Birkerød, March 11th 2026

Cyber Resilience Act (CRA)

Dear Customer and Partner,

JVL takes cybersecurity seriously and has been working proactively to meet the requirements of the CRA ahead of the December 2027 compliance deadline.

We are committed to full compliance and to supporting our customers throughout this process. Below you will find details of our product architecture, our internal development and security practices, deployment security recommendations, and our long-term support commitment.

DIGITAL ELEMENTS

All JVL motors contain digital elements. This includes the firmware responsible for motor control as well as the various supported industry communication protocols.
Both firmware and the industry protocol can be updated remotely, using JVL's MacTalk Windows program, which requires either a serial connection to the motor, or that both the motor and the Windows PC are on the same Ethernet network.

PRODUCT DEVELOPMENT PROCESS & SECURITY

JVL follows a structured development process designed to maintain high software quality and security:

- All changes undergo mandatory peer review before being accepted into a release.
- Security scans are performed on all selected third-party libraries, and each library is checked for known vulnerabilities. Any identified vulnerabilities are patched, or the library is upgraded as soon as possible.
- JVL operates under an ISO 9001 certified quality management system, which underpins our structured and controlled development and change management processes.

As part of this process, JVL will include a Software Bill of Materials (SBOM) in Firmware and MacTalk releases from April 2026 onwards. The SBOM details all software libraries and components used in our products, including third-party components, providing the transparency required under the CRA.

SECURITY RECOMMENDATIONS

JVL motors are designed for deployment within dedicated, isolated industrial production networks — environments that are physically and logically separated from corporate IT networks and the Internet. This is the intended use environment for these products, and the conditions described below define how JVL motors can be deployed securely.
The recommendations below follow the Defence-in-Depth framework aligned with IEC 62443, the leading international standard for industrial cybersecurity, and are structured around three pillars: Network Security, Plant Security, and System Integrity. Machine builders and system integrators incorporating JVL motors into their products should use these recommendations as direct inputs to their own risk assessments.

Network Security

JVL motors communicate with PLCs and controllers using standard industrial Ethernet and serial protocols. These protocols do not employ over-the-wire encryption, which is consistent with how field-level industrial communications are commonly deployed. The intended security boundary is at the network level, not the protocol level.

- All control networks containing JVL motors and PLCs must be operated as isolated, dedicated production networks, segmented from corporate IT networks and with no direct Internet connectivity.

- Where remote access to the production network is required, it must be implemented through a secure gateway (e.g. a VPN with access controls or a DMZ architecture). Direct exposure of the automation network to external networks is not an acceptable configuration.

Plant Security

Physical access control is the first line of defence for industrial automation equipment.

- All cabling between PLCs and motors must be routed and protected to prevent unauthorized physical access or tampering.
- Access to the production area must be restricted to authorized personnel only.

System Integrity

Motor configuration, diagnostics, and firmware updates are performed via JVL's MacTalk software over either a serial connection or Ethernet. Access to these functions must be appropriately controlled.

- Serial configuration connectors on JVL motors must be physically protected to prevent unauthorized access to motor configuration or firmware.
- Firmware updates must only be performed by authorized personnel as part of a controlled maintenance process.
- Access to MacTalk and to the network segments on which JVL motors operate must be restricted to authorized personnel.

JVL motors — including all current and legacy series — are designed for use in exactly this type of controlled industrial environment. The CRA's security requirements are risk-based: they do not mandate specific technologies such as encrypted field-level protocols, but require that products are secure within their intended use context. When the measures above are implemented, JVL motors fulfil that requirement. Machine builders should document these deployment conditions as part of their own product risk assessment and CRA conformity process, and may reference this statement as the manufacturer's intended use declaration.

SUPPORT PERIOD

JVL motors come with a 1-year hardware warranty and 10 years of firmware updates, both effective from the date of purchase.
During the 10-year firmware support period, JVL actively monitors the firmware for known vulnerabilities, and if such are found, will:

1. Inform customers via newsletters and JVL's support website
2. Issue a patched/upgraded firmware.

CONTACT & FURTHER INFORMATION

We are happy to answer any specific questions you may have regarding CRA compliance or our products. Please do not hesitate to reach out to us at sales@jvl.dk or visit our website at www.jvl.dk for the latest information.

We look forward to continuing our close cooperation with you.

_____

Carsten E. Nielsen | CTO