

Product Security Guidelines

1. Introduction

1.1 Purpose

The purpose of this document is to indicate basic security measures for safely installing, configuring, operating, maintaining, and disposing of Totani bag-making machine and spout inserter products (hereinafter “Totani equipment”) that are meant to be implemented by users and administrators.

1.2 Intended Users

This document is written to be used in the implementation of security measures by the following types of personnel:

- Machine installation personnel
- Facility administrators
- Maintenance personnel
- IT/OT network administrators
- Operators responsible for bag removal, etc.

1.3 Scope

This document applies to the following Totani equipment and functions.

Equipment:

- Bag-making Machine/Spout Inserter main units
- HMI (operation panel, control panel, etc.)
- Control devices/controllers (computers, PLCs, etc.)
- Maintenance computers or service terminals
- Network devices connected to the bag-making machine or spout inserter
- Maintenance software

Functions:

- Network communication
- Data collection
- Remote maintenance
- Software updates

1.4 Disclaimers

The security-related information in this document is based on Totani's own analysis and investigations.

The most appropriate security measures differ depending on the customer's specific environment, and this document makes no guarantees that it can prevent all security-related damages to the customer environment.

Additionally, this document is intended to indicate the basics of safe and secure product use, not to specify the entirety of network designs, access control design, or internal operational rules in detail. Customers are asked to consider and implement the measures most suited to their own usage environment.

2. Prerequisites for Secure Use

Proper cybersecurity measures for Totani equipment require that the entire connected environment be properly protected, not just individual functions.

For that reason, customers are asked to use Totani equipment in an environment that satisfies the following requirements.

2.1 Installation Environment

- Install the equipment in an environment not easily accessible by personnel other than the intended users.
- Physically restrict access to operation panels, control cabinets, communication ports, USB ports, etc.
- Properly manage control cabinet keys, maintenance terminals, and configuration media.

2.2 Network Environment

- Do not directly connect Totani equipment to business IT networks or the internet.
- Isolate the Totani equipment network from other business networks.

2.3 Governance

- Establish a responsible administrator for each piece of Totani equipment.
- Configuration changes, software updates, and maintenance connections should only be performed by personnel with access privileges.
- Establish points of contact and response procedures in the event of equipment failure, abnormal communication, or authentication failure.

3. Security Support Period

The support period for product security is the five years from the acceptance date (until the same date in the same month five years later).

During the support period, the equipment will be issued security patches, software updates, etc.

4. Security Features

Totani equipment is equipped with the following types of security features that will protect the equipment and customer assets if used appropriately.

However, the features included differ depending on the specifications of equipment model and option package.

4.1 User Authentication and Access Controls

This feature is used to confirm the identity of users who perform operations or change settings.

It is intended to prevent unauthorized users from performing operations or changing settings.

There are three types of user privileges: Operator, Maintenance Technician, and Administrator.

Through these different roles, it is possible to restrict the ability of users to perform configuration changes and access maintenance functions and system information.

4.2 Logs

This feature creates logs to record logins, changes to settings including bag-making parameters, alerts, abnormal events, maintenance operations, etc.

Logs are used to investigate abnormalities, determine causes, and rapidly detect unauthorized activity.

4.3 Secure Communications Across Trust Boundaries

This feature protects communications with control devices, HMI, maintenance terminals, etc.

It is used to mitigate risk of unauthorized connections, sniffing, and falsification.

4.4 Configuration Protection

This feature restricts changes to important settings, saves configurations, performs backups, etc.

It is used to minimize the impact of incorrect configurations and unauthorized changes.

5. Initial Settings - Important Notes

If Totani equipment is used with the default settings it has immediately after initial setup, it is not secure. At the very minimum, the following actions are needed to ensure security.

5.1 Check Default Accounts

- Check for default accounts.
- Deactivate or delete unneeded default accounts.
- If there are default passwords in place, change all such passwords before putting the equipment into operation.

5.2 Password Configurations

- Do not use passwords that are easy to guess.
- Do not use equipment names, company names, model names, or sequential numbers.
- Do not use the same passwords for Administrator accounts, Operator accounts, and Maintenance Technician accounts.

5.3 Network Settings

- Only permit connections that are truly necessary.
- Do not use ports or protocols that are not needed for equipment operation.
- Ensure that the Administrator is able to see and monitor IP addresses and connection configurations.

5.4 Backups

- Ensure there is a secure place to store backup media.
-

6. Recommended Settings

The following settings are recommended for security purposes during operation.

6.1 Account Settings

- Avoid the use of shared accounts.
- Use accounts that enable you to identify individual user.
- Assign Administrator privileges only to those who need them.

6.2 Communication Settings

- Do not leave remote maintenance functionality turned on. Only enable it when necessary.
-

7. Everyday Operations - Important Notes

Once Totani equipment has been deployed for use in operations, continue to take the following steps at a minimum to ensure security.

7.1 Check on Usage Status

- Do not ignore alerts or abnormal messages. Report to an Administrator if necessary.

7.2 Check Logs

- Check the logs on a regular basis.
- If necessary, store logs in a manner that prevents tampering.
- If you notice any abnormal or suspicious activity, report to an Administrator.

- Check for unexpected logins or configuration changes.
- Check for suspicious connections, restarts, stops, etc.

