each password. Types of passwords Administrator Password No. of digits 8 digits Characters · · · Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~ Selectable from among a total of 92 characters · · · Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, $, %, &, ', (, ), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \, ], ^, _, `, {, |, }, ~, SPACE Selectable from among a total of 93 characters 20 digits · Numeric characters: 0 to 9 · Alpha characters: upper and lower case letters · Symbols: !, #, $, %, &, ', *, +, -, ., /, =, ?, @, ^, _, `, {, |, } ~ Selectable from among a total of 83 characters Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, $, %, &, ', (, ), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \, ], ^, _, `, {, |, }, ~, ", +, SPACE Selectable from among a total of 95 characters · · · Numeric characters: 0 to 9 Alpha characters: upper and lower case letters Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [,], ^, _, `, {, |, }, ~, ", + Selectable from among a total of 93 characters · · · 1. 5 Secure Print Password HDD Lock Password Encryption Key Public User Box Password 8 digits SNMP Password · Auth-password · Priv-password 8 digits or more ! Detail Note that use of the characters "","" "+," and "space" may be partly limited. Precautions for Use of Various Types of Applications When PageScope Web Connection or an application of various other types is used, the password control function of the application stores the password that has been entered in your PC.*

If you want the password not stored, disable the password control function of the application. When using the PageScope Web Connection or an application of various other types, use one that shows "" or "" for the password entered. If the client PC uses the Internet Explorer or other type of web browser, "SSL v3" or "TLS v1" should be used, not "SSL v2", for the SSL setting. Encrypting communications The following are the cryptographic algorithms of key exchange and communications encryption systems supported in generation of encryption keys. TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA 8650 1-8 Security 1 2 Note No algorithms can be selected during generation of encryption keys. SSL v3 is automatically selected for the SSL setting according to the application and browser. Do not therefore change the setting manually to SSL v2. Use the following browsers to ensure SSL encryption communication with appropriate strength.*

Use of any of the following browsers achieves SSL encryption communication that ensures confidentiality of the image data transmitted and received. Windows 98, Me, NT4.0, 2000, XP, Server2003 Recommended is Microsoft "Internet Explorer 6" or later. If "Internet Explorer 5.x" is used, Microsoft XML parser "MSXML 3.x" or later must be installed. Recommended is Netscape Navigator 7.02 or later. Recommended is Mozilla Firefox 1.0 or later. Macintosh MacOS 8.x, 9.x, MacOS X Recommended is Netscape Navigator 7.02 or later. Recommended is Mozilla Firefox 1.
0 or later. Linux Recommended is Netscape Navigator 7.02 or later. Recommended is Mozilla Firefox 1.0 or later.
SSL encryption communication with confidentiality properly maintained can be achieved in image data transmitted and received in any of the following applications. HDD Backup Utility IPP printing IPP (Internet Printing Protocol) is a function that allows Secure Print Documents and image data stored in Public User Boxes to be printed via the Internet by using the HTTP (HyperText Transfer Protocol) of the TCP/IP Protocol. IPPS (IPP over SSL/TLS) is the type of IPP that performs the SSL encryption communication. <IPP setting on Windows Vista> Windows Vista, which offers enhanced security functions, gives a certificate error message if the SSL certificate is one that is not issued by a certification body. In such cases, it becomes necessary to register with Windows Vista the certificate of this machine as that issued by a reliable party for the computer account. First, register Host Name and IP address of this machine in the DNS server in advance. Then, in TCP/IP Settings of PageScope Web Connection, set the DNS Host Name and DNS Default Domain Name registered with the DNS server. It should also be noted that, for the certificate to be imported, a certificate for SSL encryption communication should be registered in PageScope Web Connection and exported in advance as the certificate including the public key. 1 2 3 From "Continue to this website," call the PageScope Web Connection window to the screen. Click "Certificate Error" to display the certificate.

