



**BMLinkS**  
**Security White Paper**  
**Version 1.0.0**  
**May 20, 2008**

### **Disclaimer**

JBMIA offers the information in this document to all BMLinkS users as a reference only and does not make any warranty or guarantee concerning the accuracy of the information contained herein.

Consequently, in the event of any problem (including but not limited to security problems) resulting from the use or application of the information contained in this document, JBMI A assumes no responsibility whatsoever, including but not limited to warranty or indemnity obligations, and provides none to the user.

### **Trademarks**

- Product names and brands are the trademarks or registered trademarks of their respective companies.
- BMLinkS and the BMLinkS logo are registered trademarks of the Japan Business Machine and Information System Industries Association.

### **Copyright**

- The Japan Business Machine and Information System Industries Association holds the copyright to this document.
- Reproducing or copying this document, in whole or in part, is prohibited without the express written consent of the copyright holder.

# Contents

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>4</b>
1.1.	OBJECTIVE OF THE WHITE PAPER.....	4
1.2.	TARGET AUDIENCE OF THE WHITE PAPER.....	4
<b>2.</b>	<b>WHAT ARE THE SECURITY THREATS TO OFFICE DEVICES? .....</b>	<b>5</b>
2.1.	DATA THEFT AND MODIFICATION OF DATA COMMUNICATED OVER NETWORKS .....	5
2.2.	DATA INTERCEPTION AND FALSIFICATION THROUGH USER SPOOFING .....	5
2.3.	DATA INTERCEPTION AND FALSIFICATION THROUGH SERVER SPOOFING .....	5
2.4.	THEFT OR FALSIFICATION OF DATA IN NONVOLATILE MEMORY .....	6
2.5.	SCREEN SPYING OF PASSWORDS DURING ENTRY .....	6
2.6.	THEFT OF PRINTED INFORMATION .....	6
<b>3.</b>	<b>BMLINKS SECURITY EFFORTS.....</b>	<b>7</b>
3.1.	COMMUNICATION ROUTE ENCRYPTION .....	8
3.2.	USER AUTHENTICATION .....	8
3.3.	SERVER AUTHENTICATION.....	8
3.4.	ACCESS RESTRICTIONS ON CONFIGURATION DATA .....	9
3.5.	PROTECTION OF DATA IN NONVOLATILE MEMORY .....	9
3.6.	ACCESS RESTRICTIONS ON ASSET DATA.....	9
3.7.	PREVENTING SCREEN SPYING WHILE ENTERING DATA .....	10
3.8.	PRINT SECRET FUNCTION.....	10
<b>4.</b>	<b>USING BMLINKS SECURITY FUNCTIONS .....</b>	<b>11</b>
4.1.	PRINT SECRET FUNCTION.....	11
4.2.	ENCRYPTED NETWORK CONNECTION FOR STORAGE SERVICES .....	13
<b>5.</b>	<b>OPERATION OF BMLINKS SECURITY FUNCTIONS.....</b>	<b>14</b>
<b>6.</b>	<b>SUMMARY .....</b>	<b>16</b>
<b>7.</b>	<b>REFERENCES AND LINKS.....</b>	<b>17</b>

# 1. Introduction

---

## 1.1. Objective of the White Paper

Accompanying the prevalence of information devices, a concern among the public is increasing, for example security breaches and information theft via networks make headlines in newspapers. The functionality of multifunction devices goes beyond that of just copiers, printers, and scanners; multifunction devices are equipped with the functionality of information devices. BMLinkS is part of this trend.

In response to these changing circumstances, we are coping with security issues by setting security criteria for BMLinkS devices so that users can make use of BMLinkS services securely and with peace of mind.

This white paper aims to give a clear description of our efforts in the security arena.

## 1.2. Target Audience of the White Paper

This white paper was written for administrators considering the adoption of BMLinkS devices and general users who use BMLinkS devices.

## 2. What are the Security Threats to Office Devices?

---

As is reported in newspapers and elsewhere, information leaks are often the result of attackers exploiting security weaknesses inside organizations. Thus, security considerations are essential even in offices with tight access controls.

