Schedule 3 - Cyber Security, Backup and Continuity Terms

Version: Standard Website Terms

1. Application and Scope

1.1 This Schedule applies where the Order Form includes cyber monitoring, managed detection and response, EDR, SIEM, vulnerability scanning, web application scanning, infrastructure scanning, external attack surface management, exposure management, autonomous penetration testing, breach and attack simulation, security validation, security awareness training, Cyber Essentials support, Cyber Essentials certification services, incident response, managed backup, SaaS protection, business continuity, disaster recovery, dark web monitoring, penetration testing or similar security or resilience services.

1.2 Unless otherwise stated in the Order Form, Cyber Essentials, Cyber Essentials Plus and similar certification, accreditation or assessment services procured or administered by the Company shall be supplied on a twelve-month minimum commitment basis and may be invoiced annually in advance or monthly in advance by instalments at the Company's election. Any monthly payment arrangement for such services is a billing accommodation only and shall not create a monthly cancellable service.

2. Shared Responsibility and No Guarantee

2.1 The Customer acknowledges that cyber security and resilience are shared responsibilities and that the Services reduce risk but cannot eliminate cyber threats, user error, misconfiguration, insider risk, phishing, fraud, ransomware, zero-day vulnerabilities, third-party compromise or service interruption.

2.2 The Company does not warrant or represent that the Services will prevent, detect, block, respond to or remediate every security incident, vulnerability, backup failure, recovery issue, continuity event or compliance failure.

3. Customer Responsibilities

3.1 The Customer shall: (a) maintain accurate asset inventories and user lists; (b) ensure all relevant systems are onboarded to the agreed security tooling; (c) keep supported operating systems and applications within vendor support where reasonably practicable; (d) maintain suitable password, MFA, access and administrative control policies; (e) promptly implement reasonable remediation actions notified by the Company; and (f) maintain internal incident escalation contacts and decision-makers.

3.2 The Company shall not be liable for any loss or compromise arising from assets, users, locations, workloads or applications which were not disclosed, not onboarded, not licensed, not reachable by the tooling, or excluded from scope.

3.3 If the Customer refuses, delays or materially obstructs implementation of baseline security recommendations, onboarding steps, asset coverage, logging requirements, backup scope or remediation actions, the Company may suspend or limit the affected Services, exclude affected assets from monitoring, terminate the affected Services for cause and continue to charge in accordance with the Agreement.

4. Monitoring, Alerts and Response Authority

4.1 The Company may investigate alerts, assess suspicious activity and, where expressly included in the Service, take containment or response actions including disabling accounts, isolating devices, revoking tokens, blocking domains, quarantining emails, terminating sessions or applying policy controls.

4.2 Unless expressly stated otherwise, the Customer grants the Company advance authority to take reasonable urgent containment steps where the Company believes delay would materially increase risk to the Customer or the Company.

4.3 The Company's monitoring obligations extend only to the agreed tools, logs, data sources and integrations. Lack of telemetry, ingestion failure, licence exhaustion, API restrictions or third-party platform limitations may affect visibility and response capability.

5. Backup, Restore and Continuity

5.1 Backup services, where provided, are subject to the scope, retention periods, storage targets, protected workloads, restoration methods, bandwidth, vendor platform limitations and recovery priorities stated in the Order Form or Service Description.

5.2 Successful completion of a backup job, health check or dashboard status does not guarantee the completeness, integrity or recoverability of the underlying data.

5.3 The Customer remains responsible for verifying that the selected retention periods, backup scope, protected repositories, archive policies, legal hold requirements and restore objectives are appropriate for its business and regulatory needs.

5.4 Unless expressly included as a managed restore testing service, the Customer remains responsible for regular restore testing and business continuity rehearsals.

5.5 Recovery time objectives and recovery point objectives are planning assumptions and target objectives unless expressly stated in the Order Form as contractual commitments.

6. Penetration Testing, Vulnerability and Compliance Services

6.1 Penetration testing, vulnerability scanning, security assessments, phishing simulations, compliance gap analyses and certification support services are point-in-time exercises based on the then-known scope, access, tooling and environment.

6.2 Such services do not guarantee that all vulnerabilities, weaknesses, control failures or compliance issues will be identified.

