Security Guide:

For the safety use of Digital Multifunction Printer (Digital MFP)

Version 1.1

January 10, 2018

Security Measures for Introduction

Ensure the following settings before introducing a product.
These settings will be a foundation of operating the product safely.

● Set secure administrator password for Kyocera Device

It is necessary to change the factory default password setting when deploying the Kyocera device on the network. Not performing these task could pose a security risks such as falsely or malicious changes to user registration information, network settings, contents of address book, or text data, etc. In order to prevent unauthorized access to MFP and ensure to setting will not be changed, first revise the device's administrator passwords. The administrator has the ability to utilize upper, lower case letter, numbers and special character up to 64 characters string logins, the logins are tracked in a log file and if multiple failed attempts to access the MFP are detected the Kyocera device can be set to lock-out (for a set time) users and the attack will be reported.

● Set the Command Center RX （Web browser) Administrator Password

Beyond the device administration password you have the ability to change the Command Center RX (Web browser) administrator password. Failing to apply the administrator's unique password will facilitate the same security risk as access as with the devices login with the possibility of unauthorized remote access to MFP and it's processing and communication over network.

● Deploying your device inside your network behind your Firewall

Do not connect MFP to the internet directly, but set it under the environment where the network is protected from outside accesses by installing firewall or secure modem. If connected to the internet directly, risks of illicit remote control or information leakage will be increased. In order for the safe operation of MFP, ensure to install Firewall, etc.

Network Protection

Kyocera devices will work optimal on your network when configured with a network scheme and IP address that allow all users and administrators access and management capabilities

● Setting Encrypted Transmission (SSL/TLS Transmission Protocols)

With enabling SSL/TLS, communication encryption it will protect information during transmission from leakage or data falsification, SSL/TLS is utilized during IPPS printing or when sending e-mails from the MFP. In SSL/TLS transmission, the TLS version and cryptographic method (cryptographic algorithm) can be set. It is recommended that stronger version of algorithms or cryptographic algorithms like TLS1.2, AES, etc be activated and not activated unused TLS versions or cryptographic methods. Also for device certificate to be used in SSL/TLS transmission, not only a self-issued certificate, but also certificates authorized by Certificate Authority can be imported and utilized.

SSL/TLS transmission can be configured in the following protocols.

- IPP over SSL
- POP3 over SSL
- SMTP over SSL
- FTP over SSL
- DSM over SSL
- eSCL over SSL
- HTTPS
- LDAP over SSL
- Enhanced WSD over SSL
- REST over SSL

● Setting Encrypted Transmission (IPsec Transmission)

IPsec transmission encrypts transmission by IP packet allowing transmissions to be encrypted without relying on an applications software or network architecture to protect the information from leakage or data falsification. Also if IPsec is enabled, information terminals to communicate the MFP can be restricted. In IPsec, IKE standards of authentication can be set. The values to be used will be set to match with customers environment. All Authentication method support pre-shared keys or certificates.

● IEEE802.1xCertification

IEEE802.1x is a certification standard to be used for network connections. In network environments where IEEE802.1x is enabled, the connection can be set to allow only terminals that are certified in advance by

enabling IEEE802.1x of a Kyocera MFP to equal your environment, Architecture can be configured to restrict all other network environments.
IEEE802.1x can support the following cryptographic methods.

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- PEAP(EAP-MS-CHAPv2)

● SNMPv3

SNMP is a protocol which obtains Kyocera device information through network the network connection and is designed to manage the fleet of MFPs. When SNMPv3 is enabled, this SNMPv3 protocol transmission is encrypted so that it can protect information from leakage.

● IP Address Filtering

When IP address filtering is enabled, terminals to communicate to MFP can be restricted to terminals with certain IP addresses only. For example, if restriction of MFP users should be set to PCs of a certain department or group, access from users not belonging to these departments or groups can be denied by enabled IP address filtering.

● Blocking Unnecessary Protocols (Ports)

MFP supports many transmission protocols. If these transmission protocols are left enabled without being set secure enough, the system might be attacked by Port Scan or unauthorized access. Ensuring to disable unused transmission protocols and closing ports are recommended.

Protection of User Data

Data Protection for Device

In HDD/SSD mounted inside MFP, user information including scanned image data, pre-printed image data, user registration information, or address book are stored. To protect these data, the following features are implemented.

