PXP Integration

Terms and Conditions

PXP Integration

Terms and Conditions

1. Application and Acceptance

1.1 These Integration Terms and Conditions (the "**Integration Terms**") apply to each Integration by which a Company accesses, connects to, interfaces with or enables interoperability with the Platform, the PXP Materials, the PXP APIs, the PXP SDKs, PXP back-office systems, PXP payment systems, or any other PXP systems, services or infrastructure.

1.2 These Integration Terms apply in addition to the Company Agreement and are incorporated into the Company Agreement by reference where: (a) the Company Agreement states that these Integration Terms apply; (b) PXP makes Integration Materials available to the Company; (c) the Company accesses or uses the Platform or the Integration Materials; (d) the Company commences development, testing, or operation of an Integration; or (e) PXP otherwise notifies the Company that these Integration Terms apply.

1.3 By accessing or using any Platform, Integration Materials, or Credentials, or by commencing or operating an Integration, the Company accepts and agrees to comply with these Integration Terms.

1.4 PXP may require a separate signed integration addendum, order form, statement of work, project plan, attestation or other document for bespoke, high-risk, POS, regulated, payment-flow, security-sensitive, or otherwise material integrations. Where such document is signed or expressly agreed by the Parties, it shall apply in addition to these Integration Terms and shall prevail to the extent of any conflict in relation to the relevant Integration.

1.5 Nothing in these Integration Terms obliges PXP to provide any payment services, acquiring services, aggregation services, regulated services, settlement services, support services, professional services, custom development or other services, unless such services are expressly agreed in the Company Agreement. The Integration is an enabling technical and operational arrangement only and does not by itself create any right to use any PXP Service, payment method, acquirer, payment provider or other Third-Party Dependency.

1.6 PXP may change these Integration Terms from time to time by publishing an updated version on its website or otherwise making an updated version available to the Company. Any changes shall take effect on the date stated in the updated version or as otherwise notified by PXP. Continued access to or use of the Platform, the Integration Materials, or the Integration after the effective date of an update constitutes acceptance of the updated Integration Terms.

2. Definitions and Interpretations

2.1 In these Integration Terms: (a) references to a statue, regulation, rule, or standard include that statute, regulation, rule, or standard as amended, replaced, or re-enacted from time to time; (b) words in the singular include the plural and vice versa; (c) headings are for convenience only and do not affect interpretation; and (d) references to "including" or "includes" are to be construed without limitation.

2.2 In these Integration Terms, the following terms have the meanings set out below:

AI Technology	means any and all machine learning, deep learning, and other artificial intelligence technologies, including statistical learning algorithms, models (including large language models), neural networks, and other artificial intelligence tools or methodologies, all software implementations of any of the foregoing, and related hardware or equipment capable of generating various types of content (including text, images, video, audio, or computer code) based on user-supplied prompts
Applicable AML Regulations	means all Applicable Laws prohibiting money laundering, including attempting to conceal or disguise the identity of illegally obtained proceeds
Applicable Laws	means all laws, statutes, regulations, regulatory rules, regulatory guidance, directions, orders, licences, permits, Card Scheme Rules, and other requirements of any governmental, regulatory supervisory, or competent authority which apply to a Party, the Integration, the Platform, the Company Services, or the PXP Services, in each case as amended or replaced from time to time and to the extent applicable to the relevant Party and its obligations under the Company Agreement and these Integration Terms
Business Day	means a day other than a Saturday, Sunday, or public holiday in England on which banks are generally open for business in London
Card Scheme	means Visa International, MasterCard International, Discover or such other card scheme as notified to the Company by PXP

Card Scheme Rules	mean all applicable bylaws, rules, regulations, operating guidelines and procedures issued by any Card Scheme from time to time and any current waivers or exceptions agreed with the Card Schemes
Company	means a counterparty of PXP, which includes, but not limited to, merchant, partner, platform, service provider, technical integrator, reseller, customer, or other counterparty that access, connects to, interfaces with or integrates with the Platform, or PXP Materials, or that is party to the Company Agreement with PXP. References to "*you*", or "*your*" shall be construed accordingly.
Company Agreement	means the written agreement entered into between the Company and PXP to which this Integration Terms apply, including any order form, schedule, statement of work, addendum, service terms, policies and other documents incorporated by reference
Company Materials	means all systems, platforms, applications, software, hardware, devices, website, mobile applications, documentation, data content, materials, processes, know-how and Intellectual Property Rights owned or licensed by the Company, excluding the Platform and PXP Materials
Company Services	means the Company's services stipulated in the Company Agreement
Company Systems	means the Company systems, platforms, applications, software, hardware, devices, websites, mobile applications, networks, infrastructure, databases, environments, and other technology used by or on behalf of the Company in connection with the Integration
Credentials	means any API key, token, password, certificate, private key, username, secrete, access code authentication credential or other security credential issued or made available by PXP or the Company in connection with the Integration

Data Protection Impact Assessment	has the meaning given to it in the Data Protection Laws
Data Protection Laws	means the UK Data Protection Act 2018, the GDPR and any other relevant data protection laws
Data Subject	has the meaning given to it in the Data Protection Laws
Data Subject Rights	has the meaning given to it in the Data Protection Laws
Go-Live	means the point at which the Integration is enabled for use in a production environment, whether for a pilot, limited release, phased roll-out or full production launch
Integration	means the technical, operational, security, and/or configuration process by which (i) the Company connects, interfaces, or enables interoperability between any Company Systems, platforms, applications, software, hardware, devices, websites, mobile applications, APIs, SDKs, plugins, hosted payment pages, data feeds, file transfers, or other technology and the Platform, PXP API, PXP Platform, PXP back-office system or any other PXP systems, or services in accordance with the Integration Manuals; and/or (ii) PXP connects, interfaces, or enables interoperability between its systems, platforms, or services and the Company systems, platforms, or services, in each case to enable the exchange of data, the facilitation of transactions, or the provision of services as contemplated by the Company Agreement. Integration is technology agnostic and may include API connections, SDKs, webhooks, hosted pages, software plugins, point-of-sale integrations, file-based exchanges, data exchanges, or other interoperability methods agreed or made available by PXP from time to time.
Integration Data	means any data, information, instructions, requests, responses, messages, files, logs, credentials, metadata, Transaction, Data Personal Data, Merchant Information, Protected Information, or other content transmitted, received, generated, accessed, stored, or otherwise processed through or in connection with the Integration

Integration Defect	means any error, defect, bug, misconfiguration, malformed request, incorrect message handling, failed webhook handling, transaction state management failure, duplicate submission, incorrect routing, reconciliation discrepancy, settlement or refund request error, performance degradation, security weakness, or other issues in or caused by the Company Systems, Company Materials, Third-Party Dependencies, or the Company's implementation, configuration, operation, or maintenance of the Integration
Integration Manuals	means the integration manuals, developer documentation, product guidelines, technical specifications, API specifications, SDK documentation, installation instructions, operating instructions, release notes, online help, security requirements, implementation guidance, certification requirements, and other similar documents or materials describing the capabilities of, or instructions for, the Integration, Platform, or integration Materials that PXP makes available to the Company from time to time
Integration Materials	Means the Platform, PXP APIs, SDKs, software, code, libraries, sample code, webhooks, hostage pages, portals, documentation, Integration Manuals, developer tools, test environments, sandbox environments, Credentials and other materials made available by PXP in connection with the Integration
Material Integration Incident	means any Integration Defect, Security Incident, outage, data discrepancy, incorrect transaction state, duplicate transaction, duplicate capture, duplicate refund, duplicate settlement request, reconciliation issue, webhook failure, excessive traffic, rate-limit breach, unauthorised access, material customer impact, material Merchant impact, regulatory issue, or other incident which has, or may reasonably be expected to have, a material legal, regulatory, security, operational, financial, reputational, or customer impact on PXP, the Platform, the PXP Services, Merchants, and or other related third parties.

