EVOGK

Information Security Policy

Including Payment Card and eCommerce Security Requirements

Organisation	EVOGK
Policy Owner	James Howarth
Website	https://evogk.co.uk/
Contact Email	info@evogk.co.uk
Website and Server Provider	Madhouse
Hosting Platform	WP Engine
Policy Date	8 July 2026

Version 1.0

Document Control

Version	Date	Owner	Approved by	Next review
1.0	8 July 2026	James Howarth	James Howarth	8 July 2027, or sooner following a material change

This policy must be reviewed at least annually and whenever there is a significant change to EVOGK's systems, website, payment arrangements, suppliers, business processes or legal and regulatory obligations.

Contents

Introduction

This policy sets out the security requirements that EVOGK applies to confidential, personal, commercially sensitive and payment-related information. It applies to James Howarth, all employees, contractors, temporary workers and third parties who are given access to EVOGK information, systems, devices or services.

EVOGK operates the website https://evogk.co.uk/. Website, hosting and server-related services are supplied and managed by Madhouse using the WP Engine hosting platform. Payment processing services are supplied through Worldpay. EVOGK must not assume that the use of a third-party provider removes its own responsibility to maintain appropriate security controls, complete relevant PCI DSS validation activities and manage supplier risk.

Everyone covered by this policy must read it, understand the requirements relevant to their role and sign the acknowledgement in Appendix A. The policy will be reviewed annually and following any security incident, material system change or change in payment arrangements.

Information Security Policy Statement

EVOGK handles business, customer and account information that must be protected against unauthorised access, disclosure, alteration, loss or destruction. EVOGK is committed to maintaining a secure environment, protecting customer privacy and supporting compliance with applicable data-protection and payment-card requirements.

All personnel must:

- Handle information according to its sensitivity and classification.
- Protect customer, account and payment-related information at all times.
- Use EVOGK systems primarily for authorised business purposes and ensure any limited personal use does not interfere with work or security.
- Keep passwords, authentication devices and user accounts secure and never share credentials.
- Obtain approval before installing software, connecting hardware, creating integrations or granting third-party access.
- Keep work areas clear of sensitive information and lock screens whenever devices are unattended.
- Report suspected security incidents, phishing attempts, unusual account activity, lost devices or accidental disclosures immediately to James Howarth and, where website or server systems may be affected, to Madhouse.
- Complete security awareness training at least annually.

EVOGK reserves the right, where lawful and proportionate, to monitor, access, review, audit, preserve or remove information held on company systems for security, compliance, operational or investigative purposes.

1. Network and eCommerce Security

EVOGK will maintain an up-to-date description or diagram of the systems and third parties involved in the eCommerce payment flow. This must identify, as applicable, the EVOGK website, website administration systems, hosting platform, payment gateway or hosted payment page, plugins or integrations, and connections to third parties.

- The website and server environment is managed by Madhouse using WP Engine.
- Payment processing is provided through Worldpay. EVOGK must use an approved integration method and must not intentionally collect or store full payment-card details on its own website, email systems or business devices.
- Security updates, supported software versions, access restrictions, malware controls, logging and vulnerability management must be maintained for the website environment.
- External vulnerability scanning must be carried out where required by the applicable PCI DSS validation route. Where an Approved Scanning Vendor scan is required, evidence of passing scans should be retained for at least 18 months.
- Any failed vulnerability scan or significant security finding must be reviewed promptly, remediated according to risk and re-tested where required.
- The payment flow and relevant security controls must be reviewed after significant website, hosting, plugin, checkout or payment-gateway changes.

2. Acceptable Use

EVOGK aims to maintain a culture of openness and trust while protecting the organisation, its customers and its suppliers from accidental or deliberate harm. Users must exercise good judgement and comply with the following requirements:

- Use only approved devices, software, accounts and cloud services for EVOGK work.
- Prevent unauthorised access to confidential, personal, account and payment-related information.
- Use strong, unique passwords and multi-factor authentication wherever available.
- Keep computers, laptops and mobile devices protected by screen locks and automatic timeout.
- Do not install unauthorised software, browser extensions, remote-access tools, wireless devices or storage devices.
- Use particular care when opening links or attachments, especially where the sender is unknown or the message creates urgency.
- Do not use EVOGK resources for illegal, offensive, discriminatory, threatening, defamatory, obscene or harassing activity.
- Report any suspected tampering, substitution or unexplained change affecting payment devices or website checkout functions.