Then, click "Install Certificate" to install the certificate. Display the physical stores. Then, deploy the certificate, which has earlier been exported, in "Local Computer" of "Trusted Root Certification Authorities" to thereby import the certificate. <IPPS printing settings in Windows Vista> Through additional printer setting, type "https://Host Name.Domain Name/ipp." For [Host Name] and [Domain Name], specify the names set with the DNS server. 8650 1-9 Security <Installing printer driver> 1 To perform IPP printing, the printer driver must be installed. From "Add Printer Wizard," select "Connect to a printer on the Internet or on your intranet" and type the URL of this machine in the following format in the "URL" field. http:// <IP address of this machine> /ipp E.g.
: If the machine IP address is 192.168.1.20 Type http://192.168.
1.20/ipp To set IPPS printing: Type https:// <IP address of the machine> /ipp. ! Detail The printer, for which the settings have been made, can be used in the same manner as the ordinary local printer. Types of Data Cleared by Overwrite All Area Function The Overwrite All Area function clears the following types of data. Types of Data Cleared Public User Box registration data/file Secure Print ID/Password/file Image files Description Deletes all Public User Box-related information and files saved in Public User Box Deletes all Secure Print Document-related information and files saved · · HDD Lock Password Encryption Key Administrator Password SNMP Password SSL certificate Network Setting Image files saved other than Secure Print Document files and Public User Box files Image files of jobs in job queue state Clears the currently set password Clears the currently set Encryption Key Clears the currently set password, resetting it to the factory setting Clears the currently set password, resetting it to the factory setting (MAC address) Deletes the currently set SSL certificate 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 8650 1-10 2 Administrator Operations Administrator Operations 2 2 2.
1 Administrator Operations Accessing the Admin. Settings This machine implements authentication of the user of the Admin. Settings function through the 8-digit Administrator Password that verifies the identity as the Administrator of the person who accesses the function. During the authentication procedure, the Administrator Password entered for the authentication purpose appears as "" or "" on the display. When the EnhancedSecurity is set to [ON], the number of times in which authentication fails is counted. 2.1.1 Accessing the Admin. Settings The machine does not accept access to the Admin. Settings under any of the following conditions.*

Wait for some while before attempting to gain access to the Admin. Settings again. The Admin. Settings has been logged on to through access made from the PC. A remote operation is being performed from an application on the PC. There is a job being executed by the machine. Immediately after the main power switch has been turned ON. A malfunction code is displayed on the machine. 2 Note Make sure that none of the general users of the machine will know the Administrator Password. @@Contact your Service Representative.
Do not leave the machine with the setting screen of Admin. Settings left shown on the display. @@Settings. While you are logging onto the Admin Mode using PageScope Web Connection, any operations from the machine's control panel are disabled.

When accessing the Admin.
Settings from the control panel, if you have already logged on to the Admin. Settings using PageScope Web Connection, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Admin. Settings once again. When accessing the Admin.
Settings from the control panel, if [Export to the device] operation is being executed using the PageScope Data Administrator, the machine displays a message that tells not to turn off the power because of the remote operation being performed and rejects any operation on the control panel. Wait until the message disappears before attempting to access the Admin. Settings once again. The Administrator must first make User Authentication settings before he or she can access User Mode. 8650 2-2 Administrator Operations <From the Control Panel> 2 1 2 Press the [Menu/Select] key. Press the [,] key to select [Admin. Settings]. ? 3 4 Is it possible to gain access to the Admin. Settings while a job is being executed? % The machine does not accept access to the Admin. Settings while a job is being executed.

Wait until the execution of the job is completed before attempting to access the Admin. Settings again. Press the [Menu/Select] or [)] key. Press the [+] and/or [,] key to enter the 8-digit Administrator Password. Press the [*] key to delete the last character entered. 5 Press the [Menu/Select] key. ? % What happens if a wrong Administrator Password is entered? If a wrong Administrator Password is entered, a message appears saying that there is a mismatch in the Administrator Passwords and entry of the Administrator Password will be prohibited for five sec. Wait for some while before entering the correct Administrator Password. % If the EnhancedSecurity is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password.
The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
6 Press the [Cancel] key to log off from the Admin. Settings. 8650 2-3 Administrator Operations <From PageScope Web Connection> 2 1 2 3 4 5 Start the Web browser. Enter the IP address of the machine in the address bar. Press the [Enter] key to start PageScope Web Connection.
Click [Logout] and [OK]. You log off from the Public User mode. Click the Administrator radio button and [Login]. 6 Select "Administrator (Admin Mode)" or "Administrator (User Mode)" and enter the 8-digit Administrator Password in the "Password" box. ? Administrator (Admin Mode) is a mode, in which settings of the machine can be registered or changed. In this mode, system and network settings can be made. Administrator (User Mode) is a mode, in which the same settings as the user authority can be made. For box setting operations, however, the same functions can be set as those of Admin Mode. User Mode also allows jobs to be checked or deleted, which is not possible in Admin Mode. What is the Administrator Password used for accessing the Admin Mode via the PageScope Web Connection? % When accessing the Admin Mode using the PageScope Web Connection, enter the same Administrator Password as that for the machine.