Merchant	means such person that has contracted with PXP for the provisioning of payments and/or other services as agreed between PXP and such Merchant
Merchant Information	means (where applicable) any such information that the Company has lawfully obtained and/or shared with PXP
Personal Data	has the meaning given to it in the Data Protection Laws
Platform	means the online, web-based, mobile, application-based, API, SDK, back-office, infrastructure, payment data, reporting, administration, and other technology platforms, systems, and tools, made available or operated by PXP from time to time, including PXP APIs, the PXP back-office system, and other PXP integration tools
POS	means a point-of-sale physical or virtual (where available) device for accepting card payments at physical locations of Merchants
Processing	has the meaning given to it in the Data Protection Laws
Protected Information	means any one or more of the following categories of information or data: (i) Merchant's information; (ii) any information or data covered by applicable law, including applicable privacy laws, (iii) all information about PXP information security and its applied information security measures; and (iv) any information specifically designated as Protected Information.
PXP	means PXP Financial Limited (company number 05433326), having its registered office address at the Corn Mill, Roydon Road, Stanstead Abbotts, Hertfordshire, SG12 8XL, UK
PXP Materials	means all systems, platforms, applications, software, hardware, devices, websites, mobile applications, documentation, data, content, materials, processes, know-how and Intellectual Property Rights owned or licensed by the Company, excluding the Platform and PXP Materials

PXP Services	means the services provided by PXP to Merchants
Routine Update	means a standard maintenance release, bug fix, patch, dependency update, minor enhancement, or similar change to the Company Systems or the Integration which does not materially affect the architecture, security controls, payment flows, transaction state management, data flows, permissions, endpoints, Payment Components, PCI scope, certification status, performance, availability, customer experience, or any previous PXP approval or attestation
Security Incident	means any actual, suspected, or threatened unauthorized access to, use of, disclosure of, alteration of, loss of, compromise of, or interference with the Platform, Integration, Integration Data, Protected Information, Credentials, Company Systems or any systems connected to the Integration, including any malware infection, vulnerability exploitation, denial of service attack, data breach, personal data breach, credential compromise, system outage, or material security weakness.
Supported Version	means a version of an API, SDK, endpoint, Platform component, Integration Material, POS Application, operating system, firmware, device model, software component, or other technology which PXP has not deprecated, suspended, withdrawn, or identified as unsupported of the relevant Integration
Third-Party Dependency	means any third-party system, service, platform, software, hardware, device, network, cloud service, payment method, acquirer, payment provider, processor, card scheme, wallet provider, open banking provider, telecommunications provider, hosting provider or other third-party technology or service used by or on behalf of either Party or any Merchant in connection with the Integration.
Transaction Data	means data relating to a payment, refund, authorisation, capture, settlement, payout, chargeback, dispute,

transaction status, transaction event, or other payment-related event processed or transmitted through the Integration

3. General Integration Obligations

3.1 The Company shall perform and maintain the Integration at its own cost and expense, in accordance with these Integration Terms, the Company Agreement, the Integration Details, the Integration Manuals, and any written instructions issued by PXP from time to time.

3.2 PXP is not responsible for providing, securing, maintaining or supporting the Company Systems, Company devices or any Third-Party Dependencies used by or on behalf of the Company. The Company shall use only systems, environments and devices that have been properly tested, remediated for known weaknesses, security configured, patched and hardened in accordance with the good industry practices.

3.3 PXP shall manage access to the Platform and the PXP Materials. The Company shall manage and remain responsible for access to the Company Systems and for the acts and omissions of all users, employees, contractors, agents, Merchants, customers, and third parties that access the Integration through, or on behalf of, the Company.

3.4 The Company shall not allow any Affiliate, Merchant, customer, subcontractor, or other third party to access or use the Platform, the Integration Materials, or Integration except as expressly permitted under the Company Agreement or approved by PXP in writing. The Company remains fully responsible for all acts and omissions of such persons as if they were the acts and omissions of the Company.

3.5 The Company shall not allow any Affiliate, Merchant, customer, subcontractor, or other third party to access or use the Platform, Integration Materials, or Integration except as expressly permitted under the Company Agreement or approved by PXP in writing. The Company remains fully responsible for all acts and omissions of such persons as if they were the acts and omissions of the Company.

3.6 Where the Company acts as a partner, reseller, platform operator, technical service provider pr other intermediary, the Company shall ensure that its agreements with Merchants, customers and other relevant third parties include terms sufficient to allow the Company to comply with these Integration Terms and to protect PXP, the Platform, PXP Materials and Protected Information to at least the same standard as these Integration Terms.

3.7 The Company shall not make any representation, warranty or commitment on behalf of PXP, or describe the Integration, Platform or PXP Services in any manner

inconsistent with the Company Agreement, the Integration Manuals or any written instruction issued by PXP.

4. Purpose and Scope of the Integration

4.1 The purpose of the Integration is to enable the Company to interact with the Platform for the purposes expressly agreed or enabled by PXP in connection with the Company Agreement.

4.2 The Integration is limited to the Integration Details and to the scope, environments, interfaces, payment methods, devices, transaction types, data flows, territories and use cases expressly enabled or approved by PXP. Any functionality, interface, product, service, payment method, territory, channel, device, data flow, or use case not expressly included is excluded from the scope of the Integration.

4.3 The Company shall not use the Integration for any purpose other than the purpose expressly agreed under the Company Agreement, Integration Details, and these Integration Terms.

4.4 Any change to the Integration scope must be agreed or approved by PXP in writing or through a PXP-approved configuration, onboarding, or change process.

5. Integration Requirements

5.1 The Company shall comply with the Integration Manuals and any other documents, technical controls, security controls or written instructions provided or made available by PXP from time to time.

5.2 The Company shall not move the Integration into production, enable live traffic or commence Go-Live without completing all testing, certification, due diligence and approval steps required by PXP and receiving PXP's written approval for Go-Live. PXP may withhold, condition, suspend or withdraw approval where it reasonably considers that the Integration, Company Systems or relevant Third-Party Dependencies may create legal, regulatory, operational, security, financial crime, Card Scheme, data protection, reputational or technical risk.

5.3 The Company shall use sandbox, test and production environments only for their intended purposes. The Company shall not use live Personal Data, live card data, or live transaction data in any sandbox or test environment unless expressly authorised by PXP in writing and permitted by Applicable Laws, Card Scheme Rules and applicable PCI standards.

5.4 The Company shall comply with any API usage limits, rate limits, authentication requirements, security controls, data formatting requirements, message specifications, release procedures, deprecation notice and other technical controls notified or made available by PXP from time to time.

5.5 The Company shall not conclude penetration testing, vulnerability scanning, load testing, stress testing, scraping, automated testing at scale or any similar activity against the Platform or PXP Materials without PXP's prior written approval and compliance with any conditions specified by PXP.

5.6 PXP may modify, upgrade, replace, suspend, deprecate, or discontinue any Integration Material, interface, API, SDK, endpoint, field, version, environment, or other component of the Platform from time to time. PXP shall use reasonable endeavours to provide prior notice of material planned changes where practicable, but may implement urgent changes without prior notice where required for security, legal, regulatory, operational or risk reasons.

6. Timeline

6.1 Where Integration timelines or milestones are agreed, the Company shall allocate sufficient resources, personnel and time to meet the timeline requirements and promptly address any issues affecting completion.

