This is our

Cyber Security

statement 2023/2024

LIQUID FRIDAY

LIQUID FRIDAY

CONTENTS

LIQUID FRIDAY

Introduction

This statement provides an overview of Liquid Friday's approach to Cyber Security.

Security Policy

Our policies address the handling of personal, sensitive and confidential information. Policies are reviewed regularly and communicated to all staff.

Our organisational information security approach & compliance standards

In addition to information security, our policies cover data protection and the Computer Misuse legislation. We are dedicated to cyber security, as well as a legal, compliance and internal audit team. To demonstrate our commitment to Cyber Security to our customers and staff we are currently undertaking UK Cyber Essentials accreditation.

Third Parties

Like most organisations, we use third parties to host or process customer information. We conduct technical due diligence against these third parties for their cyber risks and ensure our legal agreements with them appropriately address security and data handling.

In addition, we only process data with the EEA to ensure the maximum level of safeguards. If data was ever going to be processed outside the EEA, we will ensure appropriate safeguards (such as model clauses) are in place. In addition, we would undertake due diligence checks to ensure Data Protection standards reflect GDPR best practice.

Employee security practices

We undertake comprehensive checks of our employee's ID, references, and right to work. Cyber security is covered at employee inductions and training is offered on an ongoing basis (at least annually), including bespoke training if relevant to the role.

We also run regular phishing tests against staff. Violations of relevant policies could result in HR process enacting disciplinary action, up to and including dismissal.

Physical office & data centre facilities

Our major offices and all data centre facilities we use have entry controls and CCTV at entry/exit points, and we have controls in place to protect our systems from unauthorised access. These data centres are in the UK and adhere to strict GDPR best practice.

Documentation & process

We have documented operational procedures and monitoring. Our change control process includes audit trails of changes.

Infrastructure protection

We install anti-virus & malware protection on laptops and desktops as well as disk encryption on laptops. We install anti-virus & malware protection on all servers. Our policy is to apply critical security patches immediately, and less severe updates within one month on servers, where practical.

Our user and system networks are segregated. We deploy Network Intrusion Detection systems, run regular vulnerability scans, proactively scan encrypted connection via our Transport Layer Security configurations, and source code for vulnerabilities. Security logs are collected centrally within our Security Event Information Management system.

Data protection

We encrypt all public system and internal traffic in transit to international standards. It is our policy to encrypt at rest where possible and practical. We dispose of old equipment securely and ethically. We limit access to production environments to only those who need access and have environments for development and testing.

Access control

We have a standard starters and leavers process. We centrally manage access to all services. We use two-factor authentication wherever possible, especially for administrative access on key systems and for all staff using our remote access VPN.

Our users have named accounts, and we prohibit shared users. We log activity and access for audit reasons and have password complexity and rotation policies in place. Users who have privileged or network access are reviewed on a regular basis and those who no longer need this access are removed.

Internal processes

Security requirements and design are considered for all projects and products, and we follow secure development practices. Where we do store user credentials (passwords) they are hashed. We use a third party to run periodic penetration tests of our systems.

Business & incident management

We have cyber security incident response policies and plans in place. These cover detection, response, and reporting. We also have a 24×7 incident team. We run war-games and retrospectives to improve the process and practices, and our business continuity and disaster plans are regularly tested.

This statement has been reviewed and approved by the Liquid Friday Board and is owned by the Chief Operating Officer.

The statement will be reviewed regularly and updated.