8650 2-4 Administrator Operations 2 7 Click the [OK]. ? What happens if a wrong Administrator Password is entered? % If a wrong Administrator Password has been entered, the machine gives a message that tells that authentication has not been successful. In this case, click [OK] and enter the correct Administrator Password in the "Password" box. % If the EnhancedSecurity is set to [ON], entry of a wrong password is counted as unauthorized access. If a wrong Administrator Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine or more, a message appears saying that the machine accepts no more Administrator Passwords because of unauthorized access for any subsequent entry of the Administrator Password. The machine is then set into an access lock state. To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly.
? What if you fail to log on to the Admin Mode? % If you have already logged on to the Admin Mode from the control panel or using PageScope Web Connection, the machine displays a message that tells that another administrator has previously logged on and rejects any attempt to log on to the Admin Mode using the PageScope Web Connection. Click [OK] and wait for some while before attempting to access the Admin Mode once again. % If [Export to the device] operation is being executed using the PageScope Data Administrator, the machine displays a message that tells you cannot log on to the mode because of the remote operation being performed and rejects any attempts to the Admin Mode via the PageScope Web Connection. Click [OK] and wait for some while before attempting to access the Admin Mode once again. ? 8 9 Is it possible to gain access to the Admin Mode while a job is being executed? % If an attempt is made to log on to the Admin Mode while a job is being executed, the machine gives a message that tells that it is now impossible to log on to the Admin Mode.
Click [OK] and try logging on to the Admin Mode after the execution of the job is completed. Click the [Logout]. Click the [OK]. This allows you to log off from the Admin Mode. 2 Note If you have logged on to the Admin Mode using the PageScope Web Connection and if you close the web browser without clicking [Logout], the touch panel of the machine remains locked for 70 sec.
8650 2-5 Administrator Operations 2 2.

2 Enhancing the Security Function When access to the Administrator of the machine by the Admin. Settings via the control panel is authenticated, the machine enables setting of the EnhancedSecurity that allows settings for enhancing each of different security functions to be converted all at once. In the EnhancedSecurity, the machine allows selection of whether to use the EnhancedSecurity or not. If the EnhancedSecurity is set to [ON], a count is taken of the number of unauthorized accesses to the Admin. Settings, SNMP authentication, all Secure Print Documents, and all Public User Boxes. A function is also set that determines whether each password meets predetermined requirements. The security function is thus enhanced in the EnhancedSecurity. The following settings must first be made before the EnhancedSecurity is set to [ON]. 2 Note First, set the Encryption Key.

