Security recommendations
for the use of Komax machines, software and services in production

Content

1 General information

1.1 Version

This document	Date	Status
1.1	June 1, 2025	Released

1.2 Availability of the security recommendations

1.2.1 Komax machines

- Online help

1.2.2 Online

These security recommendations are not exhaustive and are continually updated. The latest version can be found online at Komax.

- Komax (online): https://www.komaxgroup.io/security/en
- Komax (online, QR Code):

1.3 Purpose

These security recommendations are designed to make the operation of Komax machines in a connected production plant at Komax customers secure and reliable.

The aim is to ensure a high availability of the machines and to ensure their production ability according to their specifications.

This involves preventing the following situations:

- Unauthorized access to data
- Unauthorized manipulation of data
- Running unwanted or unauthorized software programs
- Use of software and/or hardware of the machine for purposes other than specified
- Bringing about a targeted malfunction of single or multiple machines in the production plant with the intention of disrupting or impeding production

1.4 Scope of application

The customer bears full responsibility at all times for adequately safeguarding their infrastructure against attacks of any kind with suitable security measures in order to maintain the correct function of all system components and their availability for productive operation. This responsibility includes Komax machines, software and services.

These security recommendations are suggestions for specific measures that Komax issues to its customers for independent implementation. They apply to all machines, software and services of Komax in the corresponding production plant of the customer. The responsibility for implementation lies with the customer, i.e. not mandatory, but strongly advised.

Customers who are unsure about the implementation of these security recommendations or whose specialist knowledge with regard to IT, computers, software and network setup is not sufficient are advised to consult appropriate specialists. The responsibility for setting up and implementing appropriate security measures remains with the customer.

1.5 Roles and responsibilities

Organization	Responsibility
Komax Cluster Product Security	Creation, further development and maintenance of security recommendations
Customer	• Creation and implementation of operational and security concepts for OT and IT • Compliance with the IT/OT operating concept

1.6 General comments on handling Komax products

Komax prohibits the customer and any third parties from influencing the software or machine in any way, modifying it or otherwise changing its contractual purpose of their own volition.

1.7 Terms

Term	Description	Details
IT	Information Technology	Computer hardware and software programs in the administrative area
OT	Operational Technology	Computer hardware and software programs for monitoring and controlling physical machines in and their processes in a production plant
MES	Manufacturing Execution System	Production planning and control system, control system (computer and software)
MIKO	Real-time data interface for Komax machines	Real-time data interface with three main components • MIKO Discovery: Finding MIKO servers (machines) in the network (based on WS Discovery) • MIKO Publish: Notification service with push notifications on events and status changes (based on MQTT) • MIKO Request: Structured read/write access to all data on the machine (based on REST)
N-S Traffic	North-South-Traffic	Traffic between the public Internet and the customer's network infrastructure
E-W Traffic	East-West Traffic	Data traffic between OT and IT
TopImage	Operating system for Komax machines	Operating system based on Microsoft Windows. Basis for installing the Komax HMI or TopWin user interface.
Komax HMI	User interface for Komax machines	Software for machine operation by the user. This software contains the operating elements and workflow control of the machine, as well as the network connection to higher-level systems such as MES.
TopWin	Operating software for Komax machines (previous generation, legacy)	Previous software (previous generation) for machine operation by the user. This software contains the operating elements and workflow control of the machine, as well as the network connection to higher-level systems such as MES.

2 Security recommendations for the use of Komax machines, software and services

2.1 Organization

2.1.1 Designate a person responsible for internal IT security. (Same procedure as for physical occupational safety.)

2.1.2 Designate a person responsible for the administration of OT. (Same procedure as for IT administration.)

2.1.3 The administrator account should only be used by the administrator.
The administrator password is only to be used for the administrator account, ie. for administration purposes and must be kept secret.
Machine users who do not carry out any administrative tasks should work with a user account that does not have any administration permissions.

2.1.4 Have in place and keep up to date the list of authorized administrators whose area of responsibility includes access to the machine.

2.1.5 Only allow administrators to access the hardware (e.g. control cabinet).

2.1.6 If possible, only allow administrators to use physical interfaces (e.g. USB) or set up dedicated security measures to prevent malware from being introduced.

2.1.7 Use the physical interfaces exclusively for the installation of Komax software and for the storage of data in the event of operational or technical problems.
Block, prevent or prohibit the use of the USB interface for other purposes.

Examples: Charging of smartphones, use of an external storage device (hard disk, SSD), use of USB adapters for connecting further devices.