3. Protection of Stored Data

- EVOGK must not store full primary account numbers, card verification values, magnetic-stripe or chip-equivalent track data, PINs or encrypted PIN blocks in electronic or paper form.
- Payment-card data must not be entered into or retained in email, chat, support tickets, spreadsheets, documents, screenshots or customer notes.
- Where a legitimate business record displays a card number, it must be masked so that no more than the first six and last four digits are visible, unless a stricter display rule applies.
- Any sensitive information retained for a valid business purpose must be protected against unauthorised access and retained only for as long as necessary.
- Backups, exports, test environments and developer copies must not contain prohibited payment-card data.

It is strictly prohibited to store sensitive authentication data after authorisation, including CVV/CVC/CID values, track data and PIN data.

4. Information Classification

Information must be handled according to the following classification levels:

Classification	Examples	Required handling
Confidential	Customer personal data, account information, security credentials, financial information, contracts, incident records.	Access limited to authorised persons; secure storage and transfer; no unauthorised disclosure.
Internal Use	Internal procedures, pricing, operational information and non-public business records.	Share only with people who have a business need.
Public	Approved website content, published marketing materials and public contact information.	May be shared publicly once approved.

5. Access to Account and Cardholder Data

- Access must be authorised, role-based and limited to the minimum required for the person's duties.
- EVOGK personnel must not have routine access to full card details. Worldpay should handle payment-card entry and processing through the approved payment flow.
- Customer and order information must only be accessed for legitimate business purposes.
- Access must be removed promptly when a person leaves EVOGK or no longer requires it.
- EVOGK will maintain a list of third-party service providers that can affect the security of account data or the payment environment.
- Contracts or service terms must define relevant responsibilities, including each provider's responsibility for systems or data it manages.
- EVOGK will carry out appropriate due diligence before appointing relevant third parties and will monitor their security or PCI DSS status where applicable.
- A responsibility matrix should be maintained where needed to distinguish EVOGK's responsibilities from those of Worldpay, Madhouse, WP Engine and any other relevant provider.

6. Physical Security

Physical access to devices, records and areas containing confidential information must be restricted to authorised individuals.

- Paper records containing confidential information must be secured when unattended.
- Visitors must be supervised where they could gain access to confidential information or business systems.
- Devices used to access EVOGK systems must be protected from theft, unauthorised use and casual viewing.
- Any payment terminal or point-of-interaction device used by EVOGK must be recorded in Appendix B and inspected for tampering or substitution.

- Personnel must verify the identity and authority of anyone claiming to install, repair, replace or inspect a payment device.
- Lost or stolen devices must be reported immediately.

7. Protection of Data in Transit

- Payment-card details must never be sent through ordinary email, text message, chat, collaboration tools or support tickets.
- Confidential information must be transmitted only through approved, appropriately protected services.
- EVOGK's website must use HTTPS and valid encryption certificates for customer and administrative connections.
- Administrative access must use secure, encrypted connections and multi-factor authentication where available.
- Physical transfer of confidential media must be authorised, recorded and carried out using a secure and traceable method.

8. Secure Disposal of Data

- Information must be securely destroyed when it is no longer required for legal, contractual or legitimate business purposes.
- Paper containing confidential information must be cross-cut shredded or destroyed by an approved confidential-waste provider.
- Electronic storage media must be securely erased using an accepted method or physically destroyed before disposal or reuse.
- Information awaiting destruction must be stored securely and access restricted.
- EVOGK must periodically review retained customer, order, financial and operational information and remove records that are no longer required.
- Prohibited payment-card data discovered in any system or record must be removed securely and treated as a potential security incident.

