EPSON

# Security Guidebook

- For Customers Using an Intranet Environment -

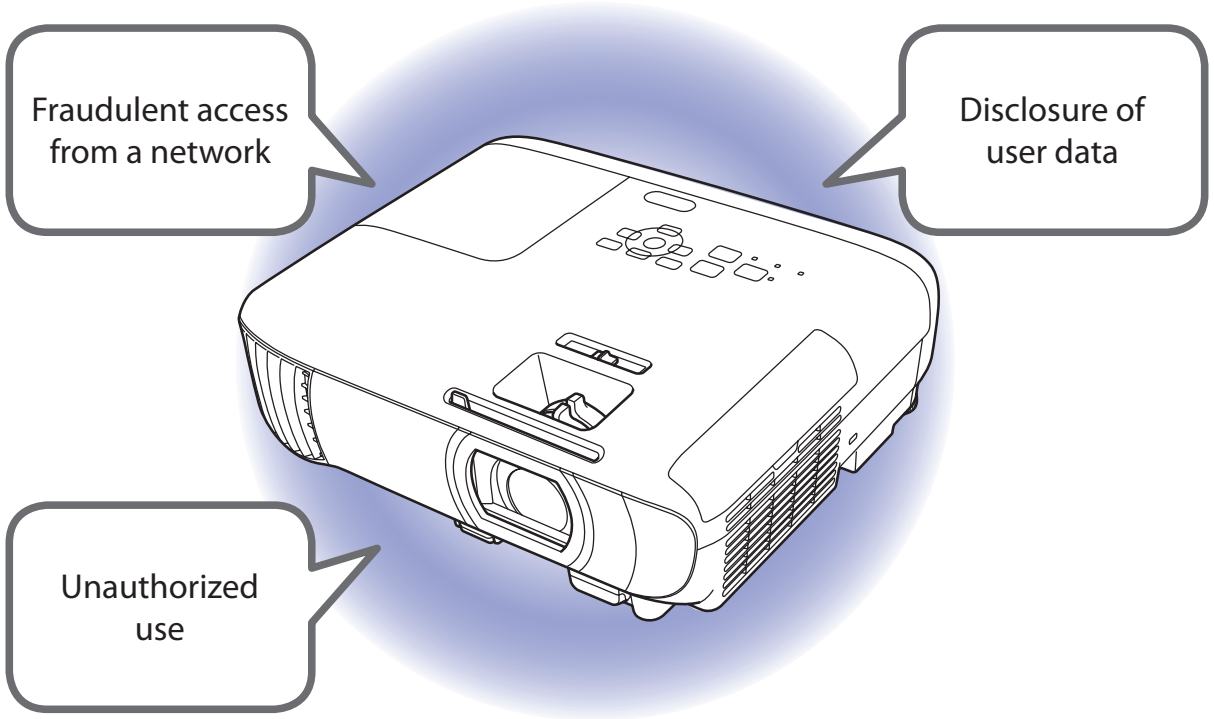
# Table of Contents

# 1. Introduction

At Epson, we have been enhancing the network-compatible features of our products to improve customer convenience.

Meanwhile, the increasing sophistication and complexity of cyberattacks by malicious third parties have increased threats to devices connected to the network, raising concern about security measures.

Because Epson's products are equipped with a variety of features, proper consideration for security is necessary, especially when they are connected to a network, as is the case with computers and servers.




This guidebook introduces Epson's approach to security and advice for the customer, and guides you through the security functions available for use.

The icons next to each function in the text have the following meanings.

: Security features with this mark are the minimum requirements that should be handled by the administrator.

: Security features with this mark can only be configured by the administrator and are available to users in the configured security environment.

: Security features with this mark can be set and used by administrators and users.

: Other security features. Applicable for security features built into products as part of their specifications.

Check your product's manual for how to set up security.

Note that the security functions and compliance with security standards outlined in this guidebook vary depending on the product being used. Some products may not have such features or do not comply with such security standards. Therefore, be sure to refer to the separate feature list of each product.

