**PARTNERSHIPS**
**SECURITY STANDARDS**

## 1. Definitions

| | |
|---|---|
| **Security Incident** | means breach of security affecting the Partner Services provided or leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Outpayce Data. |
| **Security Requirements** | means the Outpayce's policies, standards and procedures, including any security related requirements applicable to those systems, provided by Outpayce to the Partner from time to time. |
| **Industry Best Practices** | means the most effective methods, strategies, and procedures widely accepted and implemented by organizations within the payments industry to ensure optimal performance, security, and compliance with globally recognized standards, frameworks, and methodologies, such as ISO/IEC 27001, NIST Cybersecurity Framework, or CIS Controls, to effectively manage and protect information. |

## 2. Security standards

2.1 General

2.1.1 Any breach of any of the obligations outlined in this Appendix will be regarded as a material breach of the Contract.

2.1.2 The Partner must protect against the unauthorized access, collection, use, disclosure, copying, modification, alteration, disposal, accidental or unlawful destruction, damage to, theft or loss of Outpayce Data that is in the possession, control, or is otherwise processed by the Partner including those safeguards that are set forth in this section 2. This section 2 is based on ISO 27001 controls and require Partner to implement and maintain physical, administrative and technical safeguards designed to protect the confidentiality, integrity, availability and security of the products and services and security of Outpayce Data processed in the provision of the services.

2.1.3 When accessing Outpayce owned or managed information systems, networks or devices (including APIs, equipment or facilitates), the Partner (and its Personnel) will comply with the Security Requirements.

2.1.4 The Partner must develop and implement a security program against information security or cybersecurity attacks, aligned with Industry Best Practices.

2.2 Security Requirements

2.2.1 Information security. The Partner must maintain and comply with the Security Requirements. The Security Requirements will be reviewed and, if required, updated by the Partner at least on an annual basis, taking into account good industry practices.

2.2.2 Organization of information security

(a) Security ownership. The Partner will designate a security official responsible for information security and control and implementation of the Security Requirements.

(b) Security roles and responsibilities. The Personnel is subject to confidentiality obligations; Individuals will have documented security roles and responsibilities where relevant.

(c) Risk management program. The Partner will have in place a risk management process to perform risk assessments before and while providing the products and services.

(d) Reviews. The Partner must carry out security reviews periodically to ensure compliance with the policies and procedures established for these purposes.

2.2.3 Human resources security

(a) Screening. The Partner will screen Personnel as part of the hiring process, to the extent permitted by applicable law.

(b) During employment. The Partner will make Personnel aware of security rules and procedures through a documented security awareness and training program including informing the Personnel of consequences of breaching security rules and procedures.

(c) Termination of employment. The Partner must enforce the relevant Security Requirements, including the removal of system accesses after termination or change of employment of the Personnel.

2.2.4 Asset management

(a) Asset inventory. The Partner will maintain an inventory of (a) the place in which the Outpayce Data is stored and (b) all software and computer hardware assets (including removable devices) relating to the provision of services under this Contract.

(b) Classification and labelling of Outpayce Data. The Partner will ensure access to Outpayce Data is appropriately restricted, according to the classification.

(c) Acceptable use policy. The Partner will have in place an acceptable use policy that applies to information and assets that contain Outpayce Data.

(d) Handling of assets and disposal of assets. The Partner will have in place procedures for the handling, management and secure disposal of information and assets, including remote access or processing Outpayce Data outside of Outpayce's facilities

(e) Integrity. The Partner will maintain the accuracy and integrity of Outpayce Data throughout the assets' lifespan, from acquisition/development to decommissioning, and will store these assets on a network that is both logically and physically separate from other providers.

2.2.5 Access control

(a) Access policy. The Partner will maintain a record of access and security privileges of individuals having access to Outpayce Data.

(b) Access authorization. The Partner must maintain a record of Personnel authorized to access information systems that contain Outpayce Data. Where Personnel have access to Outpayce information systems, Partner will notify Outpayce of any changes in job function. Individual Personnel must have separate identifiers or logins, and the Partner must deactivate authentication credentials that have been inactive for a period not exceeding six months.

(c) Traceability. The activity through user accounts must be traceable and attributable to a single person.

(d) Least privilege. Access to Outpayce Data is restricted to those individuals who are required to access the Outpayce Data to perform their job function on a need-to-know basis.

(e) Integrity and confidentiality. The Partner must implement system and application access controls.