9. Security Awareness and Procedures

- All personnel must receive security awareness information when they join and at least annually thereafter.
- Training must cover phishing, passwords, multi-factor authentication, secure handling of customer data, incident reporting and payment-card security relevant to the person's role.
- This policy must be made available to all personnel and acknowledged using Appendix A.
- Third parties with access to EVOGK systems or data must be subject to appropriate contractual and security requirements.
- This policy and supporting procedures must be reviewed annually and after material changes or incidents.

10. Payment Card Security Incident Response Plan

10.1 Incident Response Roles

Role	Named contact	Responsibility

Incident Lead / Information Security Officer	James Howarth	Coordinates the EVOGK response, records decisions and authorises notifications.
Website and Server Support	Madhouse	Assists with website, hosting, access, logging, containment and technical investigation.
Hosting Platform	WP Engine	Provides hosting-platform support and relevant security information in accordance with its service arrangements.
Payment Provider	Worldpay	Provides payment-specific incident guidance and coordinates card-industry reporting where required.

10.2 Reporting and Initial Response

- Anyone who suspects a security incident must report it immediately to James Howarth. Where the website, hosting, checkout or server environment may be affected, Madhouse must also be contacted without delay.
- Do not delete files, wipe devices, alter logs, contact a suspected attacker or attempt an uncoordinated investigation.
- Record the date and time, systems involved, symptoms observed, people notified and actions taken.
- Preserve relevant logs, emails, screenshots and other evidence in a secure manner.

10.3 Containment, Investigation and Recovery

- Isolate affected systems, accounts, plugins, integrations or devices where this can be done safely without destroying evidence.
- Reset or revoke compromised credentials and sessions as directed by the incident lead or technical provider.
- Review available logs and security alerts and determine the likely scope, entry point and affected data.
- Engage Worldpay and any required qualified forensic or security specialist where payment-card compromise is suspected.
- Do not restore normal service until the incident lead and relevant technical providers are satisfied that the immediate threat has been contained.
- After recovery, document lessons learned, update controls and verify that remedial actions are effective.

10.4 Notifications

James Howarth will coordinate notifications with Worldpay, Madhouse, WP Engine, insurers, legal advisers, regulators, law enforcement and affected individuals as appropriate. EVOGK must follow Worldpay's current incident-reporting instructions and any applicable legal notification deadlines. Card brands should not normally be contacted independently unless directed by Worldpay, EVOGK's acquiring bank, legal advisers or an authorised investigator.

10.5 Incident Record

Incident reference	
Date and time detected	
Reported by	
Systems or data affected	

Actions and notifications	
Closure and lessons learned	

11. Transfer of Sensitive Information and Third-Party Management

- Relevant third parties must provide services under appropriate terms, service levels or agreements.
- Providers with access to EVOGK systems or confidential information must apply appropriate security controls and use the information only for authorised purposes.
- Providers that can affect the payment environment must acknowledge their responsibility for the security of the systems or data they manage.
- EVOGK will maintain a list of relevant third-party providers in Appendix C and review it at least annually.
- EVOGK will seek evidence of applicable PCI DSS compliance or other security assurance from relevant providers where appropriate.
- Third-party access must be removed when no longer needed.

12. User Access Management

- New access must be requested and approved by James Howarth or an authorised manager.
- Each person must use an individual account. Shared or generic accounts should be avoided and must be specifically approved where unavoidable.
- Access rights must reflect the person's role and follow the principles of least privilege and need to know.
- Administrative access to the website, hosting, payment and business systems must be restricted and protected by multi-factor authentication wherever available.
- Access must be reviewed periodically and immediately when responsibilities change.
- When a person leaves, all accounts, sessions, application passwords, API keys and remote access must be disabled or revoked promptly.