6.2 The Company shall appoint and maintain named technical, operational and project contracts for the Integration and shall ensure that such contacts have sufficient authority, availability and technical knowledge to progress the Integration, respond to PXP requests and make or procure decisions required for delivery and ongoing support.

6.3 The Company shall respond to requests, queries, defect reports, security findings, testing issues and approval conditions from PXP within any agreed response times or, if no response time is agreed, within a commercially reasonable period having regard to the urgency and risk of the matter. For material security, production or customer-impacting matters, the Company shall treat PXP requests as urgent and shall provide prompt updates until resolved.

6.4 If the Company repeatedly misses milestones, fails to allocate sufficient resources, fails to respond to PXP within a reasonable period, or otherwise causes material delay to the Integration, PXP may require an escalation meeting, revised project plan, remediation plan and/or revised milestones. Where the Company does not comply with such requirement within a reasonable period specified by PXP in writing, PXP may pause, deprioritise, reschedule, or close the Integration project without liability to the Company.

6.5 Unless agreed otherwise in the Company Agreement or an applicable statement of work, PXP shall not be liable for any delay, cost, loss, or missed launch date arising from the Company' failure to provide timely resources, information, access, approvals, testing, remediation, or other assistance necessary for the Integration.

6.6 The Company shall be liable for any remedies, service credits, liquidated damages, cancellation fees, project reactivation fees, or other commercial consequences for material delay only where such remedies are expressly agreed in the Company Agreement, Integration Details, or an applicable statement of work. Where such remedies are not expressly agreed, PXP's remedies for delay caused by the Company include suspension, deprioritisation, project closure, charging additional professional services fees and/ or incurred costs, termination or suspension.

7. Responsibilities

7.1 Company is solely responsible, at its own cost and expense, for designing, developing, implementing, configuring, testing, operating, monitoring, supporting and maintaining the Company Systems, the Company Materials, any Third-Party Dependencies and all parts of the Integration implemented, operated, or controlled by or on behalf of the Company.

7.2 The Company shall conduct testing and quality checks on the Integration in sandbox, test and production environments as necessary to ensure functionality, security, compatibility and proper operation with the Platform.

7.3 The Company shall maintain its Integration with the Platform, including applying updates, patches, fixes, migrations and remediation steps issued or reasonably required by PXP from time to time.

7.4 The Company shall monitor the Integration's performance and conduct regular maintenance on the Company Systems and any relevant Third-Party Dependencies as necessary to support the proper operation of the Integration. If the Company identifies any technical issue, vulnerability, weakness, degradation, data discrepancy or other problem affecting or that may affect the Integration, the Platform or Protected Information, the Company shall promptly investigate, remediate, and mitigate the issue and keep PXP promptly and sufficiently informed of material developments.

7.5 The Company shall ensure that the Integration, the Company Systems and any Third-Party Dependencies do not introduce malware, malicious code, vulnerabilities, excessive traffic, denial of service conditions, unauthorised access paths or other security or operational risks to the Platform or the PXP Materials.

7.6 The Company shall maintain accurate and complete technical, operational and security logs relating to the Integration for such period as is required by Applicable Laws, Card Scheme Rules, the Company Agreement or PXP's reasonable instructions, and shall make relevant logs available to PXP where reasonably required to investigate incidents, disputes, errors, complaints, security events, regulatory enquiries, or reconciliation issues.

7.7 The Company shall not change the Company Systems, data formats, message flows, endpoints, security configuration, transaction flows, devices, third-party tools, or other elements of the Integration in a manner that may materially affect the Integration, the Platform, PXP Services, PXP Materials, or Protected Information without prior testing and, where PXP reasonably requires, prior written approval from PXP

7.8 The Company shall be responsible for the accuracy, completeness, legality and integrity of all Integration Data, instructions, requests, and messages submitted by or on behalf of the Company, its Merchants, customers, users, employees, contractors, agents, or Third-Party Dependencies through the Integration.

7.9 The Company shall not use the Integration to process unlawful, fraudulent, misleading, prohibited, restricted, or unauthorised transactions or data, or to circumvent any security, risk, compliance, routing, transaction monitoring, authentication or other control implemented by PXP or any Third-Party Dependency.

7.10 The Company shall promptly notify PXP of any material change to the Company Services, the Company Systems, ownership, control, business model, regulated status, licences, permissions, payment flows, Merchant base, transaction profile or risk profile that may affect the Integration, PXP, the Platform, or the PXP Services.

7.11 The Company shall implement and maintain appropriate idempotency controls, deduplication controls, and transaction state management controls to prevent duplicate transactions, authorisations, captures, refunds, voids, reversals, payouts, settlement requests, webhooks, notifications, and other duplicate or inconsistent processing through the Integration.

7.12 The Company shall comply with all API rate limits, usage limits, concurrency limits, and traffic management requirements notified or made available by PXP from time to time, and shall implement appropriate retry, timeout, backoff, throttling, circuit-breaker and error-handling mechanisms to ensure that the Integration does not generate excessive, duplicate, or harmful traffic or otherwise affect the Platform.

7.13 The Company shall properly handle all API responses, error codes, asynchronous messages, callbacks, webhooks, notifications, and transaction status updates made available through the Integration. The Company shall not treat a transaction, capture, refund, payout, settlement requests or other payment actions as successful, failed, cancelled, or final unless the relevant status is received and interpreted in accordance with the Integration Manuals and PXP's written instructions.

7.14 The Company shall maintain accurate reconciliation, transaction lifecycle and state-management processes for all transactions or data processed through the Integration, including controls to identify and resolve mismatches, missing

webhooks, duplicate messages, pending states, rejected requests, timeout scenarios and inconsistent records.

7.15 The Company shall not disable, bypass or materially alter any idempotency, security, risk, transaction monitoring, authentication, reconciliation, webhook, status management, rate-limiting or other controls required by the Integration Manuals or PXP's written instructions without PXP's prior written approval.

8. Supported Versions, Compatibility and Migration

8.1 The Company shall maintain compatibility with the Supported Versions of the Platform, APIs, SDKs, endpoint, Integration Materials, security requirements and other PXP integration requirements notified or made available by PXP from time to time.

8.2 The Company shall implement any changes, upgrades, migrations, replacements or remediation reasonably required by PXP within the timeframes specified by PXP in writing, taking into account the nature, complexity, risks and urgency of such changes.

8.3 Where PXP deprecates, withdraws, replaces, or migrates any API, SDK, endpoint, Platform component, Integration Material or integration method, the Company shall migrate to the replacement or Supported Version within the notice period specified by PXP or, if no period is specified, within a commercially reasonable period. PXP may restrict, suspend, or terminate access to unsupported or deprecated versions after the applicable notice period or earlier required for security, regulatory, Card Scheme, operational or other risk reasons.

9. PXP Responsibilities

9.1 PXP shall use commercially reasonable endeavours to make available the relevant APIs, SDKs, Integration Manuals and other documentation required for the Integration, to the extent agreed by the Parties and subject to the Company Agreement, planned maintenance, emergency maintenance, service availability, technical limitations, security controls, Applicable Laws, Card Scheme Rules, and any Third-Party Dependencies.

9.2 Where PXP has agreed to support the Integration, PXP shall make available reasonable technical support to assist the Company in resolving issues directly related to the Platform. Unless expressly agreed otherwise, PXP is not responsible for first-line support, Merchant support, Company Systems, Company Materials, or Third-Party Dependencies.

9.3 PXP shall use commercially reasonable endeavours to maintain the PXP APIs, SDKs, Integration Materials, documentation and development tools made available by PXP

in accordance with PXP's internal security and compliance standards and Applicable Laws applicable to PXP.

