MJM Technology

Acceptable Use Policy

Version 1.0 | Effective January 2025

IT · Networking · Security

This Acceptable Use Policy forms part of the MJM Technology Customer Terms and Conditions (v1.1). It is incorporated by reference into all Quotes, Orders, and Agreements issued by MJM Technology.

1. Purpose and Scope

1.1 This Acceptable Use Policy ("AUP") sets out the rules governing how customers and their authorised users may use the services, systems, networks, hardware, and infrastructure provided or managed by MJM Technology ("Services").

1.2 This AUP applies to all customers of MJM Technology, including their employees, contractors, and any other authorised users who access or use the Services (collectively "Users").

1.3 This AUP is designed to protect MJM Technology's infrastructure, other customers, third parties, and the Customer's own business from misuse, security threats, and legal exposure.

1.4 This AUP should be read alongside the MJM Technology Customer Terms and Conditions ("T&Cs"). Capitalised terms used in this AUP have the same meanings as defined in the T&Cs unless otherwise stated here.

> *T&Cs Reference — Clause 1.1 (Definitions) and Clause 1.3 (Order of Precedence): In any conflict between this AUP and the T&Cs, the T&Cs shall take precedence.*

1.5 This AUP is published on the MJM Technology website and is incorporated by reference into all Quotes and Orders. By placing an Order or accepting a Quote, the Customer confirms that it has read and agrees to this AUP on behalf of itself and all its Users.

> *T&Cs Reference — Clause 2.1 (Orders / Incorporation by Reference): Acceptance of a Quote or Order constitutes acceptance of both the T&Cs and this AUP without the need for a separate signature.*

2. Who This Policy Applies To

1.6 This AUP applies to all of the following in relation to the Customer's use of the Services:

(a) the Customer organisation itself;

(b) all employees and directors of the Customer;

(c) contractors, temporary staff, and consultants working for or on behalf of the Customer;

(d) any third party granted access to the Services by the Customer; and

(e) any device or system connected to MJM Technology-managed networks or infrastructure.

1.7 The Customer is responsible for ensuring that all Users are made aware of, and comply with, this AUP. Breach of this AUP by any User will be treated as a breach by the Customer.

> *T&Cs Reference — Clause 7.1(h): The Customer is responsible for ensuring that its authorised users comply with the Terms and Conditions, including this AUP.*

3. Permitted Use

1.8 The Services may only be used for lawful business purposes in connection with the Customer's normal commercial activities.

1.9 Permitted activities include:

(a) accessing business applications and cloud services for day-to-day operations;

(b) sending and receiving business communications via email and messaging platforms;

(c) using MJM Technology-managed networks and connectivity for legitimate business internet access;

(d) remotely accessing the Customer's own systems via MJM Technology-provided VPN or remote access tools, in accordance with clause 5 of this AUP; and

(e) using hardware and software supplied or managed by MJM Technology for the purposes stated in the relevant Order.

1.10 The Customer acknowledges that MJM Technology provisions and configures services specifically for the Customer's agreed business use. Any use outside this scope must be agreed in writing with MJM Technology before commencing.

4. Prohibited Activities

The following activities are strictly prohibited. This list is not exhaustive — MJM Technology reserves the right to treat any activity that causes harm, risk, or reputational damage as a breach of this AUP.

4.1 Security Circumvention

1.11 Users must not bypass, disable, modify, or attempt to circumvent any security control, policy, or configuration implemented and managed by MJM Technology, including:

(a) disabling, reconfiguring, or bypassing firewall rules, content filtering, or intrusion detection/prevention systems;

(b) attempting to access network segments, systems, or data outside the User's authorised scope;

(c) installing unapproved software or tools designed to bypass security controls (e.g. proxy bypassing tools, VPN clients not provided by MJM Technology); or

(d) disabling endpoint protection, logging agents, or monitoring tools deployed by MJM Technology as part of a managed service.

> *T&Cs Reference — Clause 7.2(b): The Customer shall not introduce viruses, malware, or other harmful code into MJM Technology's systems or networks. Clause 11.4(c): Breach of the AUP is grounds for immediate suspension of Services.*

4.2 Credential and Access Sharing

1.12 Users must not share credentials, access tokens, or authentication details provided by or through MJM Technology, including:

(a) sharing usernames, passwords, or multi-factor authentication codes with any other person, including colleagues, unless explicitly authorised under a shared account arrangement agreed with MJM Technology;

(b) providing third parties (including contractors, partners, or clients) with VPN access, remote desktop credentials, or any network access credentials supplied by MJM Technology without prior written consent from MJM Technology;

(c) allowing a single named-user licence or account to be used by more than one individual; or

(d) storing credentials in insecure locations such as unencrypted documents, spreadsheets, or shared drives accessible beyond the intended user.