To set the Encryption Key, HDD Format must first be executed. Execution of the HDD Format clears various setting values. For details of items that are cleared by HDD Format, see "Items cleared by HDD Format" on page 2-7. If both the HDD Lock Password and Encryption Key have been set, it is not possible to cancel the setting of either one of these. If initialization is executed by the Service Engineer, set the Administrator Password and turn [ON] the EnhancedSecurity again. If User Authentication is set to [ON] with the EnhancedSecurity turned [ON], it cannot be set to [OFF] as long as the EnhancedSecurity is [ON]. To turn [OFF] the User Authentication, first turn [OFF] the EnhancedSecurity. Settings to be Made in Advance Administrator Password HDD Lock Password, Encryption Key Certificate for SSL CE Password CS Remote Care HDD installation setting AuthDeviceSetting Description An 8-digit password that meets the Password Rules. The factory setting is "12345678." Set the 20-digit HDD Lock Password or Encryption Key, or both. (Encryption Key can be set only when the Security Kit SC-503 is mounted.) Register the self-signed certificate for SSL communications. Calls for setting made by the Service Engineer. For details, ask your Service Representative. Setting the EnhancedSecurity to [ON] changes the setting values of the following functions.
*Function Name Password Rules Prohibited Functions Factory Setting OFF Mode 1 When EnhancedSecurity is set to [ON] ON (not to be changed) Mode 2 (not to be changed) : Three times is set. * The number of times can be changed to once, twice, or three times. Mode 2 (not to be changed) * In association with Prohibit Functions the method is changed from authentication using Secure Print ID and password (Mode 1) to that using the password with the secure document first narrowed down by Secure Print ID (Mode 2). ON (not to be changed) OFF (not to be changed) Only Read is enabled (not to be changed) The security level can be selected from among [auth-password] and [auth/priv-password]. An 8-digit-or-more auth-password and priv-password can both be set. Restrict (not to be changed) Restrict Security Print Access Mode 1 SSL FTP Server SNMPv1/v2c SNMP v3 Security Level and auth/priv-password OFF ON Read/Write enabled auth/priv-password Print Data Capture Network Setting Clear Allow Enabled 8650 2-6 Administrator Operations 2 Factory Setting Enabled 5 min. MINIMUM When EnhancedSecurity is set to [ON] Restrict (not to be changed) The setting value should be 5 min. or more (no value less than 5 can be set) Not to be set to OFF * If OFF is selected, it is changed to MINIMUM. The MINIMUM or ON option, if selected, remains unchanged. Prohibits the administrator from performing [Firmware Update] (not displayed). Function Name Administrator Password Change Via Network Release Time settings Admin. Sec. Levels Firmware Update Enabled (displayed) 2 Reminder When Password Rules is set to [ON], the characters and the number of digits used for each password are restricted. For details of Password Rules, see "Password Rules" on page 1-8. 2.*

2.1 Items cleared by HDD Format Following are the items that are cleared by HDD Format. Whenever HDD Format is executed, be sure to set the EnhancedSecurity to [ON] again. Types of Data Cleared EnhancedSecurity Public User Box registration data/file Secure Print ID/Password/file Description Set to [OFF] Deletes all Public User Box-related information and files saved in Public User Box Deletes all Secure Print Document-related information and files saved 8650 2-7 Administrator Operations 2 2.2.2 Setting the EnhancedSecurity 2 Note When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. @@Do not leave the machine with the setting screen of Admin. Settings left shown on the display. @@Settings. <Setting can be made only from the control panel> 0 For the procedure to call the Admin.
Settings to the display, see "Accessing the Admin. Settings" on page 2-2. Call the Admin. Settings to the screen from the control panel. Press the [,] key to select [Security Settings].
1 2 3 4 Press the [Menu/Select] or [)] key. Press the [,] key to select [EnhancedSecurity]. 5 6 Press the [Menu/Select] or [)] key. Press the [+] and/or [,] key to enable the EnhancedSecurity and select [ON]. ? What is the factory setting for the EnhancedSecurity? % The EnhancedSecurity is factory-set to [OFF]. Be sure to turn [ON] the EnhancedSecurity so as to enable the security function of the machine. 8650 2-8 Administrator Operations 2 7 Press the [Menu/Select] key. The following screen appears if the previously required settings are yet to be made by the Administrator of the machine. Make the necessary settings according to the corresponding set procedure. The following screen appears if the previously required settings are yet to be made by the Service Engineer. Consult the Service Representative. 8 Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch. If the EnhancedSecurity is properly set to [ON], the following icon appears on the lower right portion in the screen, indicating that the machine is in the EnhancedSecurity. 8650 2-9 Administrator Operations 2 2.

3 HDD Installation When access by the Administrator of the machine through the Admin. Settings via the control panel is authenticated, the machine enables setting of HDD Installation. The following types of data are cleared when the setting for HDD Installation is changed from [Installed] to [Not Installed]. If the HDD Installation is later changed back from [Not Installed] to [Installed], be sure again to make the settings for the types of data that have been cleared. Types of Data Cleared EnhancedSecurity User Box Function Description Set to [OFF] Disabled 2 Note When the setting for HDD Installation is changed from [Installed] to [Not Installed], EnhancedSecurity is set to [OFF].