● Encryption of HDD/SSD (Data Security Kit)

This is to encrypt data to be stored in HDD/SSD to protect them. By doing so, interpreting data is impossible even they are connected to an analysis tool of PC, e.t.c. Encryption Algorithm adopts AES 256bit. In order to enable HDD/SSD encryption feature, Data Security Kit Option is required.

● Erase all processed data (Data Security Kit)

Image data is temporarily stored in the system when copying or scan job is processed in MFP. After completion of the job the information is erased completely with overwriting of meaningless data after, the risk of data access is eliminated. In the overwriting method, either 3 times (DoD method) or once is selectable. At the default setting, 3 times is set. In order to enable Overwriting unnecessary data feature, Data Security Kit Option is required.

Print Data Protection

● Private Print

When enabling the Private Print feature in the Kyocera Printer Driver a password (pin code) can be set for the print data. With this setting, the pin code should be entered at the MFP operation panel of the device and the stored job will be released. This feature will help meet compliance for prohibited taken-away of printed sensitive information or incidental glances at printed pages.

● Stamp

Because printed copies from MFP are physically papers, there is a risk of information leakage caused by malicious persons who illegally copy them. With this function, a custom notification stamp can be placed on all printed pages ensuring that publisher source can be traced by the identifying information in the stamp even after they are multiple generation of the information from copies or circulation. The stamp may also deter the creation of illegal copies.

Protection of Transmitted Data

● Encrypted Transmission

Encrypting protocols with SSL/TLS, when sending scanned information, the function can protect from data leakage, e.t.c., caused by wire-tapping. Encrypted transmission should be set by protocol for sending scanned information. (More detail under network protection section)

● Encryption PDF

An Encrypted PDF Files enables you the ability to send an encrypted PDF that requires the recipient to utilize a password to view the information. This feature can be as easy as selecting adding a password scanning the information and sending or storing. By setting a password, information leakage or falsified data can be prevented in case of the PDF file is circulated to the public or sent to an incorrect destination.

● Prevention of Erroneous Fax Transmissions

A critical information leakage might occur when sending information/data to a wrong Fax destination unintentionally. In order to prevent this accidental data leakage caused from erroneous transmission destinations you are prompted to enter the phone number 2 times to ensure they match you need to enable Erroneous Transmission Prevention Function.
For this function, the following can be set.

- Urging to check the destination before transmitting data.
- Necessitating to enter the destination twice.
- Prohibiting broadcast transmission.
- Prohibiting direct input and ten-key input.
- Prohibiting redialing.

● Fax Sending Limit

Fax destination can be restricted to designated addresses only. With this feature, devious or erroneous fax transmission can be prevented.

User Authentication/Access Control

User Authentication

The user authentication feature, allows administrators to manage users activity on the MFP and identify all activity. IT management can allow authorized users to be registered for access. There are two methods to authenticate; local authentication and network authentication, and both of them can be used concurrently. Also this function not only allows to identifying users but also linking integrates with Job Accounting, Management such as limiting the number of pages to be used or access to MFP functionality.

● Local Authentication/Network Authentication

Local Authentication is a certifying method of identifying authentication following user information registered in MFP. In local authentication, detailed user management is possible locally or remotely from management tools. Network authentication is a certifying method of identifying authentication linking with an existing authentication servers such as Kerberos, Active Directory, e.t.c. . Both local and network authentication can utilize pin codes or card reader technology, furthermore, there is a 2-step certifying method using a card and password combination.

● User Account Lockout

if ever inside your network a brute-force attack occurs to eliminate any chance of user account access to information you can enable the Account Lockout feature with which a login ID can be locked out for a certain period if a certain number of attempts to log on to an account fail. The number of failures or time duration for freezing the account can be set freely. Also the brute-force attack is often conducted via network, therefore, account log-in subject to Lockout can be optioned either from network only or all log-ins including from an operation panel set for local authentication.

● Password Policy

Network Authentication password should have been set by your Administration and meets your minimum length of the password or complexity of the password these are set in advance. Password Policy can be set for local authentication method.

Access Control

With Access Control, data stored in MFP or the use of MFP can be controlled for identified users. By setting access permission scope depending on a user's role, information leakage by an internal crime or a human error can be prevented.

● Document Box

Creating document boxes in HDD/SSD mounted on a MFP, scanned data or printed data can be stored in it. The document box can have an owner and a password on it to prevent any access from a malicious user.