2.1.8 Only allow responsible administrators or personnel by Komax or its partner companies to carry out installations and configuration adjustments of the software (eg. operating system). This also includes keeping secret and, if necessary, regularly changing passwords for protected areas of the software.

2.1.9 Set individual passwords, do not use default passwords.

Please note: Setting an individual password for the administrator account implies that, for service calls by Komax or its partner companies, an administrator of the customer must approve the administrator account for a service engineer to carry out the necessary work on the machine. This approval may need to be given several times during the course of the work (e.g. when restarting the machine).

2.1.10 Assign and use individual passwords for each user. Passwords are personal and must be kept confidential by the user.

If passwords are written down, restrict and control access to the password register (e.g. store it in a safe place, only enable or allow access to trusted persons).

2.1.11 Manage users individually in MS Windows Active Directory, define user groups, assign users to user groups.

Examples: Specific groups for operators, setters, engineering, quality management, maintenance, administration

2.1.12 Set up different permission sets for the respective user groups on the machines (e.g. in Komax HMI).

2.1.13 If no differentiation of operators is required and/or if the machine is operated without a network connection, TopImage's Windows system login can be configured to launch Windows without the explicit input of user details. The relevant settings for the corresponding machines are described in the Komax HMI Online Help.

Important: The customer bears full responsibility at all times for ensuring that the settings are secure and cannot be tampered with by unauthorized persons.

2.1.14 Regulate internet access.

2.1.15 Review all measures regularly and update them if necessary. Always keep operating systems and the configuration of network elements, security software and network group policies (GPO) up to date as well as backups and instructions.

2.1.16 Note down the network topology and configuration of network elements and keep notes up to date at all times. Ensure that your notes and protocols are available in emergencies in case the network, server(s) and/or affected machines are unavailable.

2.1.17 Create a business continuity plan/playbook and verify the smooth functioning of all measures in regular functional tests. Ensure that your notes are available in emergencies in case the network, server(s) and/or affected machines are unavailable.

2.2 Network and infrastructure

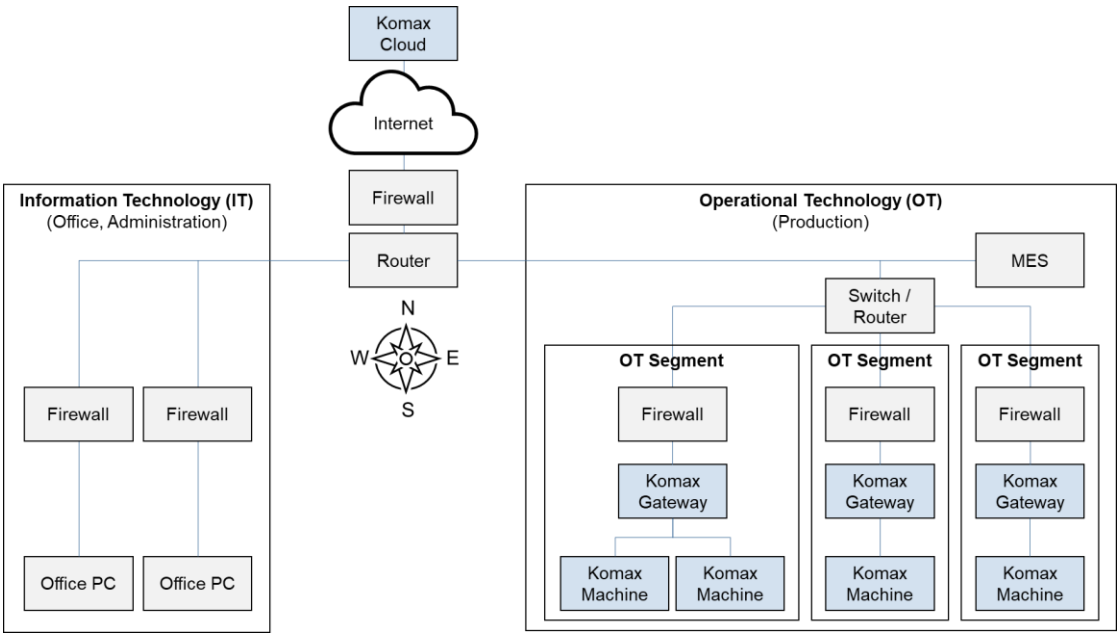
2.2.1 Use a firewall to filter or restrict communication between the OT network and the internet (North-South Traffic).