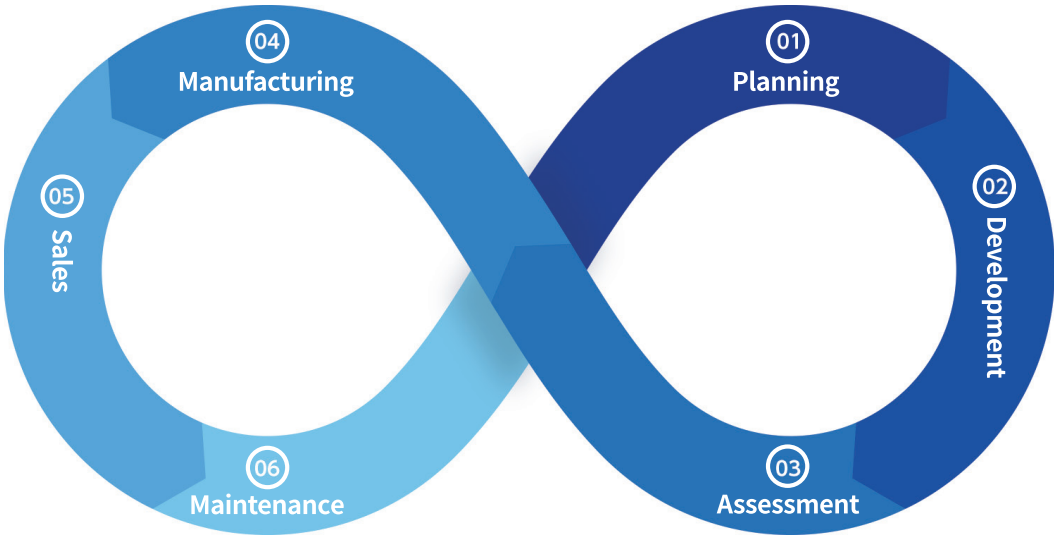
# 2. Epson's Security Basic Policy

At Epson, we take the following approach regarding security so our customers can use our products safely and with ease.

## 2-1. Basic Policy

Epson views product security as the cornerstone of product quality.

We practice product (endpoint) security throughout the entire lifecycle from planning, development, evaluation, manufacturing, sales, and maintenance to ensure that customers can use our products in more secure conditions by closely examining the diverse usage environments for each product genre.




① Planning

At the product planning stage, we continuously monitor the newest security trends and potential vulnerabilities. We also listen to our customers' requests, identifying and analyzing security-related requirements. This way, we eliminate potential problems in our products before any risks can materialize.

② Development

Using our proprietary common platforms and technologies developed through creating a wide range of products, from home projectors to compact, high-brightness commercial projectors, we strive to enhance protection against security risks.

③ Assessment

In addition to thorough in-house testing, we also involve third-party organizations for objective security assessment. With our strict security verification system, we conduct the assessment from different angles to ensure high security for our products.

④ Manufacturing

To ensure the highest quality of our manufacturing operation, we have implemented a thorough information asset management system at our factories, where we install software that enables the functionality of our products.

⑤ Sales

We are committed to supporting our customers by proposing and implementing solutions to minimize security risks depending on the use environment and operational conditions. We also make sure to quickly address any vulnerabilities that may arise after the installation of our products.

When products need to be replaced and disposed of, we make sure to reset the devices to the factory default settings to prevent confidential information leaks.

⑥ Maintenance

We quickly respond to security-related issues and concerns reported by clients who purchase our products.

## 2-2. Providing Information

We actively provide our customers with information and actively keep them aware of security.

## 2-3. Support in Responding to Vulnerabilities

We are constantly addressing vulnerabilities.

- We test for vulnerability using the industry's standard tools and strive to ship products free of vulnerabilities.
- We regularly monitor information about vulnerabilities from open source software used in the firmware of our products.
- When new vulnerabilities are found, we promptly analyze them and provide information and countermeasures.

## 2-4. Compliance with Codes and Standards

We strive to comply with and obtain security standards.

# 3. What You Should Do When You Install Your Product

The "administrator" for business products refers to a person who has IT literacy and is capable of managing the security of the usage environment and can procure and configure network devices (such as computers, routers, and so on) to which the product is connected.