> *T&Cs Reference — Clause 9 (Data Protection): Sharing credentials may constitute a personal data breach. Clause 7.1(d): The Customer is responsible for procuring and securing adequate network access.*

4.3 Unauthorised Devices

1.13 Users must not connect any device to an MJM Technology-managed network or infrastructure without prior authorisation, including:

(a) personal laptops, tablets, smartphones, or mobile devices not registered with MJM Technology or listed in an Order;

(b) network equipment such as routers, switches, wireless access points, or repeaters installed without MJM Technology's knowledge or approval;

(c) IoT devices, smart devices, or any equipment capable of connecting to the network that has not been declared to MJM Technology; or

(d) any device belonging to a third party, visitor, or contractor without prior written approval.

1.14 Connecting an unauthorised device may compromise network security, invalidate security configurations, and create vulnerabilities across the Customer's environment. MJM Technology accepts no liability for incidents arising from unauthorised device connections.

> *T&Cs Reference — Clause 13.5: MJM Technology's liability is limited where incidents arise from the Customer's failure to maintain a secure environment. Clause 7.4: MJM Technology is not liable for costs arising from Customer acts or omissions.*

4.4 Illegal and Harmful Activities

1.15 Users must not use the Services for any illegal, fraudulent, harmful, or malicious purpose, including:

(a) transmitting, storing, downloading, or distributing material that is unlawful, offensive, defamatory, discriminatory, or in breach of any third party's rights;

(b) engaging in, facilitating, or enabling cybercrime, including phishing, social engineering, ransomware distribution, or any form of fraud;

(c) accessing, attempting to access, or interfering with systems, networks, or data belonging to third parties without authorisation;

(d) using MJM Technology-managed infrastructure for cryptocurrency mining, distributed computing, or any resource-intensive activity outside the agreed service scope;

(e) sending unsolicited bulk communications (spam) or conducting mass marketing activities without appropriate consent in breach of applicable law; or

(f) infringing the intellectual property rights of any third party, including the unauthorised copying, distribution, or use of software, media, or content.

4.5 Network and Infrastructure Misuse

1.16 Users must not take any action that could degrade, disrupt, or overload MJM Technology-managed networks or services, including:

(a) intentionally generating excessive traffic volumes beyond the Customer's contracted service scope;

(b) running unauthorised servers, network services, or peer-to-peer file sharing applications on managed networks;

(c) modifying, reconfiguring, or interfering with any managed hardware or software supplied by MJM Technology; or

(d) attempting to test, probe, or scan network security without prior written authorisation from MJM Technology (including penetration testing — see clause 6).

5. Credential and Access Management

1.17 The Customer is responsible for managing access to all systems and services within its environment, whether managed by MJM Technology or not.

1.18 The Customer shall ensure that:

(a) all User accounts are unique to individuals and not shared;

(b) accounts for leavers or role-changers are disabled or modified promptly — MJM Technology recommends within 24 hours of the change taking effect;

(c) strong passwords or passphrases are enforced in line with current NCSC guidance (minimum 12 characters or three random words);

(d) multi-factor authentication (MFA) is enabled on all systems where MJM Technology has implemented or recommended it; and

(e) administrative or privileged accounts are used only for their intended purpose and not for routine day-to-day activity.

1.19 MJM Technology will not be liable for any security incident, data loss, or service disruption arising from the Customer's failure to manage access appropriately in accordance with this clause.

> *T&Cs Reference — Clause 7.1(e): The Customer must nominate an appropriately skilled contact. Clause 13.5: Liability is capped by the PI Insurance limit — incidents arising from Customer access failures may reduce MJM Technology's liability further.*

6. Penetration Testing and Security Scanning

1.20 The Customer must not conduct, commission, or permit any penetration test, vulnerability scan, security assessment, or any form of simulated attack against MJM Technology-managed networks, systems, or infrastructure without first obtaining MJM Technology's express prior written consent.

1.21 Where consent is granted, MJM Technology will agree the scope, timing, and conditions in writing before any testing commences. Testing conducted outside the agreed scope will be treated as a breach of this AUP.

1.22 MJM Technology may itself conduct scheduled security assessments and vulnerability scans of managed infrastructure as part of the Services. The Customer will be notified in advance where this may cause disruption.

> *T&Cs Reference — Clause 4.5 (Prohibited Activities): Attempting to impair or probe systems without authorisation is a breach of the Customer Obligations. Clause 11.4: Grounds for immediate suspension.*

7. Network Monitoring and Traffic Inspection

1.23 Where network monitoring is included in the Customer's Order as part of a Managed Service, MJM Technology will monitor network traffic, system logs, and security events across managed infrastructure. This may include full traffic inspection for security purposes.

1.24 The purpose of monitoring is to:

(a) detect and respond to security threats, anomalies, and incidents;

(b) ensure compliance with this AUP and the T&Cs;

(c) maintain service performance and integrity; and

(d) provide the Customer with reporting and visibility as agreed in the Order.

