TERMS AND CONDITIONS FOR IT SUPPORT AND CYBER SECURITY SERVICES

1. Definitions

"Client" means the person, company or organisation purchasing the Services.

"Provider" means Mainstream Digital Ltd

"Services" means IT support, managed services, cyber security services, consultancy, monitoring, remediation, incident response, cloud services, software licensing, hardware procurement and any related services provided by the Provider.

"Agreement" means the Contract between the Provider and the Client comprising these Terms and Conditions together with any Statement of Work, Proposal, Quote or Service Schedule.

"Cyber Incident" means any event affecting the confidentiality, integrity or availability of systems, data, networks or services, including malware, ransomware, phishing, social engineering, denial of service attacks, unauthorised access, insider threats or data breaches.

---

2. Basis of Contract

2.1 These Terms and Conditions apply to all Services supplied by the Provider.

2.2 No Client terms shall apply unless expressly agreed in writing.

2.3 A Contract comes into existence when the Provider accepts an order or commences provision of Services.

---

3. Provision of Services

3.1 The Provider shall exercise reasonable skill and care in delivering the Services.

3.2 The Provider does not warrant that all faults, vulnerabilities or security risks can be identified, prevented or eliminated.

3.3 The Provider may use subcontractors and third-party providers where appropriate.

3.4 Services shall be provided during agreed support hours unless otherwise specified.

---

4. Client Responsibilities

The Client shall:

a) provide accurate information and access to systems;

b) maintain valid software licences;

c) implement recommendations made by the Provider within reasonable timescales;

d) maintain appropriate backups of all data;

e) ensure users comply with security policies;

f) notify the Provider immediately of any suspected Cyber Incident;

g) maintain cyber insurance where appropriate;

h) cooperate fully during incident response investigations.

---

5. Cyber Security Services

5.1 The Provider will use reasonable skill and care in providing cyber security services.

5.2 The Client acknowledges that:

a) no cyber security solution can guarantee protection from all threats;

b) threat actors continually develop new attack methods;

c) vulnerabilities may exist that are unknown to software vendors, security researchers or the Provider;

d) cyber risks can be reduced but never eliminated.

5.3 The Provider does not warrant or guarantee:

a) complete prevention of cyber attacks;

b) uninterrupted security monitoring;

c) detection of all malicious activities;

d) prevention of all ransomware infections;

e) protection against all insider threats;

f) recovery of encrypted, deleted or compromised data.

---

6. Incident Response

6.1 Where incident response services are provided, the Provider shall use reasonable endeavours to investigate, contain and remediate security incidents.

6.2 The Provider shall not be responsible for delays caused by:

a) lack of Client cooperation;

b) incomplete access permissions;

c) actions of third parties;

d) failures of internet, cloud or telecommunications providers;

e) law enforcement requirements.

6.3 Recommendations made during incident response are advisory in nature unless expressly agreed otherwise.

---

7. Backups and Disaster Recovery

7.1 Unless expressly stated within a Service Schedule, the Provider is not responsible for maintaining backups.

7.2 Where backup services are supplied, the Provider will take reasonable steps to ensure backup operation but does not guarantee:

a) successful restoration;

b) completeness of backed-up data;

c) uninterrupted backup functionality.

7.3 The Client shall regularly test restoration procedures.

---

8. Third-Party Products and Services

8.1 The Provider is not responsible for acts, omissions or failures of:

- software vendors;
- cloud providers;
- internet service providers;
- telecommunications providers;
- managed hosting providers;
- hardware manufacturers.

8.2 Third-party warranties shall apply exclusively between the Client and the relevant supplier.

---

9. Charges and Payment

9.1 Fees shall be payable in accordance with the applicable quotation or service agreement.

9.2 Invoices shall be payable within 30 days unless otherwise agreed.

9.3 The Provider may suspend Services for overdue accounts.

---

10. Intellectual Property

10.1 The Provider retains ownership of all methodologies, documentation, scripts, software tools and know-how developed before or during provision of the Services.

10.2 Upon payment in full, the Client receives a non-exclusive licence to use deliverables for internal business purposes.

