Cyber Security Policy

Issue Date: 23/04/2026 Issue Number: 1

Introduction

Cyber security is an important part of our overall risk management and operational resilience. FlipFix Limited is committed to protecting its systems, devices, networks, information and digital services against unauthorised access, misuse, loss, disruption, damage or disclosure.

Effective cyber security helps safeguard our operations, commercially sensitive information, personal data and reputation. We therefore seek to maintain reasonable and proportionate safeguards and to encourage secure working practices across the business.

Application of this Policy

This policy applies to all directors, officers and employees, as well as temporary workers, contractors, consultants and any other individual who are given access to Company systems, devices, networks or information in connection with their work.

It applies to the use of Company technology, software, email, messaging systems, internet services, stored information and related resources, whether used on Company premises, remotely or through any other approved working arrangement.

Where third parties are permitted to access Company systems or information, they are expected to meet the security standards relevant to that access.

Legal and Regulatory Framework

This policy supports our approach to complying with applicable legal, regulatory and contractual obligations relating to cyber security, confidentiality, privacy, data protection and the secure use of information.

In implementing this policy, we will comply with relevant legislation, regulatory expectations, customer commitments and recognised good practice. This policy should be read alongside any related requirements concerning confidentiality, acceptable use, privacy, data protection, intellectual property and standards of professional conduct.

Responsibilities for Management and Employees

Senior Management has oversight of our cyber security arrangements and is responsible for ensuring that suitable measures, controls and procedures are maintained. This includes taking reasonable steps to protect systems and information, manage access to technology and data, support secure use of Company resources, and ensure that security concerns are addressed appropriately. Senior Management is also responsible for promoting awareness of cyber risk and keeping arrangements under review.

Employees and other individuals covered by this policy are expected to use Company systems and information carefully, responsibly and in accordance with instructions issued by FlipFix Limited. They must co-operate with security requirements, protect the confidentiality of Company information, and avoid any act or omission that could expose our systems, services or data to unnecessary risk.

No individual may knowingly, recklessly or negligently compromise the security, availability, integrity or confidentiality of Company systems or information.

Access, Systems and Acceptable Use

Company systems, devices, software and information must be used for legitimate business purposes, subject to any limited personal use that we may permit from time to time.

Access credentials, including passwords and similar login information, must be kept secure and must not be shared with unauthorised persons. Individuals must take reasonable care to prevent unauthorised access to Company accounts, systems and information.

No software, application, program, plug-in or similar tool may be installed on Company equipment without prior authorisation. Individuals must not attempt to disable security settings, work around access controls, use unauthorised platforms for Company business, or access systems or data beyond the permissions granted to them.

All systems, records, software, information and other materials created, stored or used in the course of employment or engagement remain the property of FlipFix Limited unless expressly agreed otherwise. On request, and in any event on termination of employment or engagement, all Company information and assets must be returned or made available to us.

Email, Messaging and Internet Use

Email, messaging and internet access are provided primarily to support communication, service delivery and business operations. These tools must be used in a way that is responsible and does not create avoidable security, legal, operational or reputational risk.

Individuals must not use Company systems to distribute malicious material, inappropriate content, unauthorised software, confidential information without authority, copyright-infringing material, chain communications, or material that is unlawful, offensive, defamatory, discriminatory, abusive or otherwise inconsistent with Company standards or interests.

Care should be taken when dealing with unexpected messages, links, attachments or requests for information, particularly where the source is unfamiliar, suspicious or unverified. Concerns of this kind must be reported promptly to a Director, or through the appropriate internal reporting procedure.

Any limited personal use of email, messaging or internet services must remain sensible, must not interfere with work, and must not consume unreasonable resources or introduce additional risk. We reserve the right to restrict such use where necessary.

Confidential Information and Data Handling

Information held by FlipFix Limited, including customer information, internal business information and personal data, must be handled with due care and only for authorised purposes. It must not be copied, shared, transferred, disclosed or stored in a manner that exposes it to unnecessary risk.

Access to confidential information and personal data must be limited to those with a legitimate business reason and appropriate authority. Where information is shared externally, this must be done in accordance with Company requirements, legal obligations and any relevant contractual arrangements.

We will maintain reasonable and proportionate organisational and technical measures to support the secure handling of information. Those measures do not remove the responsibility on individuals to follow Company procedures and act with appropriate caution.

Reporting Concerns and Security Incidents

Any suspected weakness, suspicious activity or actual security issue must be raised without delay. This includes, for example, phishing attempts, unauthorised access, lost data, compromised devices, misuse of systems or any other event that may affect the security of Company systems or information.

Reports made under this policy will be considered seriously and dealt with according to the nature of the issue and the level of risk involved. We may take whatever steps are reasonably necessary to contain, assess, investigate, correct or manage a security issue, including restricting access to systems, accounts or devices where appropriate.

Delays in reporting may increase the risk of harm to FlipFix Limited, its customers and other affected parties. Prompt escalation is therefore expected.

Monitoring and Review

Where lawful, legitimate and proportionate, we may monitor or review the use of our systems, devices, email, messaging and internet services for purposes including security, business continuity, compliance, investigation of suspected wrongdoing and protection of Company assets and information.

We will keep this policy and the supporting arrangements under review to ensure they remain suitable, up to date and aligned with legal, regulatory and operational requirements. Reviews may also be carried out following relevant changes to systems, working practices, supplier arrangements, business activities or identified security incidents.

Employees are encouraged to raise suggestions that may help strengthen our cyber security arrangements.

Approval and Ownership

This policy is owned by Senior Management, who are responsible for overseeing its implementation and ensuring that appropriate measures, procedures and standards are maintained.

The policy has been approved by the Board of Directors.

For any questions regarding this policy, please contact a Director.