Administrators and users must, at the very least, keep the following threats in mind each time they use office devices.

Note that these threats are not specific to BMLinkS alone; they apply generally to all office devices.

Nevertheless, awareness of these threats is needed, as BMLinkS devices are also office devices.

### 2.1. Data theft and Modification of Data Communicated over Networks

There is a danger that attackers will intercept (packet sniffing) data being communicated over networks between client computers and office devices and stealing client document data, address books, logs and other security management information, and communicated passwords. Data may also be tampered with or falsified.

### 2.2. Data Interception and Falsification through User Spoofing

There is a danger that attackers will impersonate registered users or administrators (user spoofing) to gain authorization to office devices and intercept client document data, address books, logs and other security management information, and communicated passwords. Data may also be tampered with or falsified.

### 2.3. Data Interception and Falsification through Server Spoofing

There is a danger that attackers will intervene as a third party while a client computer and an office device is authenticating connection legitimately and communicating with each other. There is a danger that attackers will intervene as a third party while client computers and office devices perform legitimate connection authentication operations or communication operations in network communications. and, by spoofing as a server (server spoofing), will steal client document data, passwords, or other information or else tamper with or falsify data.

## **2.4. Theft or Falsification of Data in Nonvolatile Memory**

There is a danger that attackers will steal client document data, address books, logs and other security management information, and configuration settings (passwords, server certificates) or else tamper with or falsify data that are stored in nonvolatile memory (hard disks, flash memories, etc.) in client computers and office devices.

## **2.5. Screen Spying of Passwords During Entry**

There is a danger that attackers will surreptitiously read passwords from the screen while the user is entering them on an office device.

## **2.6. Theft of Printed Information**

There is a danger that attackers will walk off with information that the user has printed at an office device.

## 3. BMLinkS Security Efforts

---

BMLinkS defines the user assets that BMLinkS devices should protect to counter the general security threats, described in the previous chapter, to office devices and defines the security functions that BMLinkS devices should implement to protect the availability, integrity, and confidentiality of those assets.

Beyond this, BMLinkS provides detailed provisions on security functions BMLinkS devices implement to maintain common security, operability, and connectivity between office devices produced by multiple vendors.

BMLinkS defines **client document data** that is communicated between BMLinkS devices and/or stored on BMLinkS devices and **address books** and logs that are kept on BMLinkS devices as user assets that should be protected.

BMLinkS also takes into consideration maintaining **asset-protection functions**, as changing a BMLinkS device's settings, for instance, may disable the security functions of the device and, thus, circumvent asset protection.

This chapter describes the measures for dealing with each of the security threats mentioned in Chapter 2. The table below indicates the correspondence between the threats and the protective measures.

Security Threat	Protective Measure
2.1. Theft and modification of data communicated over networks	3.1. Encryption over the wire
2.2. Data interception and falsification through user spoofing	3.2. User authentication
2.3. Data interception and falsification through server spoofing	3.3. Server authentication 3.4. Access controls on configuration data
2.4. Theft or falsification of data in nonvolatile memory	3.4. Access restrictions on configuration data 3.5. Protection of data in nonvolatile memory 3.6. Access restrictions on asset data
2.5. Screen spying of passwords during entry	3.7. Preventing screen spying while entering data
2.6. Theft of printed information	3.8. Print secret function

## 3.1. Communication Route Encryption

BMLinkS defines encryption of communication routes in an effort to counter the threat of data theft and/or modification communicated over networks. There are many communication route encryption standards in use today, including SSL, TLS, IPSec, and WEP (for wireless communications).

Of these technologies, BMLinkS stipulates the use of TLS Ver. 1.1 (RFC 4346), the most widely used technology at present. BMLinkS also stipulates that encryption strengths be equivalent to or stronger than the standards listed below.