● Authorization Settings

Utilization limit to copy, print, transmission of scanned data, FAX, Box storage, external memory storage features can be set for each user through authentication. By limiting usage functions, illicit taken-away of information or information leakage by a human error can be prevented.

Limiting functions/Preventing Illicit Usage

Limiting Each Function/Preventing Illicit Usage

As MFP has various features, execution of each feature, edit of settings, or reference authority can be set in detail.

Also, in order to prevent from illicit usage of a device, locking an operation panel and disabling USB port are also feasible.

● Setting Edit Authority for Address Book

Setting for edit authority for address book can be set. There are two ways of setting authority; one is only for an administrator, and another is for all users.

● Setting Reference Authority to Job Status/History

Users to have reference authority for job status or job history can be set. There are 3 ways to give reference authority; one is only to an administrator, another is to an administrator and an owner of the job, but limiting to his jobs only, and the other is to all users.

● Operation Panel Lock

Limiting settings that a user can operate from a panel is configurable. By using Operation Panel Lock, operation of these settings is only permitted to an administrator. The settings in the following scope can be possible for Panel Lock.

- Panel Lock: ON (To lock every target setting)
  - All operations on system menu are limited.
    For a partial limit, use the following Partial lock function.
- Partial Lock 1
  - Network settings, system settings, or document box settings are limited.
- Partial Lock 2
  - In addition to the limit of [Partial Lock 1], panel settings, printer settings, and settings related to job execution are limited. (For example: Use of a stop key, or Job cancellation, e.t.c.)
- Partial Lock 3
  - In addition to [Partial Lock 2], settings related to paper are limited. (For example: Cassette settings or MP tray settings, e.t.c.)

● Interface Block

In order to prevent information leakage by illicit uses of USB port mounted in a device, USB port can be disabled (blocked). Because USB port is used in various usage, disabling or blocking is set according to usages.

- USB device
  - This is a local port to connect PC/Mac and MFP and to be used for printing. Blocking USB device, local port connection is disabled.
- USB Host
  - This is a port to be mounted for USB memory (USB storage), and to be used for direct printing for a file stored in USB memory, or storing scanned data directly into USB memory. This port can also be used by installing USB key boards or IC card readers. Blocking USB Host, all these connections are disabled.

    Disabling USB Host, information leakage from illicit uses of USB port can be prevented.
- USB Storage

  Only USB memory (USB Storage)-related functions can be disabled among other feasible functions with USB Host. Blocking USB Storage, the use of USB key board or IC card reader can remain possible while the connection of USB memory is disabled.

● Audit Log (History Settings)

Audit logs are obtained from MFP or execution can be reported via e-mail as audit logs. Events for this Audit logs are login/log-out, job execution, user information or box information registration, or security-related values settings. Logs obtained can be transmitted to a specified e-mail address. By looking into audit logs, illicit operation can be traced later. In audit log settings, enable/disable, recipient e-mail address, and the number of logs for a transmission can be set in the following scope.

- Job Log History
- Login history
- Device Log history
- Security Communication Error Log history

Security when Device to be disposed

● Initialization

Past settings can all be formatted to default settings. It is recommended that settings in the past be formatted to default before disposing a device.

● Sanitization

If a device is disposed with remaining user information in HDD/SSD mounted in the device, HDD/SSD can be analyzed and exposed to a risk of reading information inside. In Sanitization function, user information is overwritten with meaningless information to erase the information completely. Furthermore, settings in a device are all formatted to default and the result is output by report. The Sanitization function can set execute time. It is recommended that Sanitization be executed before disposing a device.

Kyocera on devices with hard drives offers **End of Life Sanitization** with advance configurations

Features listed below:

1. Set sanitization by calendar date for end of lease or life
2. Auto-Generate an e-mail to the administrators indicating the sanitization process has started
3. 3 times overwrite with low level format.
4. Creates a Printed Certificate at the completion of the Sanitization process
5. Permanently indicates in Display that Sanitization Mode was performed
6. Disables the MFP from further use
7. Reactivation of formatted MFP for Lease returns is only possible by authorized Kyocera Technician

Completely erases all memory and systems on the MFP

KYOCERA Document Solutions Inc.

1-2-28 Tamatsukuri, Chuo-ku, Osaka 540-8585, Japan
Phone: +81-6-6764-3555

http://www.kyoceradocumentsolutions.com

The information contained in this document is accurate and current as of December 2017 and is subject to update without prior notices.