---

11. Confidentiality

11.1 Each party shall keep confidential all proprietary information disclosed by the other.

11.2 This clause survives termination for five years.

---

12. Data Protection

12.1 Each party shall comply with applicable data protection legislation including UK GDPR and the Data Protection Act 2018.

12.2 Where required, the parties shall enter into a separate Data Processing Agreement.

---

13. Limitation of Liability

13.1 Liability Which Cannot Be Excluded

Nothing in this Agreement shall exclude or restrict liability for:

a) death or personal injury caused by negligence;

b) fraud or fraudulent misrepresentation;

c) any liability which cannot be excluded by law.

13.2 Excluded Losses

To the fullest extent permitted by law, the Provider shall not be liable for:

a) loss of profits;

b) loss of revenue;

c) loss of business opportunity;

d) loss of contracts;

e) loss of goodwill;

f) loss of anticipated savings;

g) loss of reputation;

h) indirect or consequential loss.

13.3 Cyber Attack Exclusion

The Provider shall not be liable for any loss arising directly or indirectly from:

a) cyber attacks by third parties;

b) ransomware incidents;

c) malware infections;

d) phishing attacks;

e) social engineering attacks;

f) business email compromise;

g) denial of service attacks;

h) zero-day vulnerabilities;

i) nation-state attacks;

j) criminal activity by third parties;

except to the extent such losses result directly from the Provider's gross negligence or wilful misconduct.

13.4 Failure to Follow Advice

The Provider shall have no liability for any Cyber Incident where the Client failed to implement recommendations, patches, updates, security controls or remedial actions previously advised by the Provider.

13.5 Security Not Guaranteed

The Client acknowledges:

a) cyber security is a risk management activity and not a guarantee;

b) no system can be made completely secure;

c) successful attacks may occur despite reasonable security measures.

Accordingly, the Provider shall not be liable solely because a Cyber Incident occurs.

13.6 Data Loss

Unless expressly agreed otherwise, the Provider shall not be liable for loss, corruption, encryption or destruction of data beyond the costs reasonably incurred to restore such data from the most recent recoverable backup maintained by or on behalf of the Client.

13.7 Aggregate Financial Cap

Subject to clause 13.1:

The Provider's total aggregate liability arising out of or in connection with the Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, shall not exceed:

the greater of:

a) £100,000; or

b) 125% of the fees paid by the Client during the twelve months immediately preceding the event giving rise to the claim.

13.8 Separate Cyber Liability Cap

The Provider's total liability arising from any Cyber Incident shall not exceed the lower of:

a) £100,000; or

b) the amount recoverable under the Provider's professional Indemnity insurance policy.

---

14. Insurance

14.1 The Provider shall maintain:

- Professional Indemnity Insurance;
- Public Liability Insurance;

at commercially reasonable levels.

14.2 Evidence of insurance may be provided upon reasonable request.

---

15. Suspension of Services

The Provider may suspend Services where:

a) security risks threaten the Provider or other customers;

b) the Client breaches security requirements;

c) fees remain unpaid.

---

16. Termination

Either party may terminate:

a) on material breach not remedied within 30 days;

b) upon insolvency of the other party;

c) in accordance with any agreed notice provisions.

---

17. Force Majeure

Neither party shall be liable for failure to perform due to events beyond reasonable control including:

- cyber warfare;
- widespread internet failures;
- acts of government;
- terrorism;
- natural disasters;
- utility failures.

18. Governing Law

This Agreement shall be governed by the laws of England and Wales.

The courts of England and Wales shall have exclusive jurisdiction.

Additional Cyber Security Schedule

Schedule A - Cyber Security Services Schedule

This Cyber Security Services Schedule forms part of and shall be read in conjunction with the main Terms and Conditions.

Where there is any conflict between this Schedule and the main Terms and Conditions, the provisions of this Schedule shall prevail in relation to Cyber Security Services.

---

1. Purpose of the Services

The Provider shall supply Cyber Security Services designed to assist the Client in reducing cyber risk, improving security posture, detecting threats, responding to incidents, and supporting regulatory and standards compliance.

The Client acknowledges that Cyber Security Services are intended to reduce risk and cannot eliminate the possibility of Cyber Incidents.