13. Access Control

- All access to EVOGK systems must be authenticated and authorised.
- Passwords must be long, unique and not reused across services. Password managers should be used where appropriate.
- Multi-factor authentication must be enabled on administrative and other high-risk accounts wherever the service supports it.
- Privileged access must be limited to authorised individuals and used only when required.
- Website administrator, hosting, payment-provider, email and domain-management access must be reviewed at least annually.
- Remote access must use approved secure methods. Uncontrolled external access is prohibited.
- Users must report suspected unauthorised access, unexpected password-reset messages or unusual account activity immediately.
- Access reviews and material access changes should be recorded.

Appendix A - Agreement to Comply With Information Security Policies

I agree to take reasonable precautions to protect EVOGK information and information entrusted to EVOGK by customers, suppliers and other third parties. I will not disclose confidential information to unauthorised persons or use it for unauthorised purposes.

I confirm that I have access to EVOGK's Information Security Policy, have read and understood it, and agree to follow the policy and related procedures. I understand that failure to comply may result in disciplinary action, termination of access or contract, and possible civil or criminal consequences.

I agree to report actual or suspected security incidents, policy breaches, lost devices, phishing attempts and accidental disclosures promptly to James Howarth.

Employee / Contractor Name: _____

Role / Department: _____

Signature: _____

Date: _____

Appendix B - List of Devices

Asset / Device	Description	Owner / User	Location	Serial / Identifier	Status / Last check

Appendix C - Third-Party Service Providers

Provider	Contact / Website	Services	Can affect payment security?	Assurance / PCI status	Review date
Worldpay	Worldpay merchant support	Payment gateway and payment processing	Yes	Record current PCI DSS or service assurance evidence supplied by provider	
Madhouse	Website and server support provider	Website management,	Yes	Maintain contractual	

		technical support and server-related services		responsibilities and review relevant security controls	
WP Engine	https://wpengine.com/	Managed hosting platform for the EVOGK website	Yes	Maintain relevant hosting security and assurance evidence	

Appendix D - POI and P2PE Management

This appendix applies only if EVOGK uses a physical payment terminal, point-of-interaction device or validated point-to-point encryption solution. If EVOGK is online-only and does not use such devices, record this appendix as not applicable.

- Maintain an inventory including make, model, location, serial number and responsible person.
- Secure devices against tampering, substitution and unauthorised removal.
- Inspect devices regularly and record the inspection.
- Verify the identity of engineers or third parties before allowing installation, replacement or maintenance.
- Keep device software and configuration under authorised control.
- Report suspicious behaviour, damage, altered seals, unexpected cables or device substitution immediately.

Appendix E - eCommerce Configuration and Hardening

This appendix applies to EVOGK's eCommerce website and the systems that can affect the security of the checkout and payment flow.

Standard Configuration

- Maintain supported versions of the content-management system, themes, plugins and integrations.
- Remove or disable unused accounts, plugins, themes, services and integrations.
- Change or disable vendor-default credentials and settings.
- Use HTTPS throughout the website and protect administrative interfaces.
- Restrict administrative access and require multi-factor authentication where available.

Change and Access Control

- Only authorised personnel or approved suppliers may make website, hosting, checkout or payment changes.
- Changes must be tested and reviewed before or immediately after deployment according to risk.
- Administrative actions and significant changes should be logged or otherwise traceable.
- Access belonging to former staff, contractors or suppliers must be removed promptly.

Vulnerability and Patch Management

- Monitor recognised security sources and supplier notifications for vulnerabilities affecting the website and its dependencies.
- Assess findings according to risk and address critical or high-risk vulnerabilities without undue delay.
- Apply applicable security updates promptly and normally within one month of release, or sooner where the risk requires it.
- Carry out vulnerability scanning and malware monitoring appropriate to the environment, including ASV scanning where required by EVOGK's PCI DSS validation route.
- Re-test remediated vulnerabilities and retain evidence where required.

Payment Page Security

- Use only the approved Worldpay payment integration and authorised checkout scripts.
- Review third-party scripts and plugins that load on payment or checkout pages.
- Investigate unexpected changes to payment-page content, redirects, scripts, domains or checkout behaviour immediately.
- Maintain backups and recovery procedures, but do not restore a compromised environment without addressing the cause of compromise.

End of document