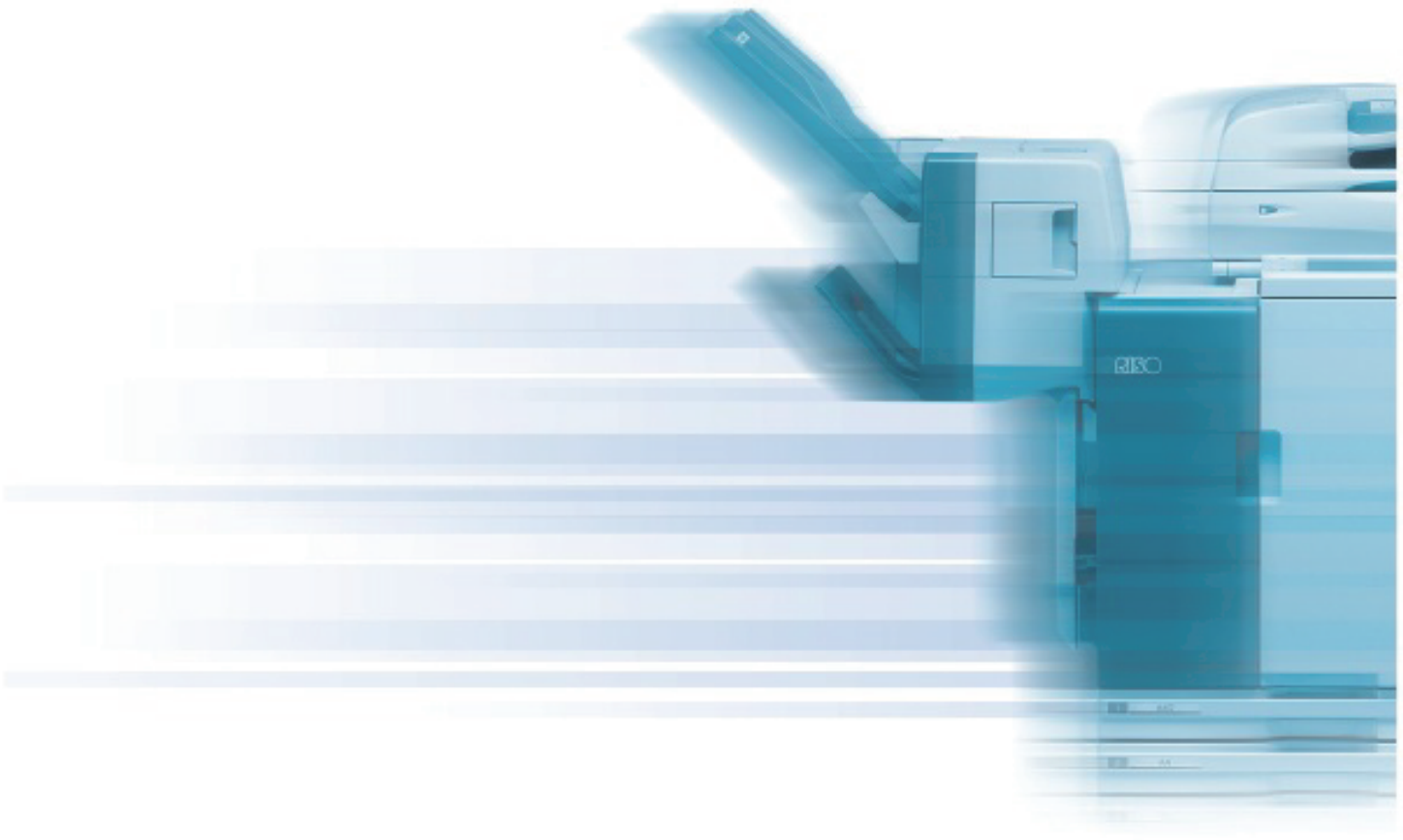
RISO KAGAKU CORPORATION

SECURITY POLICY



Introduction

RISO takes a progressive approach to protect customers' important information assets against any risk of information leakage, for their safety benefit.
However, the risk of information leakage may increase depending on the usage of our products by our customers, if the product is designed for network connection.
Therefore, we ask for your cooperation to securely use our products with the appropriate settings by reading this document and implementing the measures outlined.