Companies and organizations should appoint an administrator for the products to ensure optimal security. The administrator should configure the necessary settings according to your usage environment while complying with the security policy of the company or organization.

## 3-1. Physical Protection for the Products

The administrator should install the product in an environment that can protect it from modification, destruction, removal, and so on by third parties. In addition, to protect communication data, procure and configure network devices (such as computers, routers, and so on) in accordance with the security policy of the organization.

## 3-2. Restrictions on use of features

The "user" refers to the end user (general user) who uses the product. The administrator should provide users with passwords only for functions that are necessary to use the product. Providing users with passwords for non-essential functions may increase security risks.

## 3-3. Educating Users

The administrator should educate users on their organization's security policies and ensure compliance with them. In addition, the administrator should inform users that when projecting content with the product, there is a possibility that the projected material may be unintentionally viewed or recorded by third parties. Instruct users to check in advance whether the projected content contains confidential or personal information, especially when using projectors in public or shared spaces.

## 3-4. Password Settings

We strongly recommend setting up password protection during installation of each product.

If password protection is not set up or is left at the factory default setting, there is a risk that device settings and network settings stored in the product may be accessed or modified without authorization. There is also a risk that personal and confidential information, such as passwords and address books, may be compromised.

## 3-5. Web Control Password

We strongly recommend setting up a separate web control password during installation of each product.

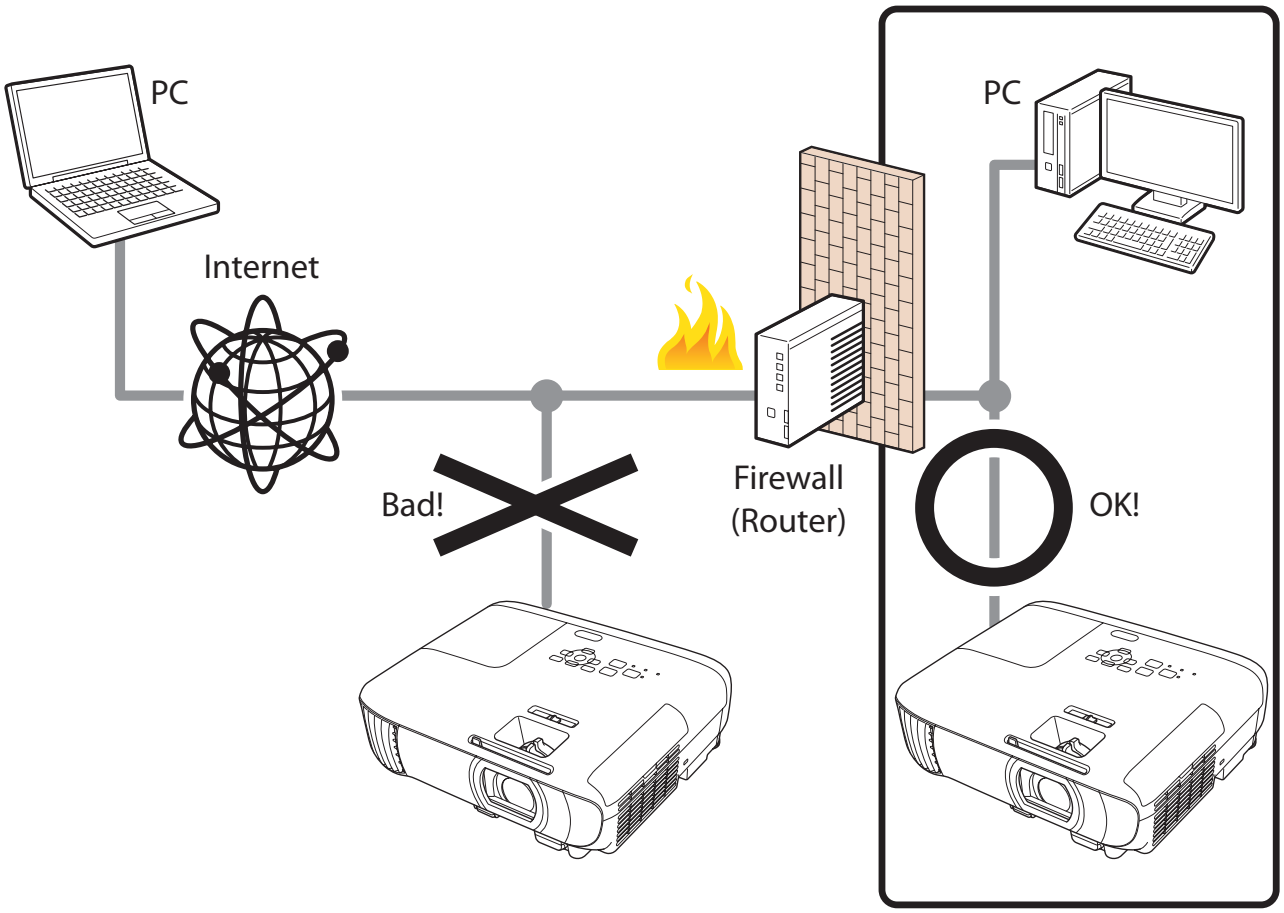
If the web control password is not set up or is left at the factory default setting, there is a risk that device settings and network settings stored in the product may be accessed or modified without authorization. There is also a risk that personal and confidential information, such as passwords and address books, may be compromised.

