Intouch Tech Limited
Schedule 3 - Cyber Security, Backup and Continuity Terms

Effective date: 1 April 2026

This schedule forms part of the Intouch Tech Master Terms and Conditions.

1. Application and Scope

1.1 This Schedule applies where the Order Form includes cyber monitoring, managed detection and response, EDR, SIEM, vulnerability scanning, 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 all consents and authority necessary for the Company to perform security testing, simulation or scanning against the relevant systems, users, domains, applications 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.

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.