9.4 PXP may provide reasonable guidance to support the Company's implementation of the Integration in accordance with PXP's security and compliance requirements.

10. Support and Incident Handling

10.1 Unless otherwise agreed in the Company Agreement, the Company shall retain first-line operational ownership for Integration issues affecting Merchants, customers, users, or the Company Systems. Prior to escalating any an issue to PXP, the Company shall conduct an initial investigation, reproduce or evidence the issue where practicable, review relevant logs, identify whether the issue arises from the Company Systems or Third-Party Dependencies, and provide PXP with the information and materials necessary to investigate any issue related to the Platform.

10.2 The Company shall not transfer operational support responsibilities for the Integration to PXP except to the extent an issue is directly caused by the Platform or PXP Materials. PXP may reject or return requests events that do not include investigation details, logs, correlation identifiers, transaction references, timestamps, environment details and steps to reproduce where such information is reasonably available to the Company.

10.3 Where a Material Integration Incident is caused by, relates to or is reasonably suspected to relate to the Company Systems, the Company Materials, Third-Party Dependencies, or the Company's implementation or configuration, the Company shall provide PXP with a written root cause analysis, impact assessment and remediation plan within a reasonable timeframe specified by PXP. The Company shall implement the remediation plan at its own expense and provide evidence of completion where required by PXP.

10.4 The Parties shall cooperate to identify, investigate and resolve incidents affecting the Integration, including system outages, data discrepancies, complaints, reconciliation issues, and Security Incidents. The Company remains responsible for the investigation and remediation of issues arising from the Company Systems, Company Materials, Third-Party Dependencies or the Company's implementation, configuration or operation of the Integration.

11. Third-Party Dependencies

11.1 Any Third-Party Dependency used by the Company as part of, or in connection with, the Integration must be pre-approved by PXP in writing where it may access, connect to, process or affect the Platform, PXP Materials, Protected Information or PXP Services

11.2 The Company shall ensure that all Third-Party Dependencies used by or on behalf of the Company comply with the technical, operational, security and regulatory standards required under these Integration Terms.

11.3 The Company shall bear all costs associated with the use of Third-Party Dependencies used by or on behalf of the Company.

11.4 The Company remains responsible for all Third-Party Dependencies used by or on behalf of the Company, including their security, availability, performance, acts, omissions, compliance with Applicable Laws and Card Scheme Rules, and impact on the Integration. PXP shall not be liable for any failure, delay, loss, compromise, outage, incompatibility, non-compliance or other issue caused by or relating to any Third-Party Dependency not provided or controlled by PXP.

11.5 PXP may require the Company to remove, disable, replace or remediate any Third-Party Dependency where PXP reasonably considers that it creates or may create legal, regulatory, security, operational, financial crime, Card Scheme, reputational or technical risk to PXP, the Platform, PXP Services, Merchants or customers.

11.6 The Company shall monitor Third-Party Dependencies used by or on behalf of the Company for end-of-life status, deprecation, vulnerabilities, performance issues, changes to functionality, terms, data flows and other risks that may affect the Integration, and shall promptly remediate, replace or remove any Third-Party Dependency that becomes unsupported, incompatible, vulnerable, non-compliant or unsuitable for continued use with the Integration.

12. Compliance, Data Protection and Security Attestations

12.1 Each Party shall comply with Applicable Laws and Card Scheme Rules in connection with the Integration, the operation and use of the Platform and the provision of its respective services.

12.2 Each Party shall comply with Data Protection Laws in connection with the Integration. The Parties' respective data protection roles shall be as set out in the Company Agreement, any applicable data processing agreement or data sharing agreement between the Parties and, where not expressly stated, shall be determined by reference to the actual Processing activities undertaken by each Party. Nothing in these Integration Terms is intended to alter the Parties' data protection roles under any separate data protection agreement between them.

12.3 Where and to the extent the Company Processes Personal Data on behalf of PXP as a processor, the Company shall: (a) Process Personal Data solely in accordance with PXP's documented instructions unless required otherwise by Applicable Laws; (b) implement appropriate technical and organisational measures to protect Personal Data; (c) ensure personnel authorised to Process Personal Data are trained

and bound by confidentiality obligations; (d) cooperate with PXP in relation to Data Subject Rights, regulatory inquiries, breach notifications, records of processing and Data Protection Impact Assessments; (e) ensure international transfers comply with Data Protection Laws; and (f) permit PXP, its auditors and, where applicable, regulators, Card Schemes or Payment Providers to verify compliance with Data Protection Laws.

12.4 The Company shall comply with Applicable AML Regulations to the extent applicable to its role, the Company Services, the Integration and any Merchants, customers, end users, partners or other third parties interacting with the Integration through or on behalf of the Company. The Company shall not use, or permit the use of, the Integration, Platform or PXP Services in a manner that facilitates money laundering, terrorist financing, sanctions breaches, fraud, bribery, corruption or other illegal activity.

12.5 The Company shall maintain accurate, complete and verifiable records relating to the Integration, transactions, users, Merchants, due diligence, risk assessments and compliance matters to the extent required by Applicable Laws, Applicable AML Regulations, Card Scheme Rules and the Company Agreement, and shall promptly notify PXP of suspicious, unusual, fraudulent, unlawful or prohibited activity identified in connection with the Integration, subject to Applicable Laws.

12.6 The Company shall comply with applicable industry-standard security frameworks and payment security requirements, including PCI DSS where cardholder data or card payment functionality is involved. The Company shall notify PXP in writing without undue delay and in any event within 24 hours after becoming aware of any actual or suspected Security Incident affecting the Integration, Platform, Credentials, Protected Information or Personal Data processed in connection with the Company Agreement.

12.7 Unless otherwise required by PXP, the Company shall complete an initial security, compliance and integration attestation before Go-Live and thereafter provide an annual or periodic evidence refresh at a frequency specified by PXP. PXP may rely on current independent certifications, attestations, audit reports or secure development evidence provided by the Company where PXP considers such evidence sufficient for the relevant Integration risk profile.

12.8 The Company shall provide additional attestations, updated documentation, testing evidence or remediation evidence where there is a material architectural, security, compliance, data flow, payment flow, transaction state management, permission, endpoint, Third-Party Dependency or operational change, or where PXP reasonably requires such evidence following a Security Incident, Material Integration Incident, audit finding, regulatory request, Card Scheme request or other risk event. Routine

Updates shall not require a new attestation unless PXP determines that a particular Routine Update affects or may affect the risk profile of the Integration.

12.9 The Company shall not input, upload, disclose or otherwise process Protected Information through any AI Technology, analytics, monitoring, debugging, support or third-party tool unless expressly permitted under the Company Agreement or approved by PXP in writing and subject to such conditions as PXP may require.

12.10 If the Integration involves cardholder data, card transactions, POS, payment terminals, payment applications, hosted payment pages, wallets or other payment functionality, the Company shall comply with all applicable PCI standards, Card Scheme Rules, device certification requirements, payment application requirements, security attestations and implementation requirements notified by PXP, the Card Schemes or any relevant Payment Provider or Acquirer.

13. Audit and Evidence Rights

13.1 To verify compliance with the Company Agreement, these Integration Terms, Applicable Laws, Card Scheme Rules and PXP's security, operational and compliance requirements, PXP may, on reasonable prior written notice, audit or require evidence of the Company's use of the Platform, Integration Materials and Integration.