Create a complex web control password that is difficult for others to guess, such as 8 or more characters that include not only letters but also symbols and numbers. The web control password can be set directly on the product's control panel or remote control, or over the network.

## 3-6. Internet Connection

Install products on a network protected by a firewall without connecting directly to the internet. We recommend setting up and utilizing a private IP address when you do this.

Even when using the product in an IPv6 environment, be sure to restrict access to the product using a firewall or other means to prevent direct access to the product from the internet.



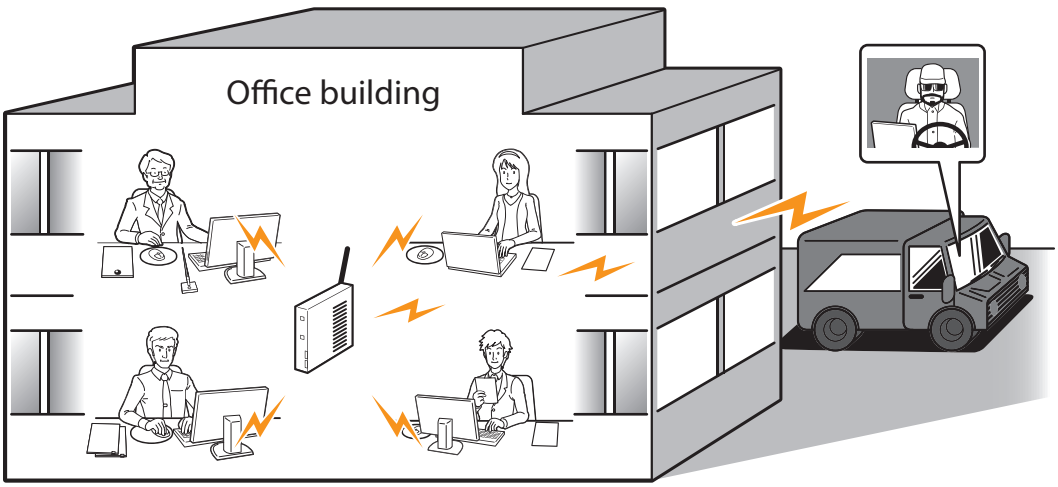
Management interfaces, such as Epson Web Control, are included for the products' network functions as well as projecting. Although Epson conducts vulnerability testing and strives to ship products that are free of vulnerabilities, direct connection to the internet poses unexpected security risks, such as unauthorized operation and information leaks, to the customer's network and devices connected to the network.

## 3-7. Wireless LAN Network

When using a wireless LAN network, set up the wireless LAN's security appropriately.

The advantage of wireless LAN is that you can freely connect to the product via a network to communicate with computer and smart phone terminals if you are within range of a signal. On the other hand, problems like the following, caused by malicious third parties, may occur if security is not properly set up.

- Personal information, such as projected data and passwords, may be viewed by others (intercepted)
- Communication content may be fraudulently rewritten (falsified)
- Certain people or devices may be impersonated and used for communication (identity theft)




See the product manual for the procedure to set up a wireless LAN.