When the HDD Installation is later changed back from [Not Installed] to [Installed], be sure again to set EnhancedSecurity to [ON]. For details of the EnhancedSecurity, see "Setting the EnhancedSecurity" on page 2-8. ! Detail When the setting for HDD Installation is first set to [Not Installed] and later changed back to [Installed] and if the original hard disk is reused, the image data and Security Print Document contained in the respective boxes become usable. Note, however, that all Personal User Boxes and Group User Boxes become Public User Boxes. If the password set for a particular box before this change does not meet the requirements of Password Rules, however, no access can be made to the Public User Box, to which that specific box was changed. In this case, the Administrator must first newly set a password that meets the requirements of the Password Rules. For details of Password Rules, see "Password Rules" on page 1-8. 2.3.1 Setting HDD Installation 2 Note Do not leave the machine with the setting screen of Admin.
Settings left shown on the display. @@Settings. <Setting can be made only from the control panel> 0 For the procedure to call the Admin. Settings to the display, see "Accessing the Admin. Settings" on page 2-2.
Call the Admin. Settings to the screen from the control panel. Press the [,] key to select [Option Settings]. 1 2 3 Press the [Menu/Select] or [)] key. 8650 2-10 Administrator Operations 2 4 Press the [,] key to select [HDD Installation]. 5 6 Press the [Menu/Select] or [)] key. Press the [+] and/or [,] key to select [Installed] or [Not Installed]. 7 8 Press the [Menu/Select] key. Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch.

2 Note When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. 8650 2-11 Administrator Operations 2 2.4 Preventing Unauthorized Access When access by the Administrator of the machine through the Admin. Settings via the control panel is authenticated, the machine enables setting of the operation of ProhibitFunctions. The machine then takes a count of the number of unsuccessful accesses to the Admin. Settings, SNMP authentication, Secure Print authentication, and Public User Box authentication to prohibit the authentication operation. Either [Mode 1] or [Mode 2] can be selected for ProhibitFunctions. The factory setting is [Mode 1]. If the EnhancedSecurity is set to [ON], it is prohibited to change the setting from [Mode 2] (check count: three times). It is nonetheless possible to change the check count to select from among once, twice, or three times.
If [Mode 2] is selected, the Release Time Settings function is enabled. When the Admin. Settings is set into the access lock state, the main power switch is turned off and on and, after the lapse of a predetermined period of time after the machine is turned on again, the access lock state of the Admin. Settings is canceled. The Release Time Settings function allows the period of time, after the lapse of which the access lock state of the Admin.
Settings is canceled, to be set in the range between 1 and 60 min. The factory setting is 5 min. For details of each mode, see the table below. Mode Mode 1 Mode 2 Description If authentication fails, the authentication operation (entry of the password) is prohibited for 5 sec. If authentication fails, the authentication operation (entry of the password) is prohibited for 5 sec.
The number of times, in which authentication fails, is also counted and, when the failure count reaches a predetermined value, the authentication operation is prohibited and the machine is set into an access lock state. 2 Note If the access lock state of the Admin. Settings is canceled by the Service Engineer, the setting of the Release Time Settings function is not applied. 2.4.1 Setting ProhibitFunctions 2 Note Do not leave the machine with the setting screen of Admin. Settings left shown on the display. @@Settings. Release Time can be set to any value between 1 min. and 60 min.

in 1-min. increments. In the EnhancedSecurity, Release Time less than 5 min. cannot be set. 8650 2-12 Administrator Operations <Setting can be made only from the control panel> 0 2 For the procedure to call the Security Settings menu to the display, see steps 1 through 3 of "Setting the EnhancedSecurity" on page 2-8. Call the Security Settings to the screen from the control panel. Press the [,] key to select [Security Details]. 1 2 3 4 Press the [Menu/Select] or [)] key. Press the [,] key to select [ProhibitFunctions]. 5 6 Press the [Menu/Select] or [)] key.
Press the [,] key to select [Mode Setting]. 7 8 Press the [Menu/Select] or [)] key. Press the [+] and/or [,] key to select [Mode 2]. 9 Press the [Menu/Select] key. 8650 2-13 Administrator Operations 2 10 Press the [,] key to select [#of Auth Attempts].
11 12 Press the [Menu/Select] or [)] key. Press the [+] and/or [,] key to set the check count. 13 14 Press the [Menu/Select] key. Press the [,] key to select [Release Time]. 15 16 Press the [Menu/Select] or [)] key.
Press the [+] and/or [,] key to set the time to cancel the access lock state of Admin. Settings. Press the [*] or [)] key to move the cursor (digit). 17 Press the [Menu/Select] key. 8650 2-14 Administrator Operations 2 2.5 Canceling the Operation Prohibited State When access to the Administrator of the machine by the Admin. Settings via the control panel is authenticated, the machine enables the operation of Release Setting performed for canceling the state of ProhibitFunctions (access lock state) as a result of unauthorized access. Release Setting clears the unauthorized access check count for all SNMP authentication, all Secure Print authentication, and all Public User Box authentication, resetting it to zero. Perform the following procedure to cancel the password entry prohibited state. Admin.