- Asymmetric key encryption algorithm: RSA algorithm
- Symmetric key encryption algorithm: TripleDES
- Hash algorithm: SHA-1

BMLinkS also recommends the additional encryption schemes given below, but this is not meant to restrict the encryption schemes that individual vendors may support.

- Symmetric key encryption algorithm: AES
- Hash algorithms: SHA256, SHA384, SHA512

These encryption schemes are subject to periodic criteria reviews.

## 3.2. User Authentication

Authenticating the identity of users has tremendous significance to security considerations. Identifying a user permits the selection of assets that only that particular user can use.

As an extension to the specification, BMLinkS stipulates the inclusion of user authentication functions in an effort to counter the threat of data intercepting and/or modification by spoofing as a certain user. The practical specifications for these functions vary between device vendors and models; however, the recommendations for these functions are as follows:

- User authentication must be performed before any operation connected to a BMLinkS service.
- Authentication passwords must be at least eight characters long.

On some of the BMLinkS services, authenticated users are by definition able to use all functions of the service because of the priority on convenience. Therefore, should accessible assets on a per-user basis be defined, it will be necessary to launch a separate instance of the same service for each user.

## 3.3. Server Authentication

As an extension to the specification, BMLinkS stipulates the inclusion of functions that perform server authentication each time SSL/TLS communications are established to counter the threat of data theft and/or modification through server spoofing on a network. The practical specifications for these functions vary between device vendor and model; for details, refer to the manual of other documentation for your particular device.

### **3.4. Access Restrictions on Configuration Data**

To counter the threats of data theft and/or modification through server spoofing or of stealing and/or falsifying data in nonvolatile memory, BMLinkS stipulates that only administrators, who are distinguished from ordinary users, can access the configuration settings of a service.

To operate BMLinkS-provided services securely, administrators of BMLinkS devices should ensure that all functions are set correctly and that administrator passwords are changed from their default settings to keep them unknown from other people.

### **3.5. Protection of Data in Nonvolatile Memory**

To counter the threat of stealing and/or falsifying data in nonvolatile memory, BMLinkS stipulates the protection by some means of data saved in nonvolatile memory.

While there are various conceivable protection schemes — such as encrypting the entire nonvolatile memory or encrypting data before storing it in memory — BMLinkS recommends using encryption equivalent to or stronger than 128-bit AES. The actual data protection schemes used within the nonvolatile memory vary according to the device used.

### **3.6. Access Restrictions on Asset Data**

To counter the threat of stealing and/or falsifying data in nonvolatile memory, BMLinkS stipulates the ability to set appropriate access restrictions so that unauthorized users cannot reference, change, or otherwise access client document data, address books, logs, or other data assets. The actual access restriction schemes vary according to the device used.

### **3.7. Preventing Screen Spying While Entering Data**

To counter the threat of attackers surreptitiously reading data from the screen during an entry operation, BMLinkS stipulates the following protection methods when entering user IDs/passwords for service access.

- Entered characters are not echoed on the screen.
- If characters are echoed on the screen, they are disguised with asterisks or some other means.