(f) Authentication. The Partner must use industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication measures are based on passwords the passwords must be renewed regularly and meet industry standard password protection practices.

(g) Network design. The Partner must have controls in place to avoid access to Outpayce Data by individuals where they may not be authorized to access.

2.2.6 Physical and environmental security

(a) Physical access to facilities. The Partner must limit access to facilities where Outpayce Data is located or accessed from to identified authorized individuals.

(b) Physical access to components. The Partner maintains records of the incoming and outgoing media containing Outpayce Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain.

(c) Protection from disruption. The Partner must use industry standard systems to protect against loss of Outpayce Data due to power supply failure or other disruptions.

(d) Equipment disposal. The Partner must use industry standards to ensure Outpayce Data is securely deleted when it is no longer needed.

2.2.7 Communications and operations management

(a) Operational policy. The Partner must maintain documentation describing security measures, the relevant procedures and responsibilities of its Personnel who have access to Outpayce Data.

(b) Environment separation. The Partner must maintain separation of development, testing and production environments.

(c) Data Recovery procedures. The Partner must have in place data recovery procedures so that Outpayce Data can be recovered, including business continuity and disaster recovery plans consistent with industry standard practices for services where Outpayce Data is processed.

(d) Backup policies and procedures. The Partner will have backup policies and procedures in place that specify the scope of the data to be backed up and the minimum backup frequency, based on the nature of the information or the level of confidentiality of Outpayce Data. The Partner will conduct these backup, restoration and recovery tests periodically.

(e) Backup systems. The activation of backup systems will not jeopardize the security of the networks and information systems, nor the availability, authenticity, integrity, or confidentiality of the data.

(f) Independent controls. The information assets included in the backup will have defined controls to ensure that access is granted only when necessary. Additionally, the Partner will ensure that all media for backups related to the Contract, as well as the management and storage systems for such media, remain secure and reliable at all times.

(g) Restoration process. The Partner must ensure the restoration of all data and systems to their original encryption status. This obligation includes, but is not limited to, reinstating the original encryption keys, algorithms, and settings used to secure the data, ensuring no residual vulnerabilities or unauthorized changes remain.

(h) Malicious software. The Partner must maintain reasonable and up-to-date anti-malware, anti-spam, and similar controls on networks, systems and devices, including controls to help avoid malicious software gaining unauthorized access to Outpayce Data, such as malicious software originating from public networks. The Partner will establish and maintain up-to-date protection systems against malicious code/software, following Industry Best Practices.

(i) Encryption in transit. The Partner must encrypt Outpayce Data that is transmitted over public networks and media leaving its facilities using modern, industry accepted cryptographic controls and methods.

(j) Encryption at rest. The Partner must encrypt Outpayce Data that it stores within its facilities

using modern, industry accepted cryptographic controls and methods. The Partner will review and evaluate the cryptographic technology and encryption algorithms it uses to ensure they remain appropriate and up to date for their intended purpose. The characteristics of the applied encryption will align with risk tolerance, as it may have an operational or performance impact. Cryptographic implementations must comply with the defined requirements and algorithms.

(k) Monitoring and logging. The Partner access and use of information systems containing Outpayce Data, registering access ID, time, relevant authorizations and to promptly identify and analyze anomalous or unauthorized behaviors, and make these logs available to Customers for their analysis upon request. Additionally, the Partner must ensure the proper safeguarding and integrity of the activity logs of these users. To achieve this, a process for reviewing user access must be implemented periodically, at least once a year.

(l) Technical vulnerability management. The Partner will maintain a vulnerability management program, addressing vulnerabilities in a timely manner based on risk assessments.

(m) Denial of service detection. The Partner will implement and maintain capabilities to detect denial of service attacks and will ensure that external channels or channels connected to the internet that are used pursuant to this Contract have adequate protection against denial-of-service attacks, guaranteeing the availability criteria agreed with Outpayce.

(n) Endpoints security. The Partner will reinforce the devices used to access Outpayce 's network or process Outpayce Data, in order to protect them against external attacks.

2.2.8 Partner management

(a) The Partner must only use third party providers who provide sufficient guarantees to implement appropriate technical and organizational measures that are equivalent to these security standards.

(b) The Partner must have appropriate contractual safeguards in place with its third-party suppliers and will carry out adequate due diligence of such third-party suppliers and retain oversight of and be responsible for the third-party suppliers' acts of omissions in connection with the provision of the services.