7.3 Configuration Change Management

- Configuration changes should be carried out in accordance with approved procedures.
- Keep records of changes, both before and after.
- If you discover configuration changes that do not have a clear cause, investigate immediately.

7.4 Handling of External Media

- Do not connect USB memory, SD cards, or maintenance tools that have not been approved by Totani.
- Computers used for maintenance purposes must be managed in accordance with the customer's internal security rules, in addition to having the latest OS updates **applied** and being virus-checked with the latest definitions.
- If using external media, perform a virus check with the latest definitions before use.

7.5 Incident Response

- Promptly contact an Administrator if you notice any unusual behavior, unexpected screen displays, or unexplained stops.
- Do not simply reset to factory settings, reconfigure, or restart Totani equipment without investigating the equipment's status.
- If necessary, remove the equipment from the network.

8. Account Management

Ensure that the following security principles are continuously applied to all accounts used on Totani equipment.

8.1 Basic Account Management Principles

- Assign each user an appropriate level of privileges.
- Assign each user only the minimum set of privileges they really need.
- Only use Administrator privileges for tasks that actually require such privileges.

8.2 Account Registration, Changes, and Deletion

- When registering a new user, set privileges appropriate for the role.
- When a user is moving within the organization, moving to a new role, or leaving the organization, promptly delete the unnecessary account.
- Regularly review accounts that have not been used for a long time.

8.3 Password Management

- Do not share passwords with other people.
- Do not write passwords down on paper, store them near the equipment, or record

them in a format that is easy to guess.

- Promptly change default passwords and temporary passwords.
- It is recommended to use passwords that are at least 8 characters long and use a mix of alphanumeric characters and symbols.

8.4 Default Accounts

- If a default account exists, check whether it is being used.
 - Deactivate if unneeded.
 - If the account needs to be used, do not leave the account name or password in a default state.
-

9. Updates and Inquiries

Totani will provide security patches and software updates for Totani equipment and devices attached to equipment.

When managing such updates or discovering a vulnerability or incident, perform the following actions.

9.1 Update Management

- Check for information provided by Totani on security, updates, and vulnerabilities.
- Before applying updates, check which equipment models are affected by the update, the scope of impact, and the impact of stopping usage.
- Before updating, back up settings and necessary data.
- After updating, check to ensure proper functionality.

9.2 Inquiries and Reports

- If you observe a security-related problem, report promptly to your own internal Administrator or specified contact hotline.
- When reporting to Totani, ensure that you include the model name, date and time of the problem, a description of the event observed, the extent of impact, and any response measures you have already taken.
- If there is suspicious activity, preserve the logs and other related information.

9.3 Contact Hotline for Reporting Vulnerabilities and Incidents

Totani has established a contact hotline for reporting equipment vulnerabilities.

https://*****

10. Disposal and Transfer - Important Notes

Delete as much information as possible before disposing of equipment or transferring it

to another owner.

10.1 Retiring a Piece of Equipment

- Check for saved network settings, connection destination settings, credentials, and maintenance settings.
- Reset to factory default or delete settings as necessary.
- Collect necessary logs, settings, and maintenance information.

10.2 Disposal

- Keep in mind that data may be retained in storage media and other parts and components.
 - Confirm that configuration information, operational information, and log data saved in the equipment have been deleted to ensure secure disposal.
 - If it is not possible to reset to factory settings or delete data, use electrical or physical means to destroy the relevant device in the equipment to prevent any information leaks.
-

11. User and Administrator Responsibilities

Administrators and users are responsible for performing the following actions.

11.1 User Responsibilities

- Only use equipment as authorized.
- Report suspicious activity, abnormal messages or screens, or authentication irregularities when discovered.
- Properly manage account information and control privileges.

11.2 Administrator Responsibilities

- Properly manage accounts, privileges, setting changes, updates, and logs.
- Check that the “2. Prerequisites for Secure Use” are being maintained.
- Maintain an organized communication network with Totani as well as your own management departments in the event that a problem arises.

11.3 Common Reminders

- Do not deactivate security settings out of convenience.
- For operations that are out of the ordinary, receive Administrator approval first.
- Follow Totani instructions regarding any matters not covered in this document.

Contact Totani head office or your local branch with any questions about this document.

- Head office/factories

Totani Corporation

5-81 Nakakuze-cho, Kuze, Minami-ku, Kyoto, 601-8213, Japan

Phone: +81-75-933-7610, Fax: +81-75-933-7602

Email: 2007gad@totani.co.jp

- China factory

Totani Dalian China

No. 2 ShengMing 2nd Road, Economical & Technical Development Zone, Dalian, 116600,
China

Phone: +86-411-8792-2338, +86-411-8792-2318, Fax: +86-411-8792-2198

Email: 2007gad@totani.co.jp

- International subsidiaries

Totani America, Inc.

1701 Mid Valley Dr.

De Pere, WI 54115

Phone: +1-920-632-7319, Fax: +1-920-632-7361

Email: sales@totaniamerica.com

Totani Europe GmbH

Bonnerstrasse 203b 40589

Düsseldorf, Germany

Phone: +49 (0)211-7407-970

Email: sales@totanieurope.com

Totani Asia Pacific Pte Ltd.

10 Anson Road #15-13 International Plaza Singapore 079903

Phone: +65-6220-2982, Fax: +65-6220-2982

Email: 2007gad@totani.co.jp