13.2 Audits shall occur no more than annually unless PXP reasonably suspects misuse, non-compliance or a Security Incident, or where an audit is required by Applicable Laws, a regulator, Card Scheme, Payment Provider, Acquirer or other competent authority. The Company shall provide reasonable cooperation, access to relevant records, personnel, systems, policies, procedures, logs and evidence, and shall promptly remediate material findings within a timeframe reasonably specified by PXP.

13.3 PXP may suspend the Integration, restrict access, rotate Credentials or require immediate remediation where an audit, assessment or other review identifies a material vulnerability, compliance failure, misuse, security weakness or other risk affecting PXP, the Platform, PXP Services, Merchants, customers or Protected Information.

14. Intellectual Property Rights

14.1 Each Party retains all rights, title and interest in and to its pre-existing Intellectual Property Rights and materials. As between the Parties, PXP owns and retains all rights, title and interest in and to the PXP Materials, Platform, Integration Materials, PXP Services and all Intellectual Property Rights in the foregoing, including any modifications, enhancements, derivative works, analytics, aggregated data, operational data, know-how, documentation, specifications, reports and other materials developed by or on behalf of PXP in connection with the Integration. The

Company owns and retains all rights, title and interest in and to the Company Materials and Company Systems, excluding any PXP Materials incorporated in or accessed through them.

14.2 Subject to the Company Agreement and these Integration Terms, PXP grants the Company a limited, non-exclusive, non-transferable, non-sublicensable, revocable licence during the term of the Company Agreement to access and use the relevant PXP Materials solely to develop, test, deploy, operate and maintain the Integration and provide the Company Services in accordance with the Company Agreement.

14.3 Subject to the Company Agreement and these Integration Terms, and to the extent necessary for PXP to perform its obligations, the Company grants PXP a limited, non-exclusive, non-transferable, revocable licence during the term of the Company Agreement to access and use the Company Systems and Company Materials solely for the purpose of developing, testing, deploying, operating, supporting and maintaining the Integration and performing PXP's obligations under the Company Agreement.

14.4 The Company shall not: (a) reverse engineer, decompile or disassemble any part of the Platform, PXP Materials or Integration Materials; (b) remove, alter or obscure any proprietary notices on or within the Platform, PXP Materials or Integration Materials; or (c) use the Platform, PXP Materials or Integration Materials for any purpose other than as permitted under these Integration Terms and the Company Agreement.

14.5 On termination or expiry of the Company Agreement, or termination or suspension of the Integration, all licences granted under these Integration Terms shall automatically terminate or be suspended to the extent required by PXP, and the Company shall immediately cease using the Platform, PXP Materials and Integration Materials except as expressly authorised by PXP in writing.

15. Confidentiality and Protected Information

15.1 The Company shall keep confidential and protect all Confidential Information and Protected Information disclosed or made available by or on behalf of PXP in connection with the Integration, and shall use such information only for the purpose of performing the Integration and complying with the Company Agreement.

15.2 The Company shall not disclose PXP Confidential Information or Protected Information to any person except to its employees, contractors, advisers and approved subcontractors who need to know it for the permitted purpose and who are bound by confidentiality obligations at least as protective as those set out in these Integration Terms or the Company Agreement.

15.3 On request, termination, expiry or suspension, the Company shall return or securely delete all PXP Confidential Information, Protected Information, Credentials, documentation and materials belonging to PXP, except to the extent retention is

required by Applicable Laws, and shall confirm deletion or return in writing within 10 Business Days after PXP's request.

16. Suspension, restriction and termination of Integration

16.1 PXP may suspend, restrict, disable or terminate the Integration, access to the Platform or any Integration Materials immediately on written notice, or without prior notice where PXP reasonably considers immediate action necessary, where:

- the Company materially breaches the Company Agreement or these Integration Terms, including any regulatory, data protection, security, PCI, Card Scheme or compliance obligation;
- the Company uses the Platform, APIs, SDKs or related tools in breach of the Company Agreement, these Integration Terms, the Integration Manuals or PXP's written instructions;
- the Company's operations or the Integration become non-compliant with Applicable Laws, regulatory requirements or Card Scheme Rules and such non-compliance is not remediated within any period specified by PXP, if capable of remediation;
- the Company ceases operations, becomes insolvent or undergoes a significant change in ownership or control that adversely impacts its ability to fulfil its obligations;
- the Company Agreement is terminated or expires;
- PXP reasonably suspects a Security Incident, fraud, misuse, unauthorised access, credential compromise, excessive traffic, vulnerability, malware, data breach, Card Scheme issue, regulatory issue, financial crime risk or other risk affecting PXP, the Platform, PXP Services, Merchants, customers, Protected Information or any Third-Party Dependency;
- continued operation of the Integration may, in PXP's reasonable opinion, expose PXP to legal, regulatory, Card Scheme, payment provider, acquirer, operational, security, financial, financial crime, reputational or technical risk;
- a regulator, Card Scheme, Payment Provider, Acquirer, court, governmental authority or other competent authority requires or requests suspension, restriction or termination;
- the Company fails to complete or maintain any certification, testing, remediation, security attestation, audit requirement, PCI requirement or other requirement specified by PXP;
- the Company fails to make meaningful progress with the Integration for any period specified in the Integration Details or, if no period is specified, for 60 days; or
- the Company fails to migrate from, remediate or cease use of an unsupported, deprecated, incompatible, vulnerable or non-compliant

version, endpoint, API, SDK, POS Application, device model, operating system, firmware version, Third-Party Dependency or other component.

16.2 On termination or suspension, the Company's access to the Platform, APIs, SDKs, Credentials and other Integration Materials shall be terminated, suspended or restricted as directed by PXP and the Company shall cease all use of the Integration, Platform, Integration Materials and documentation unless otherwise agreed by PXP in writing.

16.3 Where applicable, the Company shall notify Merchants of the termination or suspension and provide reasonable support to facilitate transition to alternative solutions, subject always to PXP's reasonable instructions and Applicable Laws.

16.4 The provisions relating to confidentiality, data protection, security, intellectual property, audit, payment, liability, indemnity and any other obligations that by their nature should survive termination shall remain in full force and effect.

17. Warranties and disclaimers

17.1 PXP warrants that, where PXP makes Integration Materials available to the Company, such Integration Materials will materially conform to PXP's official documentation in all material respects. PXP does not warrant that the Integration, Platform, PXP Materials or PXP Services will be uninterrupted, error-free, free from vulnerabilities, compatible with the Company Systems or any Third-Party Dependency, or that any particular transaction, message, request, data exchange, payment method or service will be completed, authorised, processed or successful.

17.2 The warranty in clause 17.1 does not apply to any non-conformance caused by: (a) misuse of the Integration by the Company; (b) modifications made by the Company or any third party not authorised by PXP; (c) damage not attributable to PXP; (d) any Company System or Third-Party Dependency; or (e) the Company's failure to follow PXP's instructions.

17.3 PXP's sole liability and the Company's exclusive remedy for any breach of the warranty in clause 17.1 shall be for PXP to use commercially reasonable endeavours to repair or modify the relevant PXP Integration Materials to restore material compliance, or where PXP determines that repair or modification is not commercially reasonable, to terminate or suspend the affected Integration or access to the relevant PXP Integration Materials.

17.4 The Company warrants that: (a) it has all rights, licences, permissions and authority required to perform the Integration and provide the Company Services; (b) the Company Systems, Company Materials and Third-Party Dependencies used by or on behalf of the Company will not infringe any third-party rights, introduce malware or compromise the Platform; (c) it will comply with these Integration Terms, Applicable Laws, Card Scheme Rules and the Company Agreement; and (d) it will

not submit any unlawful, inaccurate, unauthorised, misleading or malicious data, instruction or request through the Integration.