(c) The Partner must ensure that subcontractors comply with the Digital Operational Resilience Act.

2.2.9 Information Security Incident management

(a) Security Incident response process. The Partner must have a Security Incident (as defined below) response plan that includes procedures to be followed to identify, remediate and report any security breach. The plan must be regularly tested and have procedures to notify impacted stakeholders, relevant regulators and, in the case of personal data, individuals.

(b) Remediation plan. The Partner must share with Outpayce a remediation plan (action, person responsible and delivery date) with corrective measures in case of Security Incident.

(c) Investigation policy. The Partner must investigate all Security Incidents to identify root causes and resolve/mitigate future Security Incident with the same root cause (including employee training).

(d) Detection infrastructure. The Partner must have an IT infrastructure detect potential Security Incidents.

(e) Incident identification and recording. The Partner must identify, classify and register all Security Incidents. The Partner will centralize the records, protect them appropriately and retain them for at least five (5) years.

(f) Notification of Security Incidents. The Partner must report to Outpayce any Security Incident immediately, and in no event later than twenty-four (24) hours from the occurrence of the Security Incident. The Partner must keep Outpayce updated about the progress of the corrective measures implemented.

(g) Post-incident reporting. Within fifteen (15) calendar days after the restoration of the normal level of operation of the service, the Partner must provide a report including: (i) the root cause and other events relating to the Security Incident, (ii) the measures implemented by the Partner to mitigate/resolve the situation, (iii) the downtime of the systems, (iv) if the Security Incident was material enough to notify third parties, and (v) the measures implemented by the Partner to prevent such Security Incidents.

(h) Investigation and cooperation in case of Security Incidents. In the event of a Security Incident, the Partner must promptly take reasonable steps to contain, investigate and mitigate any Security Incident. Any logs determined to be relevant to the Security Incident must be preserved to assist in the investigation.

(i) Timely information. The Partner must provide timely information about the Security Incident to the extent known to the Partner, including but not limited to the nature and consequences of the Security Incident, the measures taken and/or proposed by the Partner to mitigate or contain the Security Incident, the status of the investigation and a contact point from which additional information may be obtained.

2.2.10 Service organization controls ("**SOC**")

(a) SOC reports. The Partner must be covered by a SOC1 and SOC2 Type II report, or equivalent, during the term of the Agreement, which demonstrates the effectiveness of the implementation of controls delegated/outsourced to the Partner, if applicable. The Partner must provide a copy of the most recent report on an annual basis. This report must be provided within fifteen (15) calendar days upon Outpayce's request.

(b) SOC audit. If the Partner is not covered by such a report covering the relevant controls, then the Partner must provide evidence of the effective implementation of the delegated/outsourced controls as part of the annual Amadeus and/or Outpayce SOC audit, during the term of the Agreement. This information must be provided within fifteen (15) calendar days upon Outpayce's request.

2.2.11 Business continuity

(a) Management. The Partner must establish and maintain security processes for the required level of business continuity during an adverse situation that applies to the Personnel and facilities in which the Partner processes Outpayce Data. The Partner must verify the Security Requirements at regular intervals to ensure that they are valid.

(b) Recovery of data. The Partner must have in place data recovery procedures so that customer data can be recovered, including business continuity and disaster recovery plans consistent with industry standard practices for services where customer data is processed.

(c) Good practices. The Partner must follow good business continuity practices, maintaining processes, procedures and controls in order to minimize the risks and avoid the interruption of the business activity during an adverse situation. These procedures and measures will be periodically reviewed.

(d) Recovery. In the event of failure, interruption or unavailability, Partner undertakes to recover the affected Partner's service regardless of the agent that causes it, as soon as feasible, and in no event later than twenty-four (24) hours after the relevant incident. In the event that the services provided by the Partner are of a technological nature and/or processes Outpayce Data, the Partner undertakes to carry out the corresponding backups on a regular basis.

(e) Performance of recovery actions. The performance of the recovery actions of the affected Partner's services which the Partner undertakes to take in accordance with the provisions of this section must not entail any additional cost for Outpayce.

(f) Evidence. The Partner will make available to Outpayce, upon request, evidence of its compliance with the business continuity requirements set forth in this section.

(g) Business continuity plans. The Partner must have business continuity plans for each of the Partner's services outlined under the Contract. These plans must be activated to maintain the continuity of each of the Partner's services within the established terms, as well as in those cases in which any event occurs that could affect the provision of the relevant Partner's service.