### **3.8. Print Secret Function**

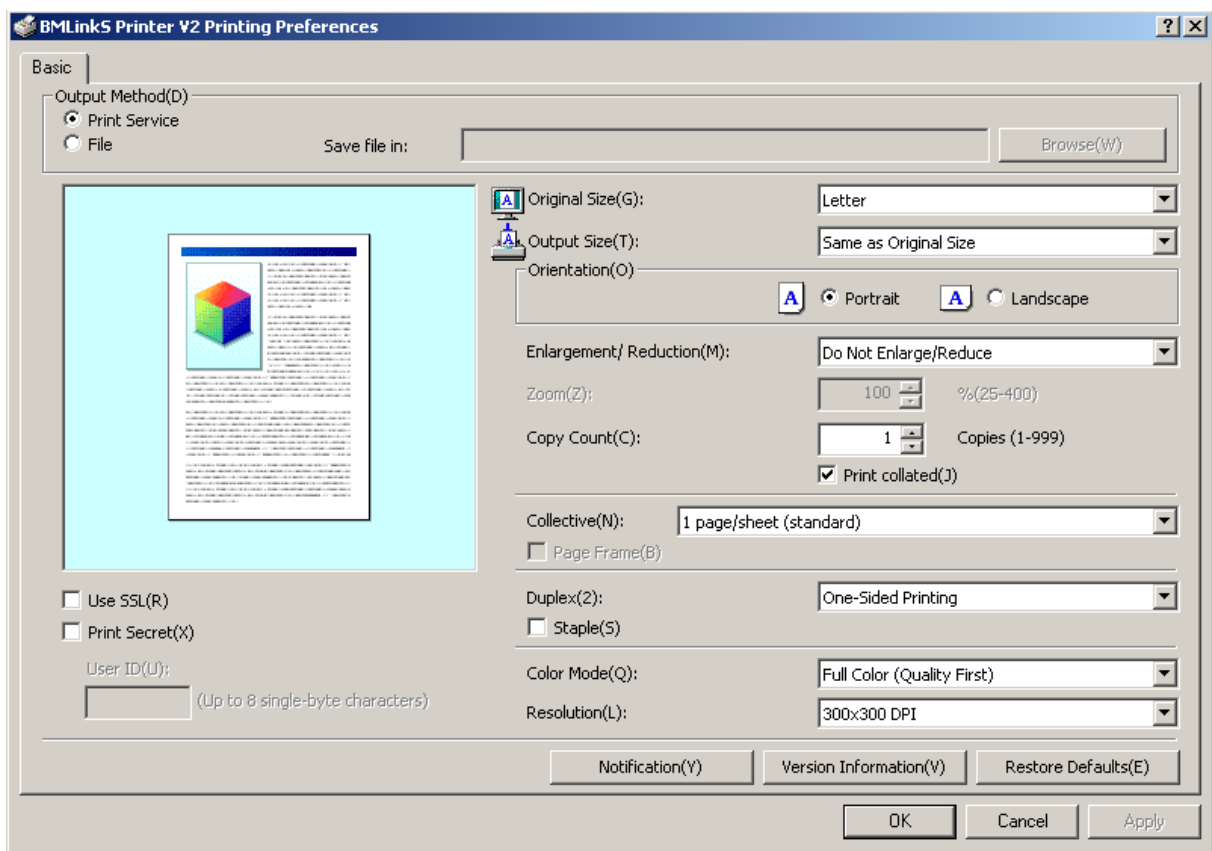
To counter the threat of attackers walking off with printouts of confidential information, BMLinkS stipulates a print secret function. Chapter 4, “Using BMLinkS Security Functions,” provides a description of the print secret function.

# 4. Using BMLinkS Security Functions

## 4.1. Print Secret Function

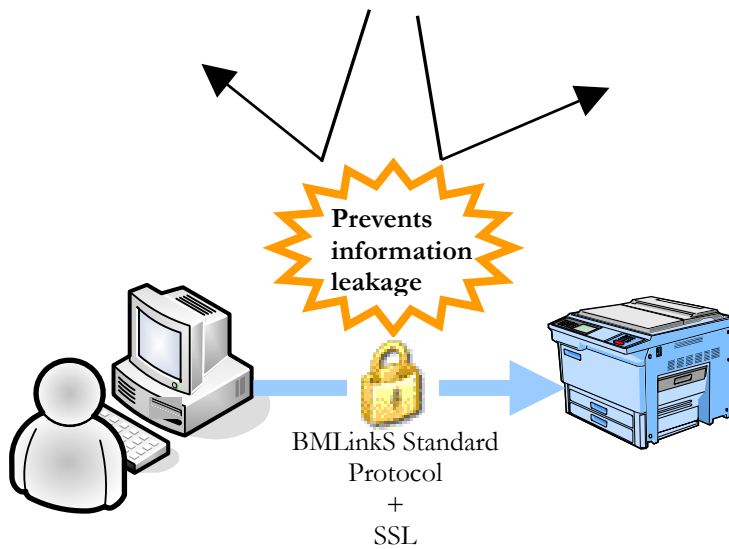
BMLinkS stipulates a print secret function, in addition to the ordinary printing method, to serve users seeking stronger security levels.