Settings: The operation prohibited state is canceled by the Service Engineer, or after the lapse of a predetermined period of time after the main power switch is turned off and on Secure Print authentication: Release Public User Box authentication: Release SNMP authentication: Release 2.5.1 Performing Release Setting 2 Note When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. @@Do not leave the machine with the setting screen of Admin. Settings left shown on the display. @@Settings. <Setting can be made only from the control panel> 0 For the procedure to call the ProhibitFunctions menu to the display, see steps 1 through 5 of "Setting ProhibitFunctions" on page 2-12. Call the ProhibitFunctions to the screen from the control panel. Press the [,] key to select [Release].

1 2 3 4 Press the [Menu/Select] or [)] key.

Press the [+] and/or [,] key to select the function, for which the state of Prohibit Setting (access lock state) as a result of unauthorized access is to be canceled. 5 Press the [Menu/Select] key. This clears the unauthorized access check count for the selected function, resetting it to zero. 8650 2-15 Administrator Operations 2 2.6 User Box Function When access to the Administrator of the machine by the Admin.

Settings is authenticated, the machine enables the User Box. It also allows the User Box Password to be changed. User Box prepares a User Box in the HDD as a space for saving image files. The Administrator of the machine is allowed to register a Public User Box that is shared among registered users. Up to 1,000 Public User Boxes can be registered.

A User Box Password may consist of 8 digits. The password entered is displayed as "" or "." 2.6.1 Setting the User Box 2 Note Do not leave the machine with the setting screen of Admin Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode. <Setting can be made only from PageScope Web Connection> 0 For the procedure to access the Admin Mode, see "Accessing the Admin. Settings" on page 2-2. Start PageScope Web Connection and access the Admin Mode. Click the [Box] tab and the [Create User Box] menu.*

1 2 3 Make the necessary settings. 8650 2-16 Administrator Operations 2 ? Are there any precautions to be used when making settings? % Be sure to enter the User Box Number., User Box Name, User Box Password, and Retype User Box Password. % A User Box Number that has been registered cannot be registered anew. 4 Click the [OK]. ? What happens if the User Box Password entered does not meet the requirements of Password Rules? % If the User Box Password entered does not comply with the Password Rules, a message appears that tells that the User Box Passwords entered cannot be used. Click [OK] to go back to the screen of step 3. Perform steps 3 and 4 once again. For details of Password Rules, see "Password Rules" on page 1-8. What happens if there is a mismatch in the User Box Passwords? % If there is a mismatch in the User Box Passwords, a message appears that tells that there is a mismatch in the User Box Passwords.

Enter the correct User Box Password. What steps should be performed to change the User Box Password and User Box Attribute? % For the procedure to change the User Box Password and User Box Attribute, see "Using User Box Attribute Change" on page 2-18. ? ? 5 Check the message that tells that the setting has been completed. Then, click [OK]. 8650 2-17 Administrator Operations 2 2.

6.2 Using User Box Attribute Change The Administrator of the machine can change User Box Attributes including the User Box Name and User Box Password of a Public User Box previously registered. 2 Note Do not leave the machine with the setting screen of Admin Mode left shown on the display. If it is absolutely necessary to leave the machine, be sure first to log off from the Admin Mode. <Setting can be made only from the PageScope Web Connection> 0 For the procedure to access the Admin Mode, see "Accessing the Admin.

Settings" on page 2-2. Start PageScope Web Connection and access the Admin Mode. Click the [Box] tab and the [Open User Box] menu. 1 2 3 Enter any given User Box Number and click [OK]. 8650 2-18 Administrator Operations 2 4 Click the [User Box Setting]. ? 5 What steps should be performed to delete a User Box? % To delete a User Box, click [Delete User Box]. A message will then appear for confirming whether the specific User Box can definitely be deleted. Click [OK] to delete the specified User Box. Make the necessary settings. To change a User Box Password, select the "User Box Password is changed.