In the event that the Partner does not have the plans referred to in the preceding paragraph for each of the Partner's services or they do not meet the requirements outlined in the Contract or, as the case may be, those previously conveyed by Outpayce to the Partner, the Partner must develop them within a maximum period of six (6) months from the date of signature of the Contract.

(h) Test. In order to guarantee the effectiveness of the plans in case of activation, these plans will be subject to maintenance and testing on an annual basis and in any case after significant business, organizational and/or technical changes. The plans must include the execution of regular tests with a minimum periodicity of one (1) year, guaranteeing, in any case, the security of the information. The participation and execution of the tests must be coordinated, including all the parties involved during their development. The execution of these periodic tests will not entail any additional cost for Outpayce.

The execution of the tests of the plans will not, under any circumstances, imply a decrease in the availability of the relevant Service, which must be adjusted to the agreed service levels. In the event of affecting the established service levels, this circumstance must be previously agreed with the areas involved.

In any case, the Partner undertakes to provide Outpayce with the document of the results of the tests carried out, for the Partner's services contained in the Contract. Namely, the Partner must provide Outpayce with certified evidence approved by Partner's management or by a trusted third party (e.g. certification body or reputable auditor) of the tests carried out (i.e. scope, simulated scenario and results), so that Outpayce can verify the effectiveness of the measures and procedures developed for the recovery of the Partner's services.

Additionally, the Partner commits to participate in any test required by Outpayce within its own periodic verification plans of the business continuity plans.

(i) Monitoring. The Partner must have solutions in place to monitor the relevant Partner's service in terms of availability and continuity and an incident response plan that allows Outpayce to be immediately notified of: (a) any interruption of the Partner's services and/or total or partial activation of each business continuity plan; (b) the expected impact on the Partner's services; (c) the corresponding deactivation of the plan, (d) the actual impact that has occurred and (e) the Incident closure report including the actions taken and the action plans identified within a period not exceeding fifteen (15) calendar days from the Security Incident.

(j) Back-up copies. In any case, the Partner undertakes to store backup copies of everything that may affect the availability of the Services (i.e. data and software) in a different location from the production systems. The Partner must have physical protection solutions and control procedures in place to safeguard its ICT infrastructure (e.g. data processing center) from environmental risks (e.g. floods and other natural disasters) as well as to ensure a suitable operating environment for the ICT systems (e.g. air conditioning systems). Likewise, the Partner must have protection and redundancy measures in place to protect the systems from power failures.

(k) Crisis management plan. The Partner must have a crisis management plan for the Partner's services, which must be subject to annual maintenance and testing.

The Partner must audit the plans at least once (1) a year, guaranteeing, in any case, the security of the information. Outpayce may request the reports resulting from such audits at any time. Otherwise, the Partner must authorize Outpayce and its agents to verify the suitability of the plans as well as the crisis management plan and their compliance with the requirements expressed in this Clause, undertaking to provide, provided that there is no conflict of interest between the Partner and the agents acting on behalf of Outpayce, direct and unrestricted access to the premises, equipment, documentation and/or information required for the aforementioned purposes, respecting, in all cases, the security protocols established in the affected facilities.

(l) Incident resolution certificate. Outpayce reserves the right to require the Partner to provide an incident resolution certificate from an independent third party.

(m) Change of environment. The Partner must immediately inform Outpayce of any change in the environment of the Partner that affects the business or the order.

2.2.12 Service design resilience requirements

(a) Outpayce will identify the need for resilience of services and the Partner will ensure that all services are designed to meet the relevant recovery time objectives.

(b) The Partner will evaluate and validate the service components every twelve (12) months to demonstrate that the services meet the resilience requirements set out by Outpayce.

(c) If any component fails to meet the applicable resilience requirements, the Partner will immediately notify Outpayce and provide detailed remediation plans (including actions to be taken and corresponding completion dates).

2.2.13 Monitoring and evidence compliance with the security standards

(a) Self-assessment. The Partner will continually monitor the security processes it has in place to comply with the Contract and will periodically assess the effectiveness of the security processes and update them as needed.

(b) Security assessment. Upon Outpayce's written request, Partner will promptly and accurately complete security questionnaires regarding any network, application, or systems applicable to the processing of Outpayce Data.

(c) Partner's services. The Partner will provide any additional assistance and cooperation that may reasonably be required during any security assessment. Except in case of Security Incidents, Outpayce can request the assessment only once per calendar year.