17.5 Except as expressly stated in these Integration Terms or the Company Agreement, all warranties, conditions, representations and terms, whether express or implied by statute, common law, custom, trade usage or otherwise, are excluded to the fullest extent permitted by Applicable Laws, including any implied warranties of merchantability, satisfactory quality, fitness for purpose, non-infringement, compatibility, availability, performance or uninterrupted operation.

17.6 Any performance targets, service levels, availability targets, timelines, implementation estimates, integration timeframes or success metrics referred to in marketing materials, proposals, presentations or discussions are not binding unless expressly incorporated into the Company Agreement as binding service levels or commitments.

18. Indemnity

18.1 The Company shall indemnify, defend and hold harmless PXP and its Affiliates, officers, directors, employees, agents, subcontractors and representatives from and against any loss, damage, cost, liability, fine, penalty, assessment, chargeback, fee and expense, including reasonable legal fees ("Losses"), arising from or relating to any claim, demand, action, investigation or proceeding alleged or asserted by a third party, regulator, Card Scheme, Payment Provider, Acquirer, Merchant, customer or other person to the extent arising out of or relating to:

- the Company's use of the Integration, Platform, PXP Materials or Integration Materials other than as expressly permitted by the Company Agreement, these Integration Terms, the Integration Manuals or PXP's written instructions;
- the use, operation, configuration or combination of the Integration, Platform or PXP Materials with Company Systems, Company Materials, Third-Party Dependencies, software, data, equipment, specifications or materials not provided or controlled by PXP;
- any breach by the Company of confidentiality, data protection, information security, AML, sanctions, PCI DSS, Card Scheme Rules or Applicable Laws;
- any Security Incident, unauthorised access, data loss, credential compromise, malware, system downtime, vulnerability or disruption caused by or relating to the Company, Company Systems, Company Materials, Company personnel or any Third-Party Dependency used by or on behalf of the Company;
- any personal injury, death or damage to tangible property to the extent caused by the Company's wrongful acts or omissions;

- the acts or omissions of Merchants, customers, users, employees, contractors, agents, Affiliates or subcontractors of the Company;
- any violation of required end user, Merchant or customer terms and conditions by customers or Merchants of the Company;
- any infringement or alleged infringement by Company Materials, Company Systems or Company-provided data, specifications or instructions;
- the Company's wilful misconduct, fraud, negligence or breach of these Integration Terms; and
- duplicate transaction processing, duplicate authorisations, captures, refunds or settlement requests, incorrect transaction routing, malformed or unauthorised requests, incorrect webhook handling, failure to implement idempotency or deduplication controls, failure to comply with API rate limits or retry/backoff requirements, reconciliation discrepancies, incorrect transaction status handling or any other Integration Defect caused by or related to the Company Systems, Company Materials, Third-Party Dependencies or the Company's implementation, configuration, operation or maintenance of the Integration.

18.2 Subject to the Company Agreement and any applicable limitation of liability, PXP shall indemnify the Company from and against Losses arising from third-party claims to the extent arising out of any claim that the Platform or PXP Materials, when used by the Company strictly in accordance with the Company Agreement, these Integration Terms and the Integration Manuals, infringe any UK patent, copyright or trade mark in effect as of the date on which the relevant Integration Materials are made available to the Company.

18.3 If all or any part of the Platform or PXP Materials becomes, or in PXP's opinion is likely to become, the subject of an infringement claim, the Company shall permit PXP, at PXP's option and expense, to: (a) procure for the Company the right to continue using the affected item; (b) replace or modify the affected item so that the Company's use becomes non-infringing without materially impairing its core functionality; or (c) terminate or suspend the Company's use of the affected item. PXP's indemnity shall not apply to claims arising from unauthorised use, modification or combination with Company Systems, Company Materials, Third-Party Dependencies or Company-provided specifications, data or instructions.

19. Limitation of Liability

19.1 Subject to any liability that cannot lawfully be excluded or limited, and without prejudice to any lower cap or exclusion in the Company Agreement, PXP shall not be liable to the Company under any theory or circumstance for loss of profit, loss of revenue, loss of business, loss of goodwill, loss of anticipated savings, loss or corruption of data, indirect loss, special loss, incidental loss, consequential loss,

exemplary damages or punitive damages arising out of or relating to these Integration Terms, the Integration, the Platform or any Integration Materials.

19.2 Subject to the Company Agreement and any liability that cannot lawfully be excluded or limited, PXP's aggregate liability under these Integration Terms for all claims arising out of or relating to these Integration Terms, the Integration, the Platform or any Integration Materials shall not exceed the fees actually paid to PXP by the Company and/or the fees paid by PXP to the Company (as the case may be) for the PXP services and/or the Company services (as the case may be) directly connected with the relevant Integration in the 12-month period preceding the event giving rise to liability.

19.3 Nothing in these Integration Terms shall limit the Company's obligation to pay fees, charges, refunds, chargebacks, assessments, fines or other amounts due under the Company Agreement, or the Company's indemnity obligations under clause 18, except to the extent such obligations are expressly limited by the Company Agreement.

20. Security and Operational Requirements

20.1 The Company shall maintain an information security programme appropriate to the nature, scale and risk of the Integration and shall align such programme with recognised industry standards, including ISO 27001, SOC 2, NIST, PCI DSS or equivalent standards where applicable.

20.2 The Company shall implement access control, multi-factor authentication where appropriate, secure credential storage, encryption in transit, encryption at rest where appropriate, vulnerability management, patch management, malware protection, change control, logging, monitoring, backup, incident response and business continuity controls for the Company Systems and any systems used to access or operate the Integration.

20.3 The Company shall remediate critical vulnerabilities without undue delay and in any event within any timeframe specified by PXP where the vulnerability may affect the Platform, PXP Materials, Protected Information, Merchants or customers.

20.4 The Company shall segregate production, testing and development environments and shall not use live Personal Data or live payment data in non-production environments unless expressly approved by PXP in writing and permitted by Applicable Laws, Card Scheme Rules and PCI DSS.

20.5 The Company shall maintain appropriate incident response and business continuity arrangements and shall cooperate with PXP in any incident, outage, disaster recovery, continuity or regulatory exercise affecting the Integration.

20.6 The Company shall provide PXP, on request, with evidence of compliance with these Integration Terms, including policies, certifications, attestations, penetration test summaries, vulnerability remediation evidence, PCI documentation and other relevant security or compliance evidence.

21. Order of precedence

21.1 These Integration Terms form part of the Company Agreement. Unless otherwise agree in the Company Agreement, in the event of a conflict between these Integration Terms and the Company Agreement, these Integration Terms shall prevail only to the extent of the conflict and only in relation to the Integration, Platform access, Integration Materials, security, technical, operational, data protection, compliance and other matters expressly addressed in these Integration Terms.

21.2 These Integration Terms shall not amend, override or disapply the commercial terms, payment terms, settlement terms, regulated service terms, acquiring terms, aggregation terms, gateway terms, general limitation of liability, governing law or termination provisions of the Company Agreement except to the extent expressly stated in these Integration Terms.

21.3 Nothing in these Integration Terms shall be construed to increase or expand PXP's liability beyond the limitations agreed in the Company Agreement or these Integration Terms, nor shall it create any obligation for PXP that is not expressly set out in the Company Agreement or these Integration Terms.

22. Governing Law and Jurisdiction

22.1 Unless the Company Agreement expressly provides otherwise, these Integration Terms and any dispute or claim arising out of or in connection with them, their subject matter or formation, including non-contractual disputes or claims, shall be governed by and construed in accordance with the laws of England and Wales.

22.2 Unless the Company Agreement expressly provides otherwise, the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with these Integration Terms, their subject matter or formation, including non-contractual disputes or claims.