1.25 The Customer acknowledges that network traffic generated by Users on MJM Technology-managed networks may be inspected, logged, and retained for security and operational purposes. MJM Technology will handle any personal data identified during monitoring in accordance with Clause 9 of the T&Cs (Data Protection).

1.26 The Customer is responsible for informing its Users that network activity on company systems and MJM Technology-managed infrastructure may be monitored. This is a legal requirement under UK employment and data protection law and MJM Technology accepts no liability for the Customer's failure to notify its Users.

1.27 Monitoring data collected by MJM Technology is used solely for delivering the Services and will not be shared with third parties except where required by law, or as necessary to engage NOC/SOC Partners in delivering the Services.

T&Cs Reference — Clause 9 (Data Protection): MJM Technology acts as Data Processor for personal data identified during monitoring. Clause 6.4: MJM Technology may use NOC/SOC Partners to deliver monitoring Services. Schedule 2, Clause 2.3: NOC/SOC Partners are subject to equivalent data protection obligations.

8. Customer Responsibilities

The following responsibilities rest with the Customer and are outside the scope of MJM Technology's managed services unless explicitly included in an Order. MJM Technology will not be liable for incidents or losses arising from the Customer's failure to meet these responsibilities.

8.1 Staff Security Awareness Training

1.28 The Customer is responsible for ensuring that all Users receive appropriate security awareness training. This is a critical control in defending against phishing, social engineering, and human-error-driven security incidents — the most common cause of breaches in SMB environments.

1.29 As a minimum, MJM Technology recommends that the Customer's Users are trained on:

- recognising and reporting phishing and suspicious emails;
- safe password and credential management practices;
- the risks of connecting personal or unauthorised devices to company networks;
- what to do (and who to contact) in the event of a suspected security incident; and
- the requirements of this AUP, particularly the prohibitions in Section 4.

1.30 MJM Technology accepts no liability for security incidents that are attributable, in whole or in part, to a User acting in a manner that security awareness training would reasonably have prevented.

T&Cs Reference — Clause 13.3: MJM Technology has no liability for indirect losses. Clause 7.2: The Customer indemnifies MJM Technology against losses arising from User breaches.

8.2 Non-MJM Technology Devices and Network Equipment

1.31 Where the Customer operates, owns, or has responsibility for devices, network equipment, or systems that are not covered by an MJM Technology Order ("Out-of-Scope Equipment"), the Customer is solely responsible for:

(a) keeping Out-of-Scope Equipment updated with current firmware, operating system patches, and security updates;

(b) applying appropriate security configurations to Out-of-Scope Equipment to prevent it from becoming a vector for attack against MJM Technology-managed infrastructure;

(c) notifying MJM Technology of any Out-of-Scope Equipment connected to networks that MJM Technology manages, so that appropriate network segmentation or controls can be considered; and

(d) ensuring Out-of-Scope Equipment complies with the prohibitions in Section 4.3 of this AUP.

1.32 MJM Technology strongly recommends that the Customer discloses all network-connected devices and equipment to MJM Technology at the outset of the relationship and whenever changes occur. Undisclosed equipment may create vulnerabilities that MJM Technology cannot protect against.

1.33 MJM Technology accepts no liability for security incidents, outages, or degradation of managed services caused by Out-of-Scope Equipment that was not disclosed to or supported by MJM Technology.

T&Cs Reference — Clause 7.1(c): The Customer is responsible for maintaining its own computing environment. Clause 13.5: MJM Technology's total liability is limited to its PI Insurance level — incidents arising from Out-of-Scope Equipment may further reduce MJM Technology's liability.

9. Data and Confidentiality

1.34 Users must handle data — whether belonging to the Customer, its clients, or third parties — in accordance with applicable data protection law, including the UK GDPR and Data Protection Act 2018.

1.35 Users must not:

(a) transmit, store, or process personal data or sensitive business data using systems or channels not approved for that purpose;

(b) share confidential business information, client data, or personal data with unauthorised parties via MJM Technology-managed systems; or

(c) attempt to access data belonging to other MJM Technology customers or any third party.

1.36 The Customer is responsible for classifying its own data and ensuring that Users understand what data may and may not be transmitted or stored on managed infrastructure.

1.37 Where MJM Technology encounters personal data during the delivery of Services (including during monitoring activities), it will handle that data in accordance with Clause 9 of the T&Cs.

T&Cs Reference — Clause 9 (Data Protection): Full data processing obligations, including the 72-hour breach notification obligation. Clause 15.1 (Confidentiality): Both parties are bound by confidentiality obligations for three years post-termination.

10. Reporting Security Incidents and Suspected Breaches

1.38 The Customer must report any suspected or confirmed security incident to MJM Technology as soon as reasonably practicable, and in any event within 24 hours of becoming aware of it.