The diagram below is the print setup dialog for the BMLinkS standard printer driver.



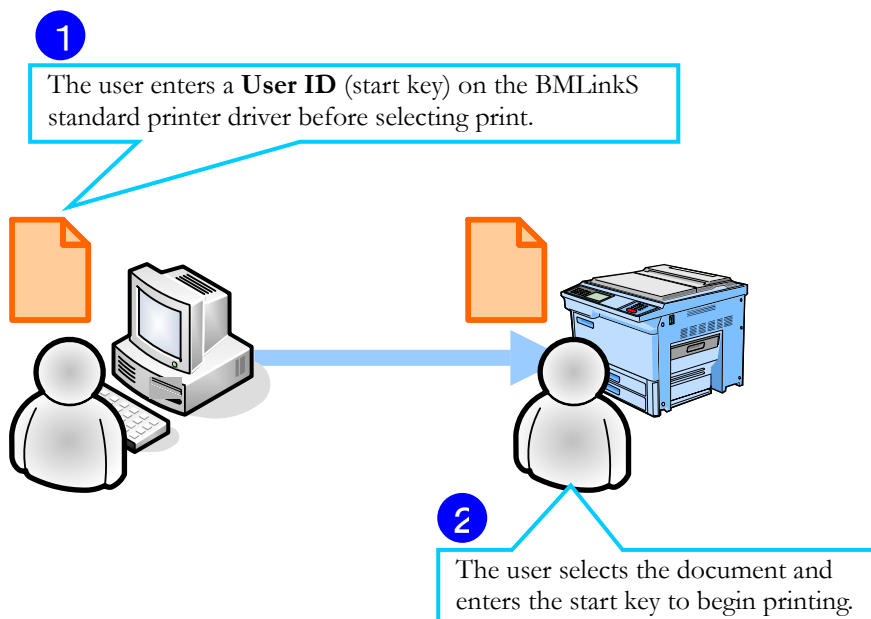
### Use SSL

For BMLinkS devices that support SSL communications, checking **Use SSL** at the bottom left of the driver window will encrypt network print communications between the print client and the destination BMLinkS device. This enables the user to protect print documents against the threat of unauthorized persons illegally obtaining print document data through network snooping.



*Print Secret*

Printing with Print Secret checked will temporarily store the print data on the BMLinkS device. Actual printing will not begin until the user enters the start key on the panel of the BMLinkS device. This function prevents unauthorized persons from walking off with unattended print results.



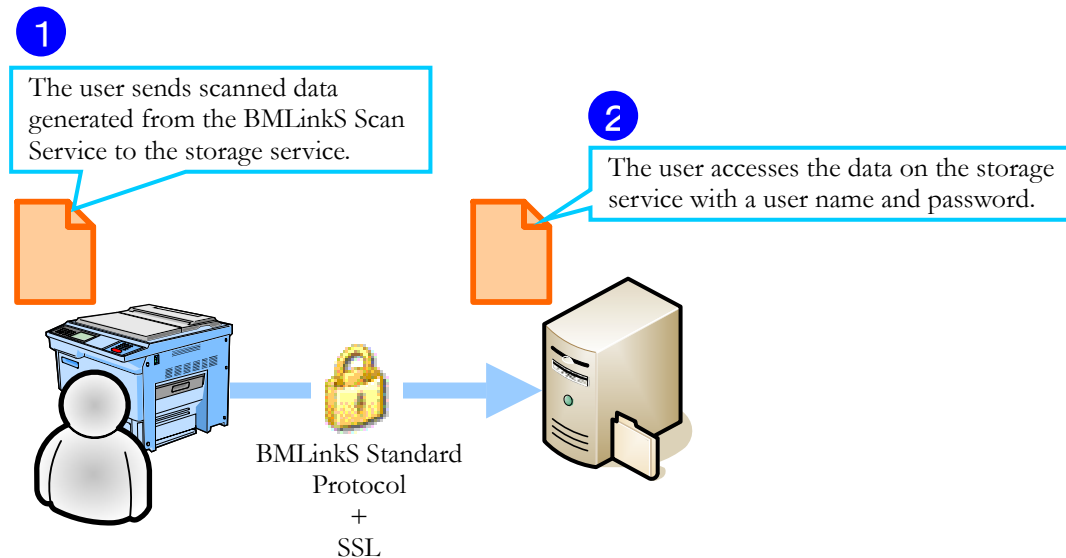
1. The user enters a **User ID** (start key) on the BMLinkS standard printer driver before selecting print.
2. The user selects the document and enters the start key to begin printing.