" check box. What precautions should be used when entering the User Box Password? % If [Public] is set for the box type of Personal/Group User Box with the User Auth/Account Track turned ON, enter the User Box Password that meets the requirements of the Password Rules in the "New Password" box. For details of Password Rules, see "Password Rules" on page 1-8. ? % In the "Retype New Password" box, enter the same User Box Password as that entered in the "New Password" box. 6 Click the [OK]. ? What happens if the User Box Password entered does not meet the requirements of the Password Rules when [Public] is set for the box type of Personal/Group User Box with the User Auth/Account Track turned ON? % If the User Box Password entered does not meet the requirements of the Password Rules when [Public] is set for the box type of Personal/Group User Box with the User Auth/Account Track turned ON, a message appears that tells that the User Box Password entered cannot be used. Click [OK] to go back to the screen of step 4. Perform steps 4 through 6 once again. For details of Password Rules, see "Password Rules" on page 1-8. What happens if there is a mismatch in the User Box Passwords? If there is a mismatch in the User Box Password between that entered in "New Password" and that entered in "Retype New Password," a message appears that tells that there is a mismatch in the User Box Password.

Enter the correct User Box Password. ? % 8650 2-19 Administrator Operations 2 2.7 Changing the Administrator Password When access to the Administrator of the machine from the control panel by the Admin. Settings is authenticated, the machine enables the operation of changing the Administrator Password required for accessing the Admin. Settings.

The Administrator Password entered for the authentication purpose appears as "" on the display. 2.7.1 Changing the Administrator Password 2 Note Do not leave the machine with the setting screen of Admin. Settings left shown on the display.*

@@@@Call the Security Settings to the screen from the control panel. Press the [,] key to select [Admin. Password]. 1 2 3 4 Press the [Menu/Select] or [)] key. Press the [+] and/or [,] key to enter the currently set 8-digit Administrator Password. Press the [*] key to delete the last character entered. 8650 2-20 Administrator Operations 2 5 Press the [Menu/Select] key. What if an Administrator Password different from that is currently registered is mistakenly entered? % If there is a mismatch between the currently registered Administrator Password and the Administrator Password entered, a message appears that tells that there is a mismatch in the Administrator Passwords. Enter the correct Administrator Password. ? % If the EnhancedSecurity is set to [ON], entry of a wrong password is counted as unauthorized access.

If a wrong Administrator Password is entered a predetermined number of times (once to three times) set by the Administrator of the machine, the Utility screen appears and the machine is set into an access lock state.

To cancel the access lock state, settings must be made by the Service Engineer; or, turn off, and then turn on, the main power switch of the machine. If the main power switch is turned off and on, the access lock state is canceled after the lapse of time set for [Release Time Settings]. When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. If there is no wait period between turning the main power switch off, then on again, the machine may not function properly. 6 Press the [+] and/or [,] key to enter the new 8-digit Administrator Password. Press the [*] key to delete the last character entered. 7 Press the [Menu/Select] key. ? What happens if the Administrator Password entered does not meet the requirements of Password Rules? % The Administrator Password entered will be cleared if it does not meet the requirements of the Password Rules. Enter the correct Administrator Password.

For details of Password Rules, see "Password Rules" on page 1-8. 8 To prevent entry of a wrong Administrator Password, press the [+] and/or [,] key to enter the new 8digit Administrator Password once again. Press the [*] key to delete the last character entered. 9 Press the [Menu/Select] key. ? What happens if there is a mismatch in the Administrator Passwords? % If there is a mismatch in the Administrator Passwords, the Administrator Password entered the second time is cleared.

Perform steps 8 and 9 once again to enter the correct Administrator Password. 8650 2-21 Administrator Operations 2 2.8 Protecting Data in the HDD When access by the Administrator of the machine from the control panel through the Admin. @@@@@@@@@@Select this function if a greater effect of encryption is desired. @@@@Try to change the password at regular intervals.