(d) Evidence of compliance with the Security Requirements. Upon Outpayce's written request, the Partner will evidence compliance with the security standards. The Partner will provide where applicable, certification, audit reports or other reports relevant to demonstrate such compliance with the services provided under the Contract. Examples of acceptable reports include but are not limited to: (a) SOC 2 Type II (based on Trusted Service Principles TSP 100); (b) SOC 1 Type II (based on SSAE 18); (c) ISO/IEC 27001 certification; and (d) PCI DSS Attestation of Compliance.

(e) Audit. The Partner must allow Outpayce upon request but no more than once per calendar year (other than in the event of a Security Incident) the right to audit the Partner on an ad-hoc basis to demonstrate compliance with these security standards. The audit may be conducted by a third-party auditor selected by Outpayce. Outpayce will notify Partner at least thirty (30) calendar days in advance. The audit will take place during normal business hours of Partner, and the auditor will not unreasonably interfere with Partner's operations during the course of

the audit. Outpayce will ensure that the auditor will be subject to confidentiality obligations sufficient to cover the auditor's engagement with the Partner for the audit.

(f) Networking scanning. Outpayce can perform network tests, such as (i) services discovery scans, (ii) vulnerability detection scans and (iii) penetration tests or vulnerabilities exploitation tests.

## 3. Matrix of responsibilities

3.1 Split of responsibilities. Pursuant to article 12.8.5 of the PCI-DSS 4, the table below reflects the PCI DSS requirements that are managed by the Partner and the requirements managed by Outpayce.

| PCI DSS Requirements | | Partner | Shared Responsibility | Outpayce |
|---|---|---|---|---|
| **Build and Maintain a Secure Network and Systems** | **1. Install and Maintain Network Security Controls.** | Accountable for the network under Partner control | YES | Accountable for the network under Outpayce control |
| | **2. Apply Secure Configurations to All System Components** | Accountable for the network under Partner control | YES | Accountable for the network under Outpayce control |
| **Protect Account Data** | **3. Protect Stored Account Data.** | Accountable for control of stored data, including Partner third parties. | YES | Outpayce stored cardholder data only |
| | **4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.** | Partner to implement secured connection<br>(c.f. to applicable PCI standard) | YES | Accepts only secured connection & protocols (c.f. to applicable PCI standard) |
| **Maintain a Vulnerability Management Program** | **5. Protect All Systems and Networks from Malicious Software** | Accountable for devices under Partner control | YES | Accountable for devices under Outpayce control |
| | **6. Develop and Maintain Secure Systems and Software** | Securely developed systems and applications | YES | Accountable for systems and applications under Outpayce control |
| **Implement Strong Access Control Measures** | **7. Restrict Access to System Components and Cardholder Data by Business Need to Know** | Accountable for granting access to Partner Personnel | YES | Accountable for granting access to Outpayce personnel |
| | **8. Identify Users and Authenticate Access to System Components.** | Accountable for granting access to Partner Personnel | YES | Accountable for granting access to Outpayce personnel |
| | **9. Restrict Physical Access to Cardholder Data** | 9.2.4, 9.3, 9.3.1, 9.3.2 – Accountable for premises under Partner control | YES | 9.2.4, 9.3, 9.3.1, 9.3.2 – Accountable for premises under Outpayce control |
| | | 9.4.1, 9.4.2, 9.4.5, 9.4.6– Accountable | Case by case, (Authorization type is PSP accountability) | 9.4.1, 9.4.2, 9.4.5, 9.4.6 Accountable for systems and applications under Outpayce control |

| PCI DSS Requirements | | Partner | Shared Responsibility | Outpayce |
|---|---|---|---|---|
| | | 9.5.1 – POS security | To be reviewed case by case | 9.5.1 – POS security |
| | | 9.1.1– Physical access policies<br><br>Partner Ops procedures | YES | 9.1.1 – Accountable for systems and applications under Outpayce control |
| **Regularly Monitor and Test Networks** | **10. Log and Monitor All Access to System Components and Cardholder Data.** | Accountable | YES | Accountable for systems and applications under Outpayce control |
| | **11. Test Security of Systems and Networks Regularly.** | Accountable | YES | Accountable for systems and applications under Outpayce control |
| **Maintain an Information Security Policy** | **12. Support Information Security with Organizational Policies and Programs.** | Accountable to the Partner as a service provider | YES | Outpayce policies only |

***