## 3-8. Disabling Unused Protocols and Functions

Disable protocols and functions that are not used.

Each protocol and function can be allowed or prohibited individually, preventing security risks if they happen to be used unintentionally.

## 3-9. Update to the Latest Firmware and Software

We provide the latest firmware and software as needed. Be sure to update to the latest

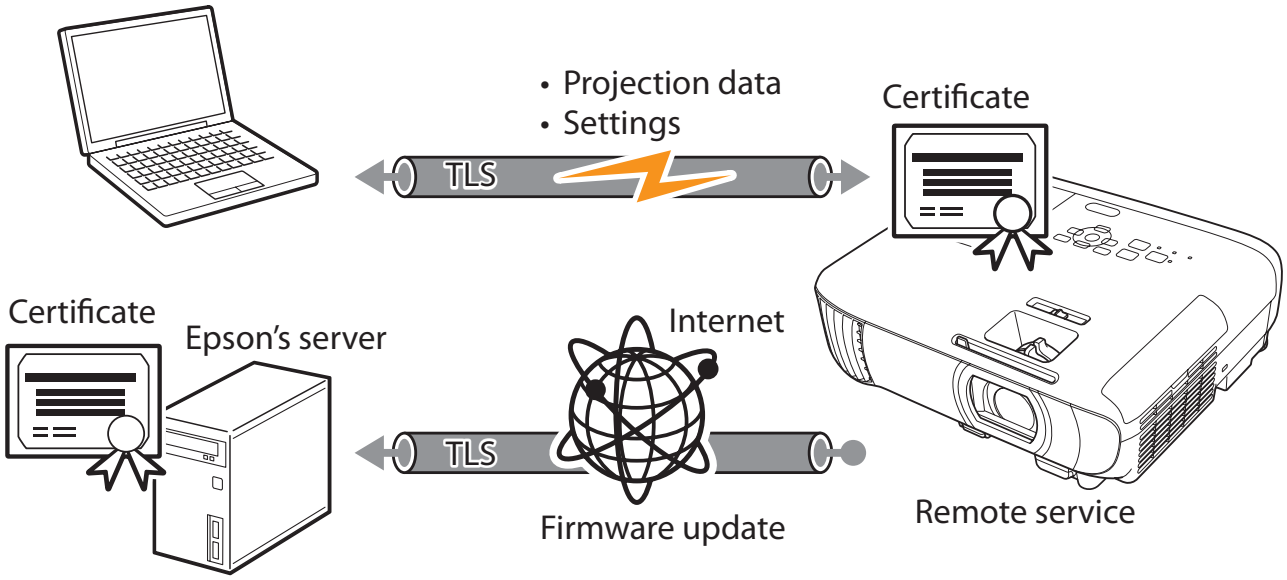
firmware to use the product.

The latest firmware and software include not only additional functionality, but also fixes for defects and vulnerabilities. For more information on the firmware or software, see the history of modifications for the firmware or software.

# 4. Network Security

## 4-1. TLS Communication

Since transmissions are protected by TLS, you can prevent the disclosure of setting information and the content of projection data by configuring your product via your browser. Encryption strength can be configured to use a much safer encryption algorithm. You are also protected by TLS when you access the Epson server on the internet through the product for EPMC (Epson Projector Management Connected) and firmware updates.




You can select the version of the TLS to be used.

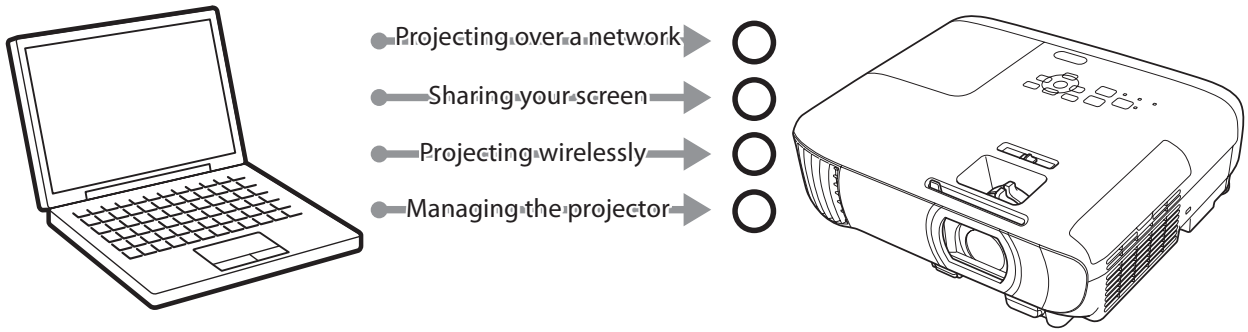
The supported TLS versions are as follows.