POS Integration Requirements and Attestation Terms

1. Scope

1.1 This POS Integration Requirements and Attestation Terms (the "**POS Integration Terms**") apply where the Integration involves, enables or is connected with any point-of-sale device, payment terminal, payment entry device, merchant application, vendor application, software component, SDK, API, plug-in, service or other technology that is deployed on, communicates with or operates in connection with a POS Device or the PXP Payment Application (a "**POS Integration**").

1.2 The Company shall comply with these POS Integration Terms in addition to the main body of he Integration Terms, the Company Agreement, the Integration Manuals, the applicable PCI standards, the Card Scheme Rules, Applicable Laws and any other instructions or requirements notified by PXP from time to time.

1.3 PXP may withhold, suspend or withdraw approval for any POS Integration, POS Application, device model, operating system, firmware version, SDK/API version or release version unless PXP is satisfied that the Company has complied with these POS Integration Terms.

2. Additional POS Definitions

Cardholder Data or CHD	has the meaning given to cardholder data under PCI DSS and includes, without limitation, the primary account number and any related cardholder data to the extent regulated by the PCI standards.
Sensitive Authentication Data or SAD	has the meaning given to sensitive authentication data under PCI DSS and includes, without limitation, full track data, card verification codes or values, PINs and PIN blocks, and any equivalent sensitive payment authentication data.
Payment Components	means the PXP Payment Application, payment kernel, SRED module, PIN entry components, card reader components, secure cryptographic components, key management components and any other payment acceptance, encryption, authentication or security component forming part of, or connected with, a POS Device or the PXP payment environment.
PCI Standards	means all applicable PCI Security Standards Council standards, requirements, guidance and validation programmes applicable to the POS Integration, including PCI DSS, PCI PTS POI, PCI Secure

	Software Standard, PCI Secure Software Lifecycle requirements and any successor or replacement standards.
POS Application	means any application, software, firmware, code, APK, package, SDK, plug-in, service, update, patch or other component provided, developed, operated or controlled by or on behalf of the Company that is installed on, deployed to, communicates with or otherwise interacts with a POS Device or the PXP Payment Application.
POS Device	means any physical or virtual point-of-sale device, payment terminal, payment entry device, peripheral, operating environment or other hardware or software environment used to initiate, accept, process or facilitate card-present or other point-of-sale transactions in connection with PXP Services.
POS Attestation Pack	means the vendor, technical, compliance and security documentation and attestations required under these POS Integration Terms in relation to a POS Integration or POS Application.
PXP Payment Application	means the PXP payment application or other PXP-controlled payment software, application, service or component operating on, connected with or supporting a POS Device.

3. POS Approval and Attestation Pack

3.1 Before any POS Application or POS Integration is deployed, tested in production, made available to any Merchant or used in connection with PXP Services, the Company shall provide a complete POS Attestation Pack to PXP in the form and manner required by PXP.

3.2 The POS Attestation Pack shall include, as a minimum:

- the Company name, application name, application version, contact name, contact email, phone number, website, supported POS Device model(s), supported operating system and Android version(s), and SDK/API version(s) used;
- vendor release notes describing all new, changed or removed functionality in the relevant release;
- a current application data flow diagram showing all logical interfaces, system boundaries, data flows, network endpoints, external services and third-party dependencies;

- a complete list of all device, operating system, browser, network and other permissions requested or used by the POS Application;
- details of all services, APIs, broadcasts, intents, inter-process communications, background services, scheduled jobs, device functions, libraries, SDKs and third-party components used by the POS Application;
- a current security testing report, which may include automated static analysis, dynamic analysis, dependency scanning, penetration testing or other testing reasonably acceptable to PXP;
- the cryptographic hash, using SHA-256 or another algorithm approved by PXP, of the release binary, APK or other deployable package;
- evidence of the Company's documented secure software development lifecycle, including secure coding, peer review, vulnerability management and release control processes;
- PCI Secure Software Standard validation evidence where applicable, including the applicable listing number, version numbers matching the attestation of compliance and PCI SSC listing, and the PCI SSC-countersigned attestation of compliance; and
- a signed attestation in accordance with clause 11 of this Annex

3.3 The Company warrants that all information provided in the POS Attestation Pack is complete, accurate, not misleading and kept up to date. The Company shall promptly notify PXP of any error, omission or change affecting the information previously supplied.

4. Technical Restrictions and Protected Payment Environment

4.1 The Company shall ensure that the POS Application and POS Integration do not access, store, process, transmit, intercept, display, log, cache, copy or otherwise handle clear-text CHD or SAD.

4.2 The Company shall ensure that the POS Application and POS Integration do not access, interfere with, bypass, modify, disable, monitor, emulate, reverse engineer, scrape, overlay, capture input from or otherwise interact with any Payment Components except through documented APIs, SDKs or interfaces expressly approved by PXP in writing.

4.3 Without limiting clause 4.2, the Company shall not access or attempt to access the payment kernel, SRED module, PIN entry components, card reader components, secure cryptographic functions, key material, secure memory, protected transaction flows or the PXP Payment Application except as expressly authorised by PXP in writing.

4.4 The Company shall ensure that the POS Application is logically isolated from the Payment Components and does not degrade, delay, interrupt, compromise or

otherwise adversely affect the security, performance, availability, certification status or compliance of the POS Device, the PXP Payment Application, the Platform or any PXP Services.

4.5 The Company shall not include any functionality that is malicious, deceptive or excessive in relation to the purpose of the POS Integration, including key logging, screen scraping, credential harvesting, unauthorised overlays, unauthorised remote access, unauthorised privilege escalation, unauthorised debugging, disabling of security controls or transmission of data to unapproved endpoints.

5. POS Security and Compliance Obligations

5.1 The Company shall design, develop, test, deploy, operate and maintain the POS Application and POS Integration in accordance with Applicable Laws, Card Scheme Rules, PCI Standards, Integration Manuals, these POS Integration Terms and good industry practice.

5.2 The Company shall maintain and follow a documented secure software development lifecycle appropriate to the risk profile of the POS Application and POS Integration. Such lifecycle shall include secure design, threat modelling where appropriate, secure coding standards, code review, dependency and open-source component management, vulnerability scanning, security testing, remediation, release approval, secure build processes and secure distribution controls.

5.3 The Company shall ensure that all vulnerabilities identified in connection with the POS Application or POS Integration are assessed, prioritised and remediated before release. Critical, high and exploitable vulnerabilities, and any vulnerability that may affect CHD, SAD, Payment Components, PXP systems or Merchant systems, must be remediated before deployment unless PXP gives prior written approval to an alternative remediation plan.

5.4 The Company shall apply the principle of least privilege to all permissions, services, network access, accounts, credentials and data flows used by the POS Application. The POS Application shall request and use only those permissions strictly necessary for its approved functionality.

5.5 The Company shall implement appropriate controls for authentication, access control, encryption in transit, certificate validation, secrets management, code signing, integrity verification, tamper resistance, logging, monitoring, malware prevention, patching and secure configuration.

5.6 Logs generated by or in connection with the POS Application shall not contain CHD, SAD, security credentials, secrets, keys or other protected data, and shall be protected against unauthorised access, modification and disclosure.

6. PCI Validation and Regulatory Evidence

6.1 The Company shall inform PXP whether the POS Application is validated against the PCI Secure Software Standard or any successor or equivalent standard. Where the POS Application is validated, the Company shall provide the applicable listing number, matching version details and PCI SSC-countersigned attestation of compliance.

6.2 The Company shall maintain all certifications, attestations, assessments, reports and evidence required to demonstrate compliance with the PCI Standards, Applicable Laws and these POS Integration Terms and shall provide copies to PXP on request.