---

2. No Guarantee of Security

2.1 The Provider does not guarantee that:

- Cyber Incidents will not occur;
- systems will remain continuously secure;
- all vulnerabilities will be identified;
- all malicious activity will be detected;
- all attacks will be prevented;
- all compromised data can be recovered;
- regulatory compliance will be achieved or maintained.

2.2 The Client acknowledges that information security is an exercise in risk management and not risk elimination.

2.3 Cyber threats evolve continuously and successful attacks may occur despite the implementation of industry good practice controls.

---

3. Client Security Obligations

The Client shall:

3.1 Security Governance

- appoint a responsible management representative for cyber security matters;
- maintain approved security policies where appropriate;
- promptly review and action recommendations issued by the Provider.

3.2 User Management

The Client shall:

- ensure users only have access required for their role;
- remove access for leavers promptly;
- notify the Provider of role changes affecting permissions;
- ensure administrator accounts are restricted to authorised personnel.

3.3 Passwords and Authentication

The Client shall:

- implement strong password policies;
- prohibit password sharing;
- require Multi-Factor Authentication (MFA) where reasonably practicable;
- implement any MFA solution recommended by the Provider unless otherwise agreed in writing.

3.4 Security Awareness

The Client shall ensure employees receive appropriate cyber security awareness training and shall take reasonable steps to minimise phishing, social engineering and credential compromise risks.

3.5 Vulnerability Remediation

The Client shall implement security recommendations within reasonable timeframes, including:

Severity	Recommended Timescale
Critical	14 days
High	30 days
Medium	90 days
Low	Risk-based approach

Failure to implement recommendations may invalidate service-related liability protections.

---

4. Supported Systems Requirement

4.1 The Provider's services are based upon the use of vendor-supported products.

4.2 Unless otherwise agreed in writing, the Provider shall have no responsibility for security shortcomings resulting from:

- unsupported operating systems;
- end-of-life software;
- unsupported hardware;
- obsolete firmware;
- unpatched software products.

4.3 The Provider may recommend replacement, upgrading or retirement of unsupported technology.

---

5. Security Monitoring Services

Where monitoring services are provided:

5.1 Monitoring systems are intended to assist in identifying suspicious or malicious activity but are not guaranteed to detect all threats.

5.2 The Provider shall not be liable for:

- attacks that evade monitoring tools;
- attacks occurring outside monitored environments;
- encrypted malicious communications that cannot reasonably be inspected;

- limitations imposed by software vendors or technology providers.

5.3 Security monitoring shall not be considered a substitute for sound security governance.

---

6. Managed Endpoint Protection

Where endpoint security services are provided:

6.1 The Client shall not disable, remove or interfere with security software.

6.2 The Provider may reinstall or reconfigure security software where required.

6.3 The Provider is not responsible for any compromise arising after:

- deliberate removal of security controls;
- unauthorised system modifications;
- use of prohibited software;
- installation of software without appropriate approval.

---

7. Vulnerability Assessments and Security Reviews

7.1 Security reviews and vulnerability assessments represent the Provider's findings as at the date undertaken.

7.2 The Provider does not warrant that:

- all vulnerabilities have been identified;
- future vulnerabilities will not arise;
- exploitation is impossible after remediation.

7.3 New vulnerabilities may emerge immediately after completion of an assessment.

---

8. Penetration Testing Services

Where penetration testing is provided:

8.1 Testing is performed on a sample basis and cannot identify every weakness.

8.2 The Provider shall not be responsible for vulnerabilities not discovered during testing.

8.3 The Client acknowledges that residual risk remains following remediation activities.

---

9. Cloud Services

The Client acknowledges that cloud security is a shared responsibility.

The Provider shall not be responsible for:

- cloud provider outages;
- security failings of cloud providers;
- changes to cloud provider services;
- cloud provider administrative actions;
- vulnerabilities within cloud provider platforms.

This clause applies whether the provider is acting as reseller, advisor, administrator or integrator.

---

10. Cyber Incident Reporting

10.1 The Client shall notify the Provider immediately upon becoming aware of:

- ransomware activity;
- credential compromise;
- phishing campaigns;
- suspicious network activity;
- data breaches;
- loss or theft of devices;
- security incidents involving suppliers.