1.39 A security incident includes, but is not limited to:

- a suspected phishing attack or successful credential compromise;
- ransomware, malware, or any form of malicious software infection;
- loss or theft of a device connected to, or used to access, managed services;
- any suspected or confirmed unauthorised access to systems or data;
- unusual network behaviour that may indicate a breach or intrusion; or
- discovery of an unauthorised device connected to the network.

1.40 Reports should be made to MJM Technology via the support contact details provided in the Customer's Order or onboarding documentation. Where a P1 (Critical) incident is suspected, the Customer should contact MJM Technology by telephone immediately.

1.41 Where an incident involves personal data, MJM Technology and the Customer each have notification obligations under UK GDPR. MJM Technology will work with the Customer to meet the 72-hour reporting obligation to the ICO where applicable.

T&Cs Reference — Clause 9.2(f): MJM Technology will notify the Customer of any personal data breach within 72 hours of becoming aware. Schedule 3 (Support): P1 response time is 1 hour / 4-hour target resolution. Clause 7.1(a): The Customer must provide timely information to enable MJM Technology to perform its duties.

11. Consequences of Breach

1.42 MJM Technology takes breaches of this AUP seriously. The response to a breach will be proportionate to its severity, taking into account the nature of the activity, the risk it creates, and whether it was deliberate or accidental.

11.1 Escalation Framework

The following framework applies to AUP breaches. MJM Technology retains discretion to apply a higher-level response where the severity of a breach warrants it.

Level	Example Breach	Initial Response	If Unresolved
Minor	Accidental unauthorised device connection; unintentional credential sharing	Written warning to Customer contact	Escalation to Serious
Serious	Deliberate bypass of security controls; repeated minor breaches; sharing VPN access with third parties	Written warning + 5-day remediation period	Partial or full suspension of Services
Critical	Illegal activity; deliberate attack on MJM infrastructure; wilful circumvention causing a security breach	Immediate suspension of all Services	Termination under T&Cs Clause 11.2

11.2 Written Warning Process

1.43 For Minor and Serious breaches, MJM Technology will issue a written warning by email to the Customer's designated contact, which will:

(a) identify the specific breach or suspected breach;

(b) specify the remediation steps required;

(c) state the deadline for remediation (typically 5 Working Days for Serious, 10 Working Days for Minor); and

(d) confirm the consequences of non-remediation.

1.44 The Customer must acknowledge receipt of the warning and confirm its remediation plan within 2 Working Days.

11.3 Suspension

1.45 Where Services are suspended following a breach of this AUP, Fees continue to accrue during the suspension period. Suspension does not constitute termination and does not affect the Customer's payment obligations.

> *T&Cs Reference — Clause 11.4 (Suspension): MJM Technology may suspend Services immediately if the Customer breaches the AUP. Clause 11.2 (Termination for Cause): Persistent or Critical breaches may constitute a material breach entitling MJM Technology to terminate. Clause 7.2: The Customer indemnifies MJM Technology against losses arising from AUP breaches.*

12. Quick Reference Summary

The table below provides a plain-English summary for the Customer's Users. This summary does not replace the full AUP — it is intended as a reference guide only.

Activity	Permitted?
Using managed services for normal business activity	✓ YES
Connecting a personal device to the managed network	✗ NO — must be authorised first
Sharing your MJM-provided VPN or login with a colleague	✗ NO

Activity	Permitted?
Sharing VPN access with an external third party	✗ NO
Disabling or bypassing firewall / security controls	✗ NO
Running a penetration test without MJM approval	✗ NO — written consent required first
Notifying MJM of new equipment added to the network	✓ YES — always required
Reporting a suspected security incident to MJM	✓ YES — within 24 hours
Using managed infrastructure for cryptocurrency mining	✗ NO
Informing staff about this AUP and security training	✓ YES — Customer's responsibility

13. Updates to this Policy

1.46 MJM Technology may update this AUP from time to time to reflect changes in law, regulation, best practice, or the Services offered. The current version will always be available on the MJM Technology website.

1.47 Where a change is material, MJM Technology will give the Customer not less than thirty (30) days' written notice before the change takes effect. Continued use of the Services after that date constitutes acceptance of the updated AUP.

1.48 The version and effective date of this AUP are shown on the cover page. Customers should ensure they are reading the current version.

> *T&Cs Reference — Clause 1.1 (Acceptable Use Policy definition): The AUP is defined as the current published version available on the MJM Technology website.*

14. Contact

If you have any questions about this AUP, wish to report a suspected breach, or need to request an exception or authorisation (e.g. for penetration testing or connecting third-party equipment), please contact MJM Technology:

All Enquiries	*help@mjmsupport.com*
Website	*https://mjmsupport.com*