Note that print secret and SSL encryption are optional. Ask the manufacturer of your BMLinkS device whether these options are supported.

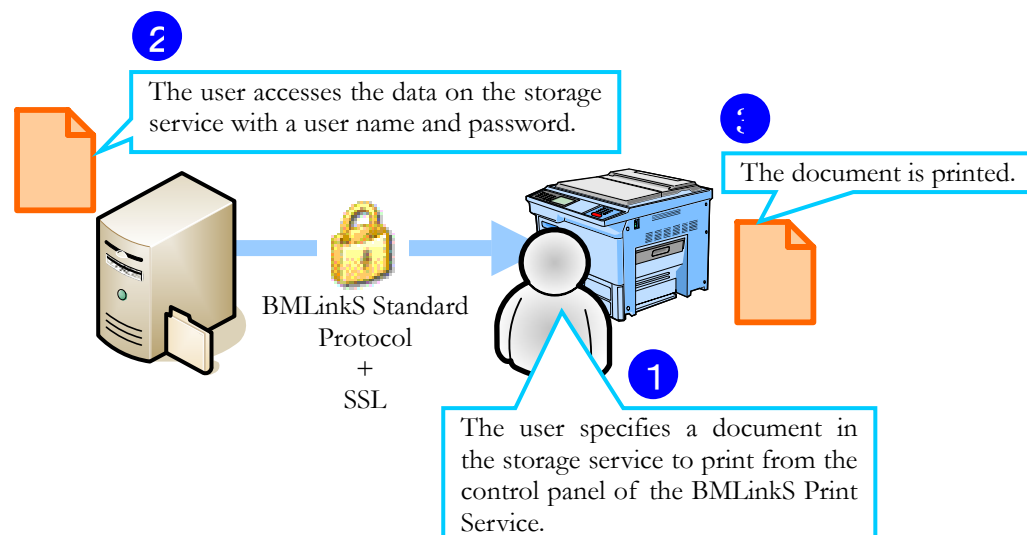
## 4.2. Encrypted network connection for Storage Services

Storage services are software packages that provide BMLinkS Storage Service functionality on user computers. Running storage services on a computer provides the following functionality.

1. Store scanned data from a BMLinkS Scan Service on the computer's hard disk (network storage)



Print client document data stored on the computer's hard disk from the control panel of a BMLinkS device (stored document printing)



Note that storage service SSL encryption is optional. Ask the manufacturer of your BMLinkS device whether this option is supported.

# 5. Operation of BMLinkS Security Functions

---

To ensure connectivity and data exchanges between office devices, a robust security management is required not only in BMLinkS devices but also in the surrounding office environment. BMLinkS has dramatically enhanced network communication for the connectivity and security.

## *Assumptions about Operating Environments*

Although BMLinkS devices are equipped with basic security functions, it is assumed the operating environment takes care of certain security aspects as well. Please pay attention to the following security matters when using BMLinkS devices.

The security functions of BMLinkS devices are defined on the assumption that the networks and environments to which BMLinkS devices are connected to are controlled and well managed. (Without this assumption, it would be necessary to design and install a great number of security functions in BMLinkS devices, which in turn would require more computer resources and physical equipment. We have chosen not to go down this path with BMLinkS because of concern that the extra security functions would inflate device prices and compromise device functionality.)