Allow only the minimum necessary connections:

- Connection to the Komax cloud
- Connection to necessary domains to perform software updates
- Enable dedicated remote access for service purposes

2.2.2 Use a firewall to separate Operational Technology (OT) and Information Technology (IT) (East-West Traffic).

2.2.3 Split the OT network into segments.
Please note: Due to the segmentation, the machines can no longer be found from outside the segment using MIKO Discovery. For the use of MIKO Discovery by a central client, a central register must be kept of the IP addresses of the machines controlled via MIKO or the message brokers used.



2.2.4 Use the Komax Gateway for decoupling of traffic between Komax machines and the customer's systems and traffic between Komax machines and the Komax Cloud.

Additionally use firewalls for the connection to the Internet and between network segments.

2.2.5 Take measures to detect lateral movement. Set up measures and solutions to detect the movement of an attacker within the attacked network, e.g. using network based intrusion detection systems etc.

2.2.6 If Network Group Policies (GPO) are used in the customer's network, they must be written to the Windows registry in order to overwrite existing entries.

Before the network-wide rollout of GPO, it is strongly recommended to test the smooth operation on a single Komax machine with active GPO.

In any case, the customer is responsible for ensuring that the measures taken do not affect the proper functioning of all system components and their availability for the operation in the production plant.

2.2.7 Ensure resilience of the OT network and all components required for production (machines, servers, software, production planning and control system etc.) against denial of service attacks (DOS/DDOS).

2.2.8 Have spare parts and replacement equipment available on site for important network elements and functions. Have current operating system software and application software available, and have installation instructions and configuration plans ready in written form. Ensure documents are available in emergencies even in case the network, server(s) and/or affected machines are unavailable.

2.3 Software

2.3.1 Information: TopImage is supplied with the latest Windows release at the time of delivery and contains support for the Komax computers, quality tools, etc. currently in use at this time. Microsoft also provides ongoing Windows updates (updates, patches) for TopImage.

2.3.2 Keep TopImage up to date: Download and install Microsoft updates (patches) regularly via the Internet or local WSUS server. Create a backup of the machine before each update.

The update process for TopImage is set to “manual” in the basic settings. Updates can also be carried out “automatically” if desired. In any case, the customer is responsible for checking the updates for potential incompatibilities or other problems.

It is recommended not to install updates on all machines immediately on patch day, but to test the updated software on individual machines first and then install the remaining machines in stages one day later.

2.3.3 Store Komax software delivered on memory sticks in a designated location, control access (e.g. only allow for administrators).

2.3.4 Only install 3rd party software (e.g. MES client) if absolutely necessary for operational reasons, only download it from a reliable source and check its integrity before installation, e.g. via a checksum (hash). Do not install any private software. Minimize security risks in general and do not jeopardize the machine’s functional availability under any circumstances.

2.3.5 Use the installed security software (MS Defender). Update the security software regularly via the Internet or local WSUS server and install the available updates promptly.

2.4 Data and data backup

2.4.1 Carry out regular backups (e.g. weekly), for example using the Database Administration Tool (Komax HMI):

- Database
- Machine configuration

2.4.2 Store backups in a central location.
Important: Never store the backup exclusively on the hard disk of the machine.

2.4.3 Define and verify the recovery process: Verify the complete recovery using the backups (incl. recovery of the operating and control software of the machine). Carry out the complete recovery in regular training runs to ensure problem-free operation in the event of an emergency.

2.4.4 Do not save any private or personal data on the machine.

2.5 Contact

Contact address for questions and feedback on the available security recommendations:

- Komax (online): https://www.komaxgroup.io/security/en
- Komax (online, QR Code):

3 Change log

3.1 Version history

Version	Date	Status
1.0	Juli 1, 2023	Released
1.1	March 1, 2025	Released

3.2 Changes to version 1.0

Section	Change	Content
1.2	Change	Availability
2.1.14	Change	Moved to section 2.1 Organization
2.1.15	New	Reviewing and updating measures
2.1.16	Change	Moved to section 2.1 Organization
2.1.17	New	Business Continuity Plan, testing
2.2.3	Addition	Drawing
2.2.4	Addition	Komax Gateway
2.2.5	New	Lateral movement
2.2.6	Change	Moved to section 2.2 Network and infrastructure
2.2.7	New	Resilience against DOS and ransomware attacks
2.2.8	New	Spare parts and backup equipment for network elements
2.5	Change	Contact address