### TLS Version

- TLS1.2
- TLS1.3

## 4-2. Controlling Protocol Permissions and Exclusions

The product communicates through various protocols when using functions such as projecting and sharing images. You can prevent security risks from unintended use before they happen by setting up individual permissions and prohibitions for each protocol.




See the "Appendix" for security risks when protocols and features are enabled and for limitations when they are disabled.

The protocols and features that can be allowed or prohibited are as follows.

- SMTP
- SNMP
- PJLink
- Secure HTTP
- AMX Device Discovery
- Crestron Connected
- Crestron XiO Cloud
- Control4 DDP
- Art-Net
- Message delivery
- Basic control
- Screen sharing
- Network folder
- LDAP
- Epson iProjection
- Printer
- Web API
- Screen Mirroring
- AirPlay
- Epson Projector Management Connected (monitor control)

## 4-3. SNMP

SNMP is a protocol for monitoring the status of and changing settings of supported equipment and management tools.

SNMPv1 and SNMPv2c do not support encryption of communications and should be used within a network protected by a firewall or something similar. However, even when using SNMPv1 or SNMPv2c, communication is performed using authentication and encryption when monitoring the status of highly confidential information or changing settings.

SNMPv3 can be used to authenticate and encrypt SNMP communications (packets) for monitoring status and configuring changes with compatible device management tools. This can ensure confidentiality when changing settings or monitoring status over the network.

## 4-4. SMB

SMB is a protocol for sharing files over a network.

SMB2.0 do not support encryption of communications and should be used within a network protected by a firewall or something similar.

SMB3.0 can be used to authenticate and encrypt SMB communications (packets) with compatible devices. This can ensure confidentiality for file sharing over the network.

## 4-5. WPA3

The product supports WPA3 which is the latest authentication and encryption technology for Wi-Fi (wireless LAN). WPA3 provides a more robust and stronger protection to safeguard your data over the wireless network.