@@@@@@@@Further, the HDD has the following function. @@Leak of data can thus be prevented. @@@@@@@@@@Do not leave the machine with the setting screen of Admin. Settings left shown on the display. @@@@Call the Security Settings to the screen from the control panel. @@@@@@% The HDD Lock Password entered will be cleared if it does not meet the requirements of the Password Rules. Enter the correct HDD Lock Password. For details of Password Rules, see "Password Rules" on page 1-8. % To change the HDD Lock Password, see "Changing the HDD Lock Password" on page 2-25. 8 To prevent entry of a wrong password, press the [+] and/or [,] key to enter the 20-digit HDD Lock Password once again.

Press the [*] key to delete the last character entered. 9 Press the [Menu/Select] key. ? 10 What happens if there is a mismatch in the HDD Lock Passwords? % If there is a mismatch in the HDD Lock Passwords, the HDD Lock Password entered the second time is cleared. Perform steps 8 and 9 once again. Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch. 2 Note NEVER forget the HDD Lock Password set through the above procedure. The HDD Lock Password must be entered when changing canceling the HDD Lock Password. 8650 2-24 Administrator Operations 2 2.8.

2 Changing the HDD Lock Password 2 Note When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. @@Do not leave the machine with the setting screen of Admin. Settings left shown on the display. @@Settings. <Setting can be made only from the control panel> 0 To call the HDD Lock Password register screen to the display, see steps 1 through 5 of "Setting the HDD Lock Password" on page 2-23.

Call the HDD Lock Password register screen to the display from the control panel. Press the [+] and/or [,] key to enter the currently registered 20-digit HDD Lock Password. 1 2 Press the [*] key to delete the last character entered. 3 Press the [Menu/Select] key. ? 4 What happens if there is a mismatch in the HDD Lock Passwords? % If there is a mismatch in the HDD Lock Passwords, a message appears that tells that there is a mismatch in the HDD Lock Passwords. Enter the correct password. Press the [+] and/or [,] key to enter the new 20-digit HDD Lock Password. Press the [*] key to delete the last character entered. 5 Press the [Menu/Select] key. ? What happens if the HDD Lock Password entered does not meet the requirements of Password Rules? % The HDD Lock Password entered will be cleared if it does not meet the requirements of the Password Rules. Enter the correct HDD Lock Password. For details of Password Rules, see "Password Rules" on page 1-8. 8650 2-25 Administrator Operations 2 6 To prevent entry of a wrong password, press the [+] and/or [,] key to enter the 20-digit HDD Lock Password once again. Press the [*] key to delete the last character entered. 7 Press the [Menu/Select] key.

? % 8 What happens if there is a mismatch in the HDD Lock Passwords? If there is a mismatch in the HDD Lock Passwords, the HDD Lock Password entered the second time is cleared. Perform steps 6 and 7 once again. Make sure that a message appears prompting you to turn OFF and then ON the main power switch. Now, turn OFF and then turn ON the main power switch. 2 Note NEVER forget the HDD Lock Password set through the above procedure. The HDD Lock Password must be entered when changing canceling the HDD Lock Password. 8650 2-26 Administrator Operations 2 2.8.3 Setting the Encryption Key (encryption word) 2 Note When the main power switch is turned off, then on again, wait at least 10 seconds to turn it on after turning it off. @@Do not leave the machine with the setting screen of Admin.

Settings left shown on the display. @@Settings. <Setting can be made only from the control panel> 0 For the procedure to call the HDD Settings menu to the display, see steps 1 through 3 of "Setting the HDD Lock Password" on page 2-23. Call the HDD Settings to the screen from the control panel. Press the [,] key to select [HDD EncryptionSet].

1 2 3 4 Press the [Menu/Select] or [)] key. Press the [+] and/or [,] key to enter the new 20-digit Encryption Key. Press the [*] key to delete the last character entered. 5 Press the [Menu/Select] key. ? What happens if the Encryption Key entered does not meet the requirements of the Password Rules? % The Encryption Key entered will be cleared if it does not meet the requirements of the Password Rules.

Enter the correct Encryption Key. For details of Password Rules, see "Password Rules" on page 1-8. % To change the Encryption Key, see "Changing the Encryption Key" on page 2-30. 8650 2-27 Administrator Operations 2 6 To prevent entry of a wrong Encryption Key, press the [+] and/or [,] key to enter the 20-digit Encryption Key once again.