

GCB FINTECH — INFORMATION SECURITY AND DATA BREACH STATEMENT

DOCUMENT CONTROL & METADATA

Platform: GCB Fintech — <https://gcbfintech.digital>
Version: 1.26 | Effective Date: October 20, 2026
Contact: customerservice@gcbfintech.digital

8. Information Security and Data Breach Statement

8.1 Security programme

GCB Fintech maintains administrative, technical and physical safeguards appropriate to the sensitivity and risk of the information and services it handles. Controls may include access management, least-privilege permissions, multi-factor authentication, encryption in transit and at rest where appropriate, secure development practices, logging, monitoring, vulnerability management, backups, business continuity, staff training, supplier due diligence and incident-response procedures.

Security controls are risk-based and cannot guarantee that a website, account, communication channel, wallet, third-party provider or transaction will never be compromised.

8.2 User responsibilities

Users must keep credentials, authentication devices, recovery codes, private keys and transaction details confidential; use secure devices and networks; apply available security updates and multi-factor authentication; verify addresses and instructions; and report suspected compromise promptly. GCB Fintech will not ask a user to disclose a private key, recovery phrase or password.

8.3 Incident response

A suspected security event is assessed, contained and investigated under the applicable incident-response process. We may suspend access, stop transactions, reset credentials, isolate systems, preserve evidence, engage specialists and notify affected providers or authorities.

Where applicable law requires notification, we will notify affected individuals and regulators within the required timeframe and with the information required by law. Notification may be delayed or limited where necessary to protect an investigation, prevent further harm, comply with law or avoid compromising security. This statement does not promise that every event will result in a public notice.

8.4 Reporting a suspected incident

Report suspected unauthorised access, phishing, account compromise, fraudulent instruction, data exposure or other security incident immediately to security@gcbfintech.digital or via the platform security reporting portal. Include the account identifier, date and time, relevant transaction reference and a description of the issue, but do not send passwords, private keys or recovery phrases.

8.5 Relationship with the Privacy Policy

Personal-data breaches are handled under the applicable privacy laws, the Privacy Policy and the responsible entity's incident-response procedures. Where the breach creates a legally defined risk of harm, the responsible entity will assess notification and reporting duties under the law applicable to the affected information and entity.