In the case of any security threat RISO has a system in place to take quick measures.
You can rest assured of the safety of RISO products.

Security measures for RISO products

RISO has various systems to implement security measures on our products.

Vulnerability inspection of operation programs by a third party

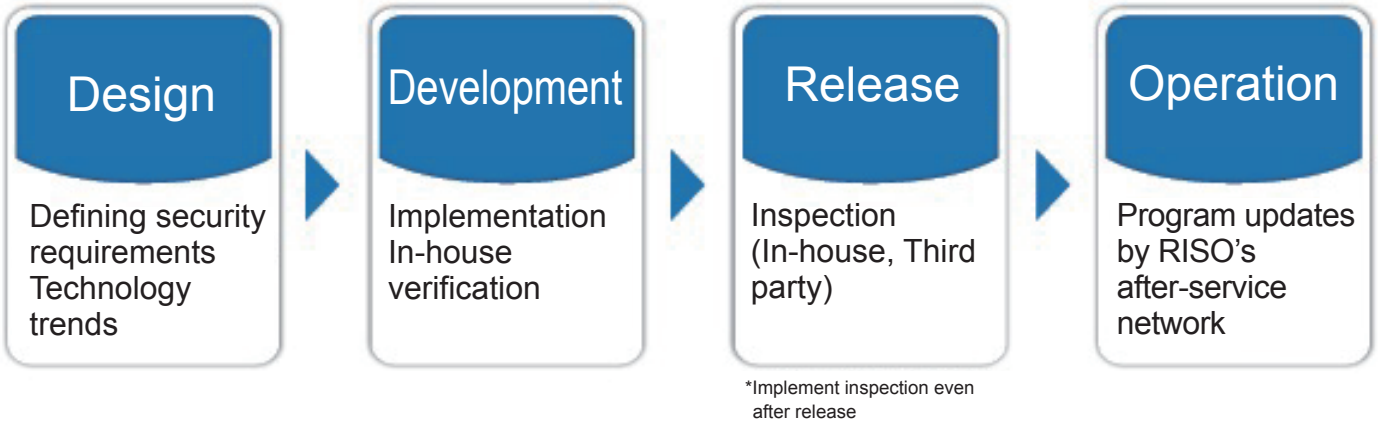
Vulnerability assessment is performed by third-party experts besides our in-house verification prior to the release of an operation program.

Program update by RISO's after-service network

Through our after-service network, we provide prompt implementation of program updates to products in use by our customers in the field.

Continuous implementation of vulnerability inspection

We address any new vulnerability by continuous assessment of vulnerability of operation programs after the release of our products.



Network connectivity

A network-connectable device is under threat of attack and carries potential risks of information leakage. These can be reduced by taking the following countermeasures.

Do not open unnecessary ports

Unnecessary open ports increase the risk of network intrusion.
Close all unnecessary ports. (Unnecessary ports are set closed at the factory default.)
Furthermore, the safe usage of functions as described on this page will prevent unauthorized access or operation thus reducing any risk of network intrusion.

Specify accessible PCs

It is possible to limit connections from unauthorized IP addresses by limiting connectable source IP addresses.