When connecting a device to a network, please be aware of what devices are connected to the network and what devices you are connecting. It is also important to have a rule that only devices approved by the network administrator can be connected to the network.

Please locate servers running BMLinkS storage services in an access controlled room and take steps to prevent the theft of hard disks and other nonvolatile memory devices. Also consider whether you may need to encrypt the data on hard disks or other nonvolatile memory devices.

## *Operation of Server Certificates*

We recommend encrypting network communication with SSL/TLS for communications between clients and BMLinkS devices or among different BMLinkS devices.

SSL/TLS communications make use of server certifications installed on BMLinkS devices. Please use trusted server certificates for your operating environment. You may use the self-signed certificates from BMLinkS devices as server certificates, but in this case you should add the server certificates to the client's trusted certificate list.

## *Recommendation of User Authentication*

User authentication is defined as an extension to the BMLinkS device functions, and as such it is possible to set BMLinkS devices so that user authentication is not required. (For example, BMLinkS storage services.) Nevertheless, in view of security concerns, we strongly encourage the enabling of user authentication at

BMLinkS devices.

Because of the priority on convenience in BMLinkS-provided services, authenticated users are by definition able to use all functions of a service. Because of this, we recommend setting the operating environment so that separate instances of the same service are launched for each user. This provides a means of preventing users from accessing the document data of other users.

#### *Password Management*

Thought must also be given to the management of passwords used to authenticate users. Obviously users should not tell their passwords to other users or write passwords down where they can be easily found. Easily guessed passwords or very short passwords are also risky. We recommend using passwords that contain at least eight characters and that are a combination of letters, numbers, and symbols. We also recommend regularly changing passwords as even difficult passwords can be discovered through brute force attacks or other means. There is also the risk that others will see a password while it is being entered. Be sure to be aware of who is around you when entering passwords.

#### *Security Training*

Basic security training for users and administrators is effective in maintaining a secure operating environment regardless of whether BMLinkS devices are used or not. Although this repeats some of the material mentioned earlier, we recommend instructing BMLinkS device users and administrators on the following matters.

For general users:

- Use passwords that are at least eight characters long and contain numbers, letters, and symbols and that others cannot easily guess.
- Regularly change your passwords.
- Use the Print Secret function when printing confidential documents.

For administrators:

- Use passwords that are at least eight characters long and contain numbers, letters, and symbols and that others cannot easily guess.
- Regularly change your passwords.
- Configure BMLinkS devices properly to maintain their security.
- Regularly check the settings of BMLinkS devices.

#### *Recommendation of the Print Secret Function*

We recommend using the Print Secret function with BMLinkS print services. With the Print Secret function, printing will not begin at the BMLinkS device until the user has entered a start key. This avoids the risk of information disclosures because printed documents were stolen or left unattended.

## 6. Summary

---

In this document, we have described the efforts to add security to BMLinkS as well as the usage and operation of BMLinkS security functions.

We first established security criteria, as discussed in Chapter 3, and then did a security assessment of the BMLinkS specifications based on this criteria. From this, we have been able to verify that the current specifications satisfy the established security criteria. We plan to conduct regular revisions of newly added functions and specifications.

We also plan to regularly review *assets*, *threats*, and *security measures* — the components of the security criteria themselves — based on worldwide developments in security standards and on the latest security technology trends, particularly in encryption algorithms and schemes.

## 7. References and Links

---

- T. Dierks and E. Rescorla. RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1  
<http://www.ietf.org/rfc/rfc4346.txt>, April 2006.

BMLinkS Security White Paper Version 1.0.0

Feb. 21, 2008

Published by: BMLinkS Project Committee, Japan Business Machine and Information System Industries Association

NP Onarimon Bldg.,

3-25-33 Nishishinbashi, Minato-ku, Tokyo 105-0003, Japan

<http://www.jbmia.or.jp/bmlinks/eng/>

Unauthorized reproduction prohibited. © 2008 Japan Business Machine and Information System Industries Association

