megacon ELECTRONIC CONTROL AND INSTRUMENTATION **Megacon Group**

INNOVATION BEYOND TRADITION

nqa. ISO 9001 Registered UKAS QUALITY MANAGEMENT 015

Cyber Security Policy

Introduction.

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, Megacon has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose.

The purpose of this policy is to (a) protect Megacon data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures and (c) define the rules for company and personal use.

Scope.

This policy applies to all of Megacon remote workers, permanent, and part-time employees, contractors, suppliers, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data.

Megacon defines "confidential data" as:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Customer leads and sales-related data.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

Device Security.

To ensure the security of all company-issued devices and information, Megacon employees are required to:

- Keep all company-issued devices password-protected. This includes tablets, computers, and mobile devices.
- Secure all relevant devices before leaving their desk.
- Obtain authorization from their manager before removing devices from company premises.
- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.

Personal Use.
Megacon employees should never use personal devices to access company systems.

Email Security.
Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, Megacon requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

Transferring Data.
Megacon recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over Megacon networks.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to Megacon Data protection policy, Data security policy and Computer and Electronic Devices policy.
- Immediately alert the IT department regarding any breaches, malicious software, and/or scams.

Emily Trembath
Operations Director
Megacon Controls Limited

Ronny Totland

Ronny Totland
Managing Director
Megacon AS

Reviewed: April 2023