Create a login authentication environment

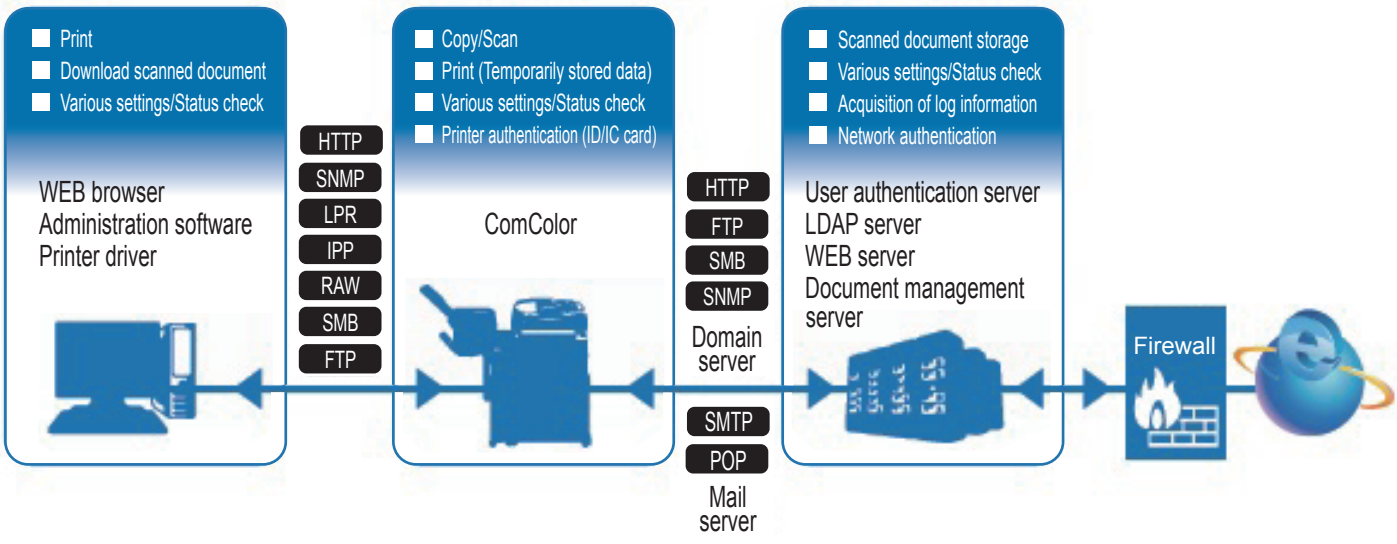
It is possible to limit users by setting login authentication requirements.

Communication data encryption

You can implement the HTTPS protocol for communicating with RISO consoles (to encrypt the communication).

Network connection overview

*ComColor is shown in the figure as an example



RISO SECURITY POLICY

USB flash drive connection

- Since RISO products disable autorun when a USB flash drive is connected, your devices are kept safe from USB drive virus attacks. Also, differently to USB devices for PCs, RISO products do not install device drivers.
- Even if a keyboard or a mouse can be physically connected to RISO products, commands will not be activated.
- USB flash drive connectivity creates potential security risks which include network system cracking by a hacker, and leakage of data stored in a printer when inappropriately operated.
- In a printer, please do not store any confidential document which was input to the printer through a USB flash drive. When you save confidential documents to a printer, please make sure to protect them with a password.

*Some of the functions are not available on digital duplicators

Data transmission

- As scanned image data can be transmitted using FTP/SMB/SMTP protocols, it is preferable that RISO products are handled with the equivalent care as network devices that use those protocols.
- Also, because scanned image data can be stored in the HDD of the printer, please do not leave confidential documents in printer.
- If you have to save confidential documents to the printer, please make sure to protect them with a password.

*Some of the functions are not available on digital duplicators

Print jobs

- Print jobs saved to folders are stored in the internal HDD. Data leakage risk may increase depending on the operation of the printer.
- Please do not leave confidential documents in the printer, and make sure to protect them with a password.

*Some of the functions are not available on digital duplicators

Administrator password setting

- To ensure your printer is securely operated, appropriate management of configurations and settings by an administrator is essential.
- Please make sure to provide login password for a user with administrator authority.
- When you log in as a user with administrator authority, you can work on data stored in the printer and can change settings.

Please refer to the user's guide for detailed operation methods