6.3 PXP approval of a POS Integration or POS Application does not constitute a certification, validation, audit opinion, legal opinion or warranty that the Company, POS Application or POS Integration complies with any PCI Standard, Applicable Law, Card Scheme Rule or third-party requirement.

7. POS Change Control and Future Releases

7.1 The Company shall obtain PXP approval before deploying any material change into production. A change shall be deemed material if it may affect functionality, data flows, security, compliance, performance, availability, user permissions, device functions, Payment Components, PXP systems, Merchant systems or the scope of any previous approval or attestation.

7.2 For Routine Updates, PXP may permit the Company to rely on its existing approval, secure software development lifecycle, release control process and periodic evidence refresh, provided that the Routine Update does not materially change the POS Integration risk profile or invalidate any previous attestation. The Company remains responsible for maintaining accurate records, checksums, test evidence and vulnerability remediation evidence for Routine Updates, and shall promptly provide such evidence as PXP may request.

7.3 PXP may require a new POS Attestation Pack, new signed attestation or additional evidence for a Routine Update where PXP considers this necessary due to the nature of the update, a security finding, incident, vulnerability, PCI requirement, Card Scheme requirement, regulatory request, Merchant impact or other risk, legal, reputational, regulatory or operational consideration.

7.4 Where an emergency security update is required to mitigate an active or imminent security risk, the Company shall notify PXP without undue delay and shall provide updated documentation, test results, cryptographic hash and attestation as soon as reasonably practicable and in any event within any timeframe required by PXP.

8. PXP Verification and Testing

8.1 The Company consents to PXP and its representatives performing independent verification, security review, functional testing, integrity checks and other testing of the POS Application and POS Integration as part of PXP's approval, onboarding, monitoring, incident response or audit processes.

8.2 The Company shall provide reasonable cooperation, information, access, test builds, test credentials, documentation, technical contacts, logs and other materials reasonably required by PXP for such verification and testing.

8.3 PXP may reject, suspend, require changes to or withdraw approval for any POS Application or POS Integration if PXP identifies or reasonably suspects a security, compliance, operational, integrity, certification, fraud, financial crime, reputational or other risk.

9. POS Deployment and Operational Controls

9.1 The Company shall ensure that only POS Applications, versions, builds, checksums, device models, operating system versions, firmware versions and SDK/API versions approved by PXP are deployed or used in connection with the POS Integration.

9.2 The Company shall maintain accurate records of all approved and deployed POS Applications, versions, builds, checksums, device models, operating system versions, firmware versions, SDK/API versions, deployment channels, Merchants and sites, and shall provide such records to PXP on request.

9.3 The Company shall immediately disable, remove, remediate or replace any POS Application, version, build or component that is unauthorised, unsupported, vulnerable, non-compliant, compromised, inconsistent with its attestation, or otherwise reasonably required by PXP to be disabled, removed, remediated or replaced.

10. POS Security Incidents and Vulnerabilities

10.1 The Company shall notify PXP in writing without undue delay and, in any event, within 24 hours after becoming aware of any actual or suspected security incident, vulnerability, compromise, unauthorised access, malware, data loss, integrity failure, breach of these POS Integration Terms or other event that relates to, affects or may affect the POS Application, POS Integration, POS Device, a Merchant, PXP systems, Payment Components, CHD, SAD, Personal Data or PXP Services.

10.2 The notification shall include, to the extent known at the time: (a) a description of the incident or vulnerability; (b) the systems, data, Merchants, devices, applications, versions and environments affected; (c) the likely cause and impact; (d) the actions taken or proposed to contain, investigate and remediate the matter; and (e) any further information reasonably required by PXP.

10.3 The Company shall cooperate fully with PXP in relation to incident response, investigation, containment, remediation, evidence preservation, communications, notifications, forensic review and any required reporting to Merchants, regulators, Card Schemes, Payment Providers, Acquirers or other third parties.

10.4 The Company shall not make any public statement or notify any Merchant, regulator, Card Scheme, Payment Provider, Acquirer or other third party in a manner that refers to PXP, PXP Services, the Platform, Payment Components or PXP systems without first consulting PXP, unless prohibited by Applicable Laws.

11. POS Integration Attestation

11.1 The Company shall provide a signed POS integration attestation for each POS Application and each material release, update or change. The attestation shall be signed by an authorised representative of the Company and shall include the signatory's name, title, company name and date of signature.

11.2 The attestation shall confirm that:

- the POS Application does not have any logical interface that allows storage, processing or transmission of clear-text CHD or SAD;
- the POS Application does not access the payment kernel, SRED module, PIN entry components, card reader components or other Payment Components except as expressly authorised by PXP;
- the POS Application has been subjected to appropriate security testing and all identified vulnerabilities have been remediated before release or otherwise addressed to PXP's satisfaction;
- a cryptographic hash of the release package has been provided to PXP for integrity verification;
- the Company maintains and follows a documented secure software development lifecycle that includes secure coding, peer review and vulnerability management;
- all future material updates will be accompanied by updated documentation, test results, a new cryptographic hash and a new attestation;
- the Company consents to PXP performing independent verification and testing as part of the approval process and on an ongoing basis as reasonably required by PXP; and
- the Company will notify PXP within 24 hours of any security incident or suspected security incident related to the POS Application, POS Integration, POS Device, Payment Components, PXP systems or any related data.

12. POS Records, Warranties and Indemnity

12.1 The Company shall retain the POS Attestation Pack, security test reports, release notes, data flow diagrams, checksums, SDLC documentation, approval records,

deployment records, incident records and other evidence required to demonstrate compliance with these POS Integration Terms for the term of the Company Agreement and for six years thereafter, unless a longer period is required by Applicable Laws, Card Scheme Rules, PCI Standards or the Company Agreement.

12.2 The Company warrants, represents and undertakes that: (a) the POS Application and POS Integration comply with this Annex; (b) the POS Application does not access, store, process, transmit or expose clear-text CHD or SAD; (c) the POS Application does not access or interfere with Payment Components except as expressly authorised by PXP; (d) all vulnerabilities identified before release have been remediated or otherwise addressed to PXP's satisfaction; (e) the Company maintains and follows a secure software development lifecycle; (f) all information supplied to PXP is complete, accurate and not misleading; and (g) each material release and update is accompanied by the documentation, testing, hash and attestation required by this Annex.

12.3 The Company shall indemnify and hold harmless PXP, its Affiliates and their respective officers, directors, employees, agents and representatives from and against all losses, liabilities, damages, fines, penalties, assessments, costs and expenses arising out of or in connection with: (a) any breach of this Annex; (b) any unauthorised access to or compromise of CHD, SAD, Personal Data, Payment Components, PXP systems, the Platform, a POS Device or a Merchant system caused by or relating to the Company, the POS Application or the POS Integration; (c) any failure of the Company, POS Application or POS Integration to comply with Applicable Laws, Card Scheme Rules or PCI Standards; (d) any security incident, vulnerability, malware, defective code, unsupported component or third-party dependency relating to the POS Application or POS Integration; and (e) any fines, penalties, assessments, claims or remediation costs imposed by any Card Scheme, regulator, Acquirer, Payment Provider, Merchant or other third party in connection with the foregoing.

12.4 Nothing in these POS Integration Terms shall increase or expand PXP's liability beyond the limitations and exclusions agreed in the Company Agreement or these Integration Terms. PXP shall not be responsible for the Company's POS Application, Company Systems, third-party dependencies, Merchant systems, device manufacturer systems, operating systems or any other technology not provided or controlled by PXP.