6.3 The Customer warrants that it has obtained and will maintain all consents, permissions, lawful authority, hosting provider approvals, cloud provider approvals, SaaS provider approvals, third-party platform approvals, internal approvals and end-user notices required for the Company and its Third Party Providers to perform security testing, simulation, scanning, probing, crawling, exploitation validation, credentialed testing, unauthenticated testing, phishing simulation or other assessment activity against the relevant systems, users, domains, applications, IP addresses, APIs, cloud tenants, wireless networks or premises.

6.4 Certification or accreditation outcomes, including Cyber Essentials, Cyber Essentials Plus and similar schemes, are determined by the relevant assessor, certifying body or framework owner and are not guaranteed by the Company.

6.5 Where the Services include Cyber Essentials, Cyber Essentials Plus or any similar certification, accreditation, assessment or compliance service, the Customer acknowledges that the Company may incur third-party assessment, certification, platform, reviewer, scheme, portal or registration fees on an upfront, annual or otherwise committed basis. Such Services may be supplied on an annual commitment basis even where the Company permits payment by monthly instalments for convenience.

6.6 Unless otherwise expressly stated in the Order Form, Charges for certification, accreditation, assessment or compliance services shall commence on the earlier of: (a) the date the relevant Order becomes binding; (b) the date the Company places the order, registers the Customer, books the assessment or otherwise incurs the relevant third-party cost or commitment; and (c) the date the Company opens, activates, issues or procures the relevant assessment, certification, portal or scheme access for the Customer.

6.7 Any delay, omission, lack of readiness, failure to provide information, failure to complete remediation actions, failure to approve submissions, failure to provide evidence, or other non-co-operation by the Customer shall not delay the commencement of Charges, suspend or extend the Minimum Term, entitle the Customer to any refund or credit, or relieve the Customer from paying any committed Charges.

6.8 To the extent the Company has incurred third-party costs or entered into third-party commitments for any certification, accreditation, assessment or compliance service, those costs and commitments shall be non-cancellable and non-refundable and shall remain payable by the Customer in full, whether or not the Customer proceeds, qualifies, passes, completes remediation, submits the required evidence, or achieves certification or accreditation.

6.9 Any rework, resubmission, reassessment, remediation support, consultancy, engineering time, project work, further review or additional evidence handling required because the Customer was not ready, failed the assessment, allowed the assessment window to lapse, changed scope, introduced new systems, withheld relevant information, or did not implement required controls shall be chargeable in addition at the Company's then-current rates.

6.10 The Company may perform or arrange security testing, managed detection, SOC, backup monitoring, awareness training, vulnerability management, certification support or incident response services through specialist subcontractors or platform vendors. The Customer agrees that applicable third-party scope limitations, tooling limitations and vendor terms may apply to such services.

6.11 Where penetration testing, vulnerability assessment or similar assurance services are supplied on a recurring, scheduled or monthly basis, each test cycle shall constitute a periodic assessment of the agreed in-scope targets only and shall not amount to continuous monitoring, continuous assurance or a guarantee of ongoing security between test cycles.

6.12 The Customer shall ensure that all IP addresses, domains, applications, APIs, cloud tenants, wireless networks, user accounts and other assets submitted for testing are lawfully owned or controlled by the Customer or are otherwise subject to valid written authority permitting such testing. The Customer shall indemnify the Company against any claim arising from testing requested without proper authority.

6.13 The Customer acknowledges that authorised security testing may cause alerts, rate limiting, account lockouts, service degradation, defensive blocking, provider intervention or other unintended operational effects. To the fullest extent permitted by law, the Company shall not be liable for such effects where the testing was conducted within the agreed scope and methodology.

6.14 Unless expressly stated in the Order Form, remediation, reconfiguration, code fixes, patching, hardening, retesting, report workshops, developer liaison and validation of remedial actions are outside scope and chargeable separately.

6.15 Where recurring testing is delivered through a third-party platform or specialist provider, the Company may modify the testing methodology, frequency, format or delivery model to reflect changes in vendor capability, service design or platform availability, provided the overall nature of the Services is not materially and adversely reduced.

6.16 Where any vulnerability scanning, penetration testing, attack simulation, exposure management, external attack surface management, breach and attack simulation, automated exploitation, validation or similar security service is delivered through a Third Party Provider or specialist platform, the Customer agrees that use of that service is subject to the relevant Third Party Provider terms, acceptable use rules, scanning restrictions, scope limitations, prohibited target rules, technical constraints, suspension rights and vendor disclaimers.

6.17 The Customer shall not, and shall ensure that its users do not, use any security testing platform, report, output, telemetry, log, methodology, exploit path, command response, test result or documentation to benchmark competing products, develop competing services, reverse engineer any platform, train or fine-tune any artificial intelligence or machine-learning model, or otherwise use vendor outputs for purposes prohibited by the applicable Third Party Provider terms.