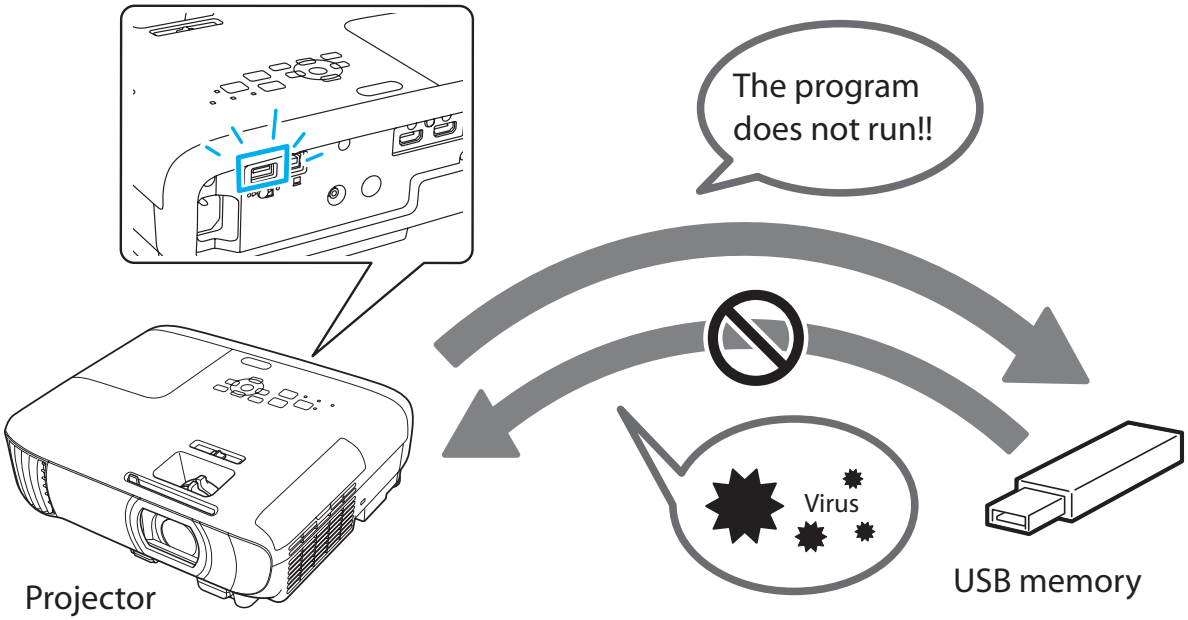
## 4-6. Separation Between Interfaces

The product includes a USB interface, wired LAN interface and wireless LAN interface. Each interface is independent, restricting access only to protocols that can be handled by that interface, and does not provide any direct transfer or routing capabilities.

# 5. Protecting Your Product

## 5-1. Handling Viruses Introduced by USB Memory

Since there are no executable functions on USB memories for Epson products, there is no danger of the product being infected with viruses via USB memory.



# 6. Wireless Projecting Security

## 6-1. Encryption Settings

To prevent potential data leakage, it is recommended to enable encryption when using the Screen Mirroring function in Epson iProjection to display content from connected devices.

## 6-2. Email Settings

The interactive email function allows users to send drawn content as an email attachment. It can be configured to restrict sending only to email addresses registered in the address book. This setting helps prevent information leakage to unintended recipients.

In the email notification function that informs users of abnormal product conditions, set an email address that does not contain any personal information to ensure privacy protection.

## 6-3. Encrypted PDF

You can save the content drawn on the projector screen as an encrypted PDF. This helps prevent unauthorized viewing of the content by third parties.

## 6-4. Protection of Network Projection (Epson iProjection)

Epson iProjection uses a proprietary communication protocol, and data transmitted during projection is protected through AES encryption.

# 7. User Data Protection

## 7-1. Handling of Saved Projection Data

The projector includes a function that allows users to save projected video data as an image. Be sure that any saved data is managed appropriately. Additionally, be sure to avoid including personal or sensitive information in the saved content.

## 7-2. Address Book

The address book used for emailing drawn content from the whiteboard function is not included in the batch configuration data. By restricting access to the address book, you can help prevent the leakage or unauthorized modification of email address information.

## 7-3. Whiteboard

All drawn content is erased when the projector is turned off.

# 8. Operational Limitation

## 8-1. Security Password

By using a security password, you can restrict operation and settings of the projector using the product's control panel. Setting a password ensures that only users who know the password can access these functions.

## 8-2. Disaling Remote Receiver / Button Lock Security

By disabling the remote control receiver, the projector can no longer be operated by remote control. Additionally, disabling the control panel blocks operation of the projector from the control panel. These functions help prevent unauthorized users from projecting content without permission.

# 9. Product Security

## 9-1. Automatic Firmware Updates

The Epson Projector Management or Epson Projector Management Connected software allows you to update firmware over the network. When new firmware is available, you can receive a notification and schedule a specific date and time for the update, ensuring you can always use the latest firmware without interrupting operations.

## 9-2. Protection Against Illegal Firmware Updates

The firmware sent to the product itself is verified as legitimate by signature before the firmware is rewritten. This prevents unauthorized firmware modification by malicious third parties.

# 10. Making Recommended Settings for Security

This section describes the recommended settings for safely managing confidential information that companies and organizations handle on a daily basis. The following settings are for products that support password protection.

**Caution:**

- Some functions may not be supported depending on the product. Set up the functions that are supported by the product. For information on the compatibility of each product, see the separate function list of each product.
- The menu structure of the setting items differs depending on the product. See the product manual.

## 10-1. Password Protection

Make the following settings using the product's control panel:

1. **Set a Password**

   When using the product for the first time, set a 4-digit password using the numeric keypad on the remote control. No default password is set.

