Danfoss A/S
DK-6430 Nordborg
CVR No.: 20 16 57 15

E-mail: danfoss@danfoss.com
Homepage: www.danfoss.com

November 3, 2026

AK-System Manager – Cybersecurity Incident in Europe – Customer Information

Dear customer,

several sites across Europe have reported suspicious changes during the early hours of November 2, including unusually high defrost temperatures, changed temperature settings and activation of electrical defrost.

Known affected Danfoss systems were directly exposed to the public internet (without VPN, not operating behind a firewall).

The affected equipment in the reported incidents were:

- End of life products AK-SM800 and AK-SC355 systems
- AK-SM800A systems operating on outdated software versions

Recommended contingency measures
(see details on mandatory requirements and best practices on next page):

- Remove internet exposure of affected units and of all units exposed on public IP
- Restore and verify the complete configuration
- Update current generation AK-SM800A systems to the latest firmware version available
- Enable Strict Mode on AK-SM800A
- Re-establish access to the units only through a secure VPN or in general over a protected network

For further technical support, please reach out to the regional technical support team.

Danfoss additionally recommends updating the fleet (AK-SC355, AK-SM800) to current generation products (AK-SM800A series), to ensure receiving continuous cybersecurity updates.

Danfoss continues to monitor the situation and remains fully committed to supporting our customers throughout this difficult situation.

Please also share this information with your supermarket end-user customers to ensure all relevant sites are informed and can take the recommended contingency measures.

Kind regards,

Jonas Hildebrandt | Senior Director Product Management
Electronic Controllers & Services | Danfoss Climate Solutions
jonas.hildebrandt@danfoss.com | Mobile: +49 151 2626 4387

AK-System Manager Cybersecurity: Mandatory requirements and recommended best practices

Cyber Security - mandatory requirements

Danfoss considers the following aspects mandatory when planning to connect your System Manager to digital networks. Failure to implement the mandatory requirements below exposes your System Manager and connected applications to malicious attacks and is outside Danfoss' recommended operating posture.

AK-SC355 (retired from sales in 2016, replaced with the AK-SM800)

- Do not connect a System Manager directly to public internet or any untrusted open networks
- Protect remote access with a secure VPN terminated behind a stateful firewall using a deny-by-default policy
- Ensure factory User and password is changed

AK-SM800 (retired from sales in 2023, replaced with the AK-SM800A)

- Do not connect a System Manager directly to public internet or any untrusted open networks
- Protect remote access with a secure VPN terminated behind a stateful firewall using a deny-by-default policy
- Ensure factory User and password is changed

AK-SM800A (actively sold and supported globally)

- Do not connect a System Manager directly to the public internet or any untrusted open networks
- Protect remote access with a secure VPN terminated behind a stateful firewall using a deny-by-default policy
- Ensure System Manager is running latest software version to maximize cyber security functionality
- Ensure the System Manager security level is set to **Strict mode** (Configuration>Security-Strict)

Cyber Security - best practices (follow these best practices in addition to the mandatory requirements)

- Change passwords on a regular basis and do not share or publish
- Change standard management ports or restrict access to allowlisted sources only
- Segment the control network (e.g., VLANs); isolate from corporate and guest networks
- Back up configurations securely
- Consult available industry standards (i.e. ISO/IEC 27002:2013) for further reference and guidance