Cyber Security and Information Policy

Evo Automotive Solutions Ltd referred to as “Evo”

Issue: G | Date: 27.04.26

Approved by MD: 27.04.26

Contents

Policy Introduction

Cyber security threats can damage Evo’s systems, interrupt operations, and harm the company’s reputation. This policy sets out the security measures, responsibilities, and working practices that protect our information, our customers, and our organisation. It aligns with Evo’s Business Continuity arrangements and supports compliance with UK GDPR and industry standards.

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk

Purpose

Protecting information assets includes much more than storing files. It involves the people who use them, the processes that govern them, and the equipment used to access them.

This policy aims to:

- Protect Evo's data, systems and infrastructure.
- Identify cyber security risks and set out appropriate controls.
- Define safe working practices for all staff.
- Set expectations for the use of company and personal devices.
- Support legal and regulatory compliance, including GDPR.
- Explain how breaches are reported and managed.
- Set out consequences for policy violations.

Scope

This policy applies to all individuals who work for or on behalf of Evo. This includes permanent staff, part time staff, warehouse staff, office staff, agency or temporary workers, contractors, and anyone else who is granted access to Evo's systems, data, or equipment as part of their role.

It covers:

- Company issued devices
- Personal devices used for Evo business
- All systems, software, networks, cloud services, and data under Evo's control

---

Information Asset Identification

Evo identifies the key types of information that are important to the business. These include customer and OEM data, supplier and commercial information, employee and HR records, financial data, quality documentation, order and shipment information, and product development material.

The systems and equipment used to store or process this information, such as Microsoft 365, SharePoint, company devices, and cloud backups, are recorded in the IT Inventory List (EVO-0134) and Asset Register.

Each area of the business is responsible for the information it uses, with overall accountability held by management. Information and supporting systems are reviewed at least annually as part of the Business Continuity and Management Review process.

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk

Identification of Security Risks

Evo recognises the following information risks:

- Unauthorised access to systems.
- Loss or theft of devices.
- Data leaks involving customers, suppliers, or internal staff.
- Malware, phishing, spoofing, and other email based threats.
- Weak passwords or shared credentials.
- Inadequate backups or unsecured file storage.
- Misconfigured access permissions.
- Disruption of essential services such as broadband, email, or phone system.

These risks guide the controls and working practices set out in this policy.

Confidential Data

Evo defines confidential data as:

- Financial information not publicly released.
- Customer, supplier, and shareholder information.
- Sales leads, pricing information, and commercial data.
- Production information and new product development.
- Employee personal data, passwords, and HR documents.
- Contracts, legal records, and documents covered by GDPR.

All staff must protect confidential data and only use it for legitimate business purposes.

Hardware/Software

Evo maintains a secure inventory of all company devices and software.
This includes laptops, desktops, mobile devices, OneDrive backups, Microsoft 365 accounts, and security tools.
The inventory is stored in Evo's Master Documents area on SharePoint and updated as part of ongoing security work.

Employees are responsible for the safe use of any device assigned to them.

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk

Implementation of Security Controls

Evo uses several layers of security across devices, accounts, systems, and cloud services. These controls include:

- Microsoft 365 Business Premium security tools.
- Multi Factor Authentication for all accounts.
- Conditional Access rules.
- Microsoft Defender for Endpoint.
- BitLocker encryption on all company devices.
- SharePoint and OneDrive with controlled access.
- Daily Microsoft 365 cloud backups.
- Email authentication standards (SPF, DKIM, DMARC).
- Regular permission and admin role reviews, carried out by our IT provider who retains the appropriate admin rights.
- Audit logging for system activity, monitored by our IT provider.

These measures strengthen Evo's compliance with GDPR and support safe operations.

Evo retains overall accountability for information security. Operational security controls, monitoring, and system configuration are implemented and maintained by the appointed external IT service provider under contractual agreement. Responsibilities are defined within the service agreement and reviewed as part of ongoing IT governance and change management.

Network infrastructure equipment, including routers, switches, and related hardware, must be physically secured against unauthorised access and restricted to authorised personnel only.

Device Security

Company Devices

Employees must:

- Protect all company devices with a password or passphrase.
- Secure devices when leaving for the day or when the office will be unattended. Staff should also lock devices if away from their workstation for an extended period.
- Request approval before removing equipment from Evo premises.
- Passwords must not be shared in day-to-day use. Where shared access is required for operational reasons, passwords must be stored securely and accessed only by authorised staff. Any shared access must be approved by management and used only for legitimate business purposes.
- Keep devices up to date and enable automatic updates.

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk

- Ensure OneDrive desktop and documents backup remains active.

Where supported, devices may use biometric login. Use is encouraged.

Personal Use

Some staff use personal phones or tablets to communicate with the factory in Italy through apps such as WhatsApp or Telegram. Where this is required for business purposes:

- Only business and industry related messages should be sent.
- No confidential or personal data should be shared through these apps.
- Devices must be protected with a passcode or biometric login.
- Staff must report any loss of the device immediately.
- Business conversations must remain professional and should not be deleted if they relate to customer orders or supply chain matters.
- Where possible, staff should move ongoing conversations to Evo's approved systems (email or Teams).
- Photos or screenshots containing confidential or personal data must not be shared through messaging apps.

This allows the business to continue coordinating with the factory while keeping data exposure minimal and controlled.

Email Security

Staff must:

- Check the sender details and avoid suspicious links or attachments.
- Be cautious with unexpected messages, requests for information, or unusual login prompts.
- Report suspicious emails to Operations Support and/or IT immediately.
- Use the secure email hosting and filtering provided through Microsoft Defender.