2. **Select the Type of Password Protection**

   Power On: Prevents users who do not know the password from turning on the projector.

   Menu Protection: Restricts changes to settings such as the user logo screen, schedule settings, network menu, and interactive menu.

3. **Enter the Password**

   When the password screen is displayed, enter the correct password to proceed.

# 11. Security Measures When You Dispose of Your Product

## 11-1. Restore Factory Defaults

When transferring or disposing of a product, you can return the projector settings and data stored in it to the factory defaults (initialization). See the product manual for initialization procedures (only for models equipped with this function).

## Security risks when protocol/security features are enabled (impact on personal information protection, unauthorized operations) and restrictions when disabled

Administrators should understand the risks and restrictions before configuring.

| Protocol/ security functions | Security risks when enabled | Limitations when disabled |
|---|---|---|
| PJLink | If control is performed without authentication, there is a potential security risk of unauthorized operation by third parties. | If control is performed with authentication, operation through compatible control software or the touch panel is disabled, and collective control or status monitoring from remote locations is no longer possible. |
| Command Communication (ESC VP.net) | When using [Compatible] mode, passwords are transmitted without encryption, which may pose risks of interception or unauthorized access. If Monitor password is not set (zero characters are entered) in [Compatibility] mode, command communication can be performed without authentication, increasing the risk of unauthorized operation. | When using [Protected] mode, compatibility with older software versions or certain external control devices may be limited. If a password is set, automatic connection with legacy devices that do not support password authentication may not be possible. |
| SNMP | Since SNMPv1 and v2c do not encrypt communication data, they pose a high risk of information leakage and unauthorized control. Devices that do not support SNMPv3 cannot ensure adequate security. | Additionally, integration with network monitoring tools may not be possible, making it difficult to automate device status monitoring and fault detection. |
| Secure HTTP | If set to [Off], communication is not encrypted, and there is a risk that passwords or configuration data entered on the Web Control screen may be intercepted or tampered with. | - |

| Protocol/ security functions | Security risks when enabled | Limitations when disabled |
|---|---|---|
| AMX Device Discovery | There is a risk that device information on the network may be accessed by third parties. | Devices are not displayed in "Devices and Printers" in Windows. Disabling this function may prevent AMX control systems on the network from automatically detecting the projector. |
| Crestron Connected | There is a risk that device information on the network may be accessed by third parties. | Disabling this function may prevent automatic integration with Crestron control systems. |
| Screen Sharing | Incorrect IP address settings may result in the screen being shared with unintended devices. | It may also prevent simultaneous display of the same screen across multiple projectors. |
| Network Folder | There is a risk that data shared through file sharing may be accessed by unauthorized third parties. | Network file sharing may become unavailable. |
| LDAP (Using Directory Services) | There is a risk that authentication information and data may be accessed by unauthorized third parties. | Email address search using the projector may become unavailable. |
| Epson iProjection Epson Classroom Connect | If encryption settings or the projector keyword settings are not properly configured, there is a risk of unauthorized access or screen interception by third parties on the same network. When the projector keyword is turned [Off], users can connect to the projector through Epson iProjection without entering a keyword, which may result in unintentional projection of content. | Network projection from mobile devices or PCs may become unavailable. |
| Printer | There is a risk that printing will be performed on an unintended printer due to incorrect IP address settings. | You will no longer be able to print from the projector. |
| SMTP (Email Notifications/ Using Email (Interactive Menu)) | If the SMTP settings are set to [Open] or [Auth Only], the communication is not encrypted, posing a risk of interception. | As a result, the projector is unable to send email notifications when an error or warning occurs. Additionally, content drawn on the whiteboard can no longer be shared by email. |

| Protocol/ security functions | Security risks when enabled | Limitations when disabled |
|---|---|---|
| Web API | If the authentication method is set to [Open], there is a risk of unauthorized operations or configuration tampering. Even when using [Digest] authentication, if the communication is not encrypted, authentication credentials may be intercepted. | As a result, control of the projector from external systems or applications may become unavailable. |

EPSON



Issued 2025.06, Rev.00.