6.18 The Customer shall ensure that all assets submitted for testing are owned or controlled by the Customer or are subject to valid written authority permitting the relevant testing. Where any asset is hosted, operated, managed or protected by a third

party, the Customer shall obtain any required prior written approval from that third party before the test is scheduled or commenced. The Customer shall indemnify the Company against any claim, demand, cost, loss, liability, penalty or expense arising from testing requested without proper authority or in breach of any third-party terms.

6.19 Before any scan, test, simulation or assessment, the Customer is strongly recommended to ensure that all relevant systems and data are backed up, that appropriate rollback and recovery arrangements are in place, that suitable maintenance windows or business-impact windows have been considered, that emergency contacts are available, and that affected internal teams and third-party providers have been notified where appropriate. Any reminder, checklist or recommendation issued by the Company is for risk reduction only and shall not transfer operational readiness, backup or recovery responsibility from the Customer to the Company.

6.20 The Customer acknowledges that security testing may use techniques similar to those used by attackers and may cause or contribute to service alerts, log volume increases, rate limiting, account lockouts, defensive blocking, email filtering, web application firewall reactions, endpoint protection reactions, service degradation, malfunction, temporary loss of availability, hardware stress, data access events, false positives, false negatives, provider intervention or other operational effects. To the fullest extent permitted by law, the Company shall not be liable for such effects where the testing was conducted within the agreed or instructed scope or was otherwise caused by Customer instructions, Customer systems, third-party platforms or the inherent nature of the testing.

6.21 The Customer acknowledges that security testing, vulnerability scanning, exposure management, penetration testing and related assurance activity may form part of the Customer's own security, compliance and risk-management obligations, including obligations relating to the security of processing. The Customer remains responsible for determining whether the scope, frequency, timing, lawful basis, notices, records, risk assessment and data protection impact assessment position for such activity is appropriate for its own business, systems, data subjects and regulatory obligations.

6.22 The Customer shall not bring, and shall ensure that its Affiliates, users, clients and end customers do not bring, any claim directly against any Third Party Provider in respect of security testing, scanning, assessment, certification, monitoring, backup, incident response or other cyber services supplied by or through the Company. The Customer shall indemnify the Company against any claim, demand, cost, loss, liability or expense arising where the Customer, its Affiliates, users, clients or end customers bring or threaten any direct claim against such Third Party Provider.

6.23 Where any certification, accreditation, assessment, questionnaire, portal submission, audit, evidence submission or technical verification is subject to a deadline imposed by the Company, a Third Party Provider, a certification body, an assessor, a scheme owner or the relevant portal, the Customer shall complete all required actions before that deadline. Failure to do so shall be a Customer Default. Any reminders issued by the Company are a courtesy only, and failure by the Company to issue reminders shall not affect the Customer's responsibility to complete the assessment, submission or audit on time.

6.24 Unless otherwise stated in the Order Form or notified by the relevant certification body, the Customer acknowledges that Cyber Essentials self-assessment access may expire if not completed within six months of purchase, registration or portal issue, and Cyber Essentials Plus assessment or verification may need to be completed within ninety days of the relevant Cyber Essentials certification date or within such other deadline notified by the Company, certification body, scheme owner or Third Party Provider. If the relevant assessment window expires, lapses or is withdrawn, the Customer shall remain liable for all Charges and any new assessment, reassessment, resubmission, re-registration, consultancy, technical testing, audit or remediation work shall be chargeable in addition.

7. Dark Web Monitoring and Threat Intelligence

7.1 Dark web monitoring, threat intelligence and compromise intelligence services are informational services only.

7.2 The Company does not warrant that all leaked credentials, exposed data, impersonation domains, typosquatting, mentions, disclosures or criminal activity relating to the Customer will be identified, verified, removed or remediated.

7.3 The Company shall not be obliged to conduct takedown action, law enforcement reporting, litigation support or attribution work unless separately agreed in writing.

8. Incident Response Limitations

8.1 Unless expressly included, incident response does not include onsite attendance, forensic imaging, malware reverse engineering, legal reporting, regulator engagement, media handling, evidential chain of custody or third-party litigation support.

8.2 The Customer shall remain responsible for business decisions, ransom decisions, legal notifications, insurer engagement and regulator reporting, although the Company may assist on a chargeable basis where requested.