Email security settings (SPF, DKIM, DMARC, SafeLinks, SafeAttachments) are maintained by IT Services to reduce phishing and spoofing.

Password Management

Employees must:

- Change default passwords before first use.
- Use strong passwords or long passphrases.
- Use different passwords for different systems.
- Enable Multi Factor Authentication on all accounts.

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk

- Avoid writing down or sharing passwords.
- Update passwords immediately if compromise is suspected.

Secure Data Transfer

Employees must:

- Avoid using USB drives unless authorised .
- Transfer confidential data only through Evo's approved systems.
- Confirm the identity and permissions of recipients.
- Follow GDPR and confidentiality requirements at all times.

Approved Network Services

The following network services are authorised for the transfer of company information:

- Microsoft 365 services (Outlook, SharePoint, OneDrive, Teams)
- Corporate email systems
- Approved business portals and cloud-based platforms

All data transferred using these services is protected by encrypted communication protocols (HTTPS/TLS).

Email communications are further protected through SPF, DKIM and DMARC authentication controls.

Where required, additional protection is applied through access-controlled sharing (e.g. restricted SharePoint links and permission-based access).

Use of Messaging Applications

The use of messaging applications (e.g. WhatsApp, Telegram) is permitted only for limited business communication where necessary.

- These applications are not approved for the transfer of confidential or sensitive information
- Sensitive information must only be transferred using approved corporate systems (e.g. Microsoft 365, email, SharePoint)
- Where business communication occurs via messaging apps, conversations should be transferred to approved systems where possible

---

Remote Working Guidelines

Remote staff must:

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk

- Meet their required working hours and deadlines.
- Protect equipment from loss, damage, or unauthorised access.
- Use secure networks and avoid public wifi unless a VPN is active.
- Store files in SharePoint or OneDrive only.
- Report any issues or concerns promptly.

Company equipment remains Evo property and must be returned when requested.

Remote Access

Remote access to Evo systems is not in routine use and is only permitted in exceptional cases.

Where remote access is required:

- access is restricted to authorised users only
- Multi-Factor Authentication (MFA) is enforced
- connections are secured using encrypted protocols
- access is granted and removed in line with access control procedures

All remote access must comply with Evo's security requirements and is subject to periodic review.

Working Environment and Privacy

When working outside Evo premises in exceptional circumstances, employees must take reasonable steps to prevent unauthorised viewing and overhearing of company information.

This includes:

- positioning screens to avoid unauthorised viewing
- using privacy screen filters on laptops where appropriate
- avoiding accessing or discussing sensitive information in public places
- using headsets where necessary to prevent conversations being overheard
- maintaining awareness of surroundings at all times

Mobile working is not standard business practice and is only permitted in exceptional circumstances.

Access Control

Access to systems and files is based on role and business need. Evo uses:

- Microsoft Entra ID for account identity.
- SharePoint permissions for document access.
- Regular reviews of access rights.
- Restrictions on admin roles.

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk

- Conditional Access rules.
- Audit logs for system activity.

Only authorised users may access sensitive information.

Change Management

Significant changes affecting IT systems, security configurations, physical security arrangements, or business-critical processes must be managed in a controlled manner proportionate to the size of the organisation.

Routine operational activities and minor administrative adjustments that do not impact security, data protection, or business continuity do not require recording in the register.

Before implementation, the potential impact of the change on:

- Information security
- Data protection
- Business continuity

must be considered and documented where appropriate.

Significant changes require management approval before implementation.

Emergency changes may be implemented immediately where necessary to protect operations, security, or business continuity. Such changes must be reviewed and recorded retrospectively.

All qualifying changes are recorded in the Change Register (EVO-0011), maintained by Operations Support. The register records a brief description of the change, impact consideration, approval, implementation date, and post-implementation review status.

Evo's information security controls and arrangements are subject to periodic internal reviews, independent assessments, and technical system audits in line with the ISMS Audit Plan.

Reporting and Recovery of Data Breaches

Suspected information security incidents must be reported immediately to management and / or the IT function via telephone or email.

All staff must report:

- Suspicious activity.
- Possible data breaches.
- Malware or unusual system behaviour.

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk

- Lost or stolen devices.

In the event of a breach, Evo will as required:

- Work with the IT provider to secure accounts and stop the attack.
- Reset passwords and isolate affected systems.
- Use Microsoft 365 cloud backups and version history to restore data.
- Activate Business Continuity measures where necessary.
- Notify the Information Commissioner's Office (ICO) and affected individuals when required under UK GDPR, based on the level of risk created by the breach.

Backups, SharePoint storage, Microsoft 365 retention policies, and the 5G emergency router support continued operations during an incident.

Information Security Awareness & Training

Employees receive information security awareness training during onboarding, at regular intervals, and following significant policy changes, incidents, or emerging threats where additional awareness is required.

Training is delivered through awareness communications, brief training sessions, or knowledge checks, depending on the nature of the risk or training requirement. Participation and completion records are retained where applicable.

Relevant changes to information security requirements or policies will be communicated to affected external business partners where applicable, and records of such communications will be retained.

Disciplinary Action

Breaches of this policy may result in:

- Verbal warnings for unintentional breaches.
- Written warnings for repeated or careless behaviour.
- Suspension or dismissal for serious or intentional misuse.

Contractors and third parties may have access removed.

Important

All employees who use company IT equipment must confirm that they have read and understood the policy.

Unit 7, Denbigh Hall, Milton Keynes MK3 7QT, England.
Tel: 01908 64 65 66, Intl: +44 1908 64 65 66, Fax: 01908 64 63 62
Email: sales@evoautomotive.co.uk