10.2 Delays in reporting may reduce the effectiveness of incident response services.

---

11. Incident Response Limitations

11.1 Incident response services are provided on a reasonable endeavours basis.

11.2 The Provider cannot guarantee:

- complete containment;
- full eradication of malicious software;

- recovery of all systems;
- recovery of all data;
- restoration within any specific timeframe.

11.3 Business recovery may be affected by factors beyond the Provider's control including:

- existing system condition;
- quality of backups;
- client preparedness;
- third-party services;
- availability of infrastructure.

---

12. Backups and Recovery

12.1 Unless expressly stated otherwise, responsibility for determining backup requirements remains with the Client.

12.2 The Client shall verify that backup retention periods are suitable for operational, legal and regulatory requirements.

12.3 Backup services do not guarantee recovery of:

- all files;
- all versions of data;
- encrypted data;
- corrupted data.

12.4 Restoration testing should be conducted regularly and at least annually.

---

13. Cyber Insurance

13.1 The Provider strongly recommends that the Client maintains its own cyber insurance policy.

13.2 Such insurance should include appropriate cover for:

- ransomware;
- business interruption;

- legal expenses;
- regulatory investigation;
- data breach costs;
- incident response costs;
- cyber extortion;
- reputational harm.

13.3 The Client acknowledges that losses resulting from a Cyber Incident may exceed the Provider's contractual liability limits.

---

14. Exclusions from Liability

Without prejudice to the general limitation of liability provisions contained within the Agreement, the Provider shall not be liable for any Cyber Incident arising wholly or partly from:

14.1 Failure to Implement Advice

Failure by the Client to implement recommendations, including:

- MFA deployment;
- security patching;
- vulnerability remediation;
- network segmentation;
- privileged access controls;
- security awareness training.

14.2 Insecure Client Practices

- shared user accounts;
- shared administrator credentials;
- weak passwords;
- unauthorised remote access;
- unmanaged devices;
- unauthorised software installations.

14.3 Third-Party Failures

- cloud providers;
- software vendors;
- telecommunications providers;
- internet service providers;
- data centre providers;
- outsourced service providers.

14.4 Criminal Acts

- ransomware attacks;
- business email compromise;
- social engineering;
- phishing;
- credential theft;
- insider fraud;
- cyber extortion;
- acts of cyber terrorism;
- nation-state attacks.

14.5 Unsupported Technology

Use of:

- unsupported operating systems;
- end-of-life software;
- end-of-life hardware;
- devices no longer receiving security updates.

---

15. Cyber-Specific Liability Cap

Notwithstanding any other provision of the Agreement:

15.1 The Provider's total aggregate liability arising from any Cyber Incident shall not exceed the lower of:

- £100,000; or

- 125% of the fees paid by the Client during the previous twelve months.

15.2 Alternatively, where the Provider maintains Cyber Liability Insurance, liability may be limited to:

The amount actually recoverable by the Provider under its applicable Cyber Liability Insurance policy in respect of the relevant claim.

15.3 In no event shall the Provider be liable for:

- ransom payments;
- regulatory fines;
- loss of future business;
- reputational damage;
- diminished corporate value;
- loss of profit;
- loss of revenue;
- loss of anticipated savings;
- consequential or indirect loss.

---

16. Acceptance of Residual Risk

The Client acknowledges and accepts that:

1. Cyber security measures substantially reduce but cannot eliminate cyber risk.
2. Some threats cannot reasonably be predicted or prevented.
3. Business disruption may occur despite implementation of industry-standard security controls.
4. The occurrence of a Cyber Incident shall not, of itself, constitute evidence of negligence by the Provider.
5. The Client retains ultimate responsibility for business risk, information assets, regulatory obligations and cyber insurance arrangements.

The Client acknowledges that certification against Cyber Essentials, Cyber Essentials Plus, ISO 27001, NIST CSF or any other security framework does not guarantee immunity from cyber attack or data breach. Such standards and certifications are

designed to reduce risk and improve security posture but do not prevent all forms of cyber compromise.