1. General

1.1 Both Parties will maintain standard environmental, safety and facility procedures, data security and back-up procedures and other safeguards, in accordance with generally accepted industry standards, against the destruction, loss, unauthorized access or alteration of: (a) with respect to Outpayce, Outpayce Data; or (b) with respect to Customer, Customer Data.

1.2 Both Parties will implement robust security measures that meet the requirements set out by PCI/DSS, international best practice standards and applicable Data Protection Legislation. This includes access controls, data encryption, security monitoring, vulnerability management and other recommended security practices.

2. Security

2.1 Customer acknowledges and agrees that the environment in which the Payment Solutions are used must be secure. Accordingly, Customer must (and must ensure that any Customer Selected Provider or other third party providing information technology services on its behalf will):

2.1.1 Implement and maintain active firewalls to limit and control incoming and outgoing traffic on Customer's client computer systems.

2.1.2 Implement secure encryption protocols, such as HTTPS protocol for accessing websites and VPN (virtual private network) protocol for establishing secure connections over public networks.

2.1.3 Use digital certificates to authenticate the identity of servers and ensure the security of encrypted communications.

2.1.4 Implement and maintain active and regularly updated anti-virus and anti-malware tools on all computers.

2.1.5 Only use still supported, up-to-date and patched versions of application software, operating systems and infrastructure components, with all security updates applied as soon as possible.

2.1.6 Use strong passwords with no sharing of access credentials between several individuals or reuse of the same password in multiple products or tools, meaning Customer must use unique passwords for each Solution, including their work e-mail account.

2.1.7 Conduct awareness sessions for its individuals on how to recognize and prevent phishing attempts. In no event will Outpayce be liable for any loss or damage to Customer resulting from or relating to Cyber-Crime affecting the Outpayce Payment Platform, networks or the internet, illegal hacking, (distributed) denial of service attacks, unauthorised access to or interference with data, identity theft, phishing, software and media piracy, website vandalism, release of viruses and worms, invasion of privacy and cyber-spying.

2.1.8 Implement good security practices such as access controls, secure working procedures, continuity of operations and safeguards, and conduct periodic audits to prove good standing on security measures.

3. Credentials and access/unauthorized access

3.1 The security and use of Customer's login credentials, access keys and passwords to the Solution(s) are Customer's sole responsibility. Customer will implement and maintain appropriate administrative procedures to ensure that such access credentials are accessible only to Customer's individuals. Customer will employ all physical, administrative and technical controls, screening and security procedures and other safeguards necessary to securely administer the distribution and use of all access credentials and prevent any unauthorised access to, or use of, the Payment Solutions and Outpayce Payment Platform and, in the event of any such unauthorised access or use, promptly notify Outpayce. Customer will not interfere with, disrupt, or cause any damage to other users of the Outpayce Payment Platform or Payment Solutions.

4. PCI DSS

4.1 Outpayce and Customer are each responsible for the security of cardholder data that are stored or processed on or transmitted through their respective systems and agree to collaborate to maintain such security to enable Outpayce and its Affiliates to certify annually to the Payment Card Industry Data Security Standards, as published and mandated by the PCI Security Standards Council at the time of certification, with respect to the storage, transmission or processing of cardholder data.

5. Responsibility Matrix

5.1 The Parties agree to comply with the PCI DSS responsibility matrix set out below:

PCI DSS Requirements (v. 4.0)		Customer	Shared Responsibility	Outpayce
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls.	Accountable for the network under Customer control	YES	Accountable for the network under Outpayce control
	2. Apply Secure Configurations to All System Components	Accountable for the network under Customer control	YES	Accountable for the network under Outpayce control
Protect Account Data	**3.** Protect Stored Account Data.	Accountable for control of stored data, including Customer third parties.	YES	Outpayce stored cardholder data only
	4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.	Customer to implement secured connection. (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 Customer 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 Customer Personnel	YES	Accountable for granting access to Outpayce personnel
	8. Identify Users and Authenticate Access to System Components.	Accountable for granting access to Customer 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 Customer 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
		9.5.1 – POS security	To be reviewed case by case	9.5.1 – POS security
		9.1.1– Physical access policies Customer 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

PCI DSS Requirements (v. 4.0)		Customer	Shared Responsibility	Outpayce
	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 Customer as a service provider	YES	Outpayce policies only

6. Immediate notice

6.1 Each Party must notify the other Party immediately if it learns or suspects that a potential unauthorized use or access to card data has occurred, providing good faith cooperation to resolve the incident.

7. Prohibited Activities

7.1 Customer will not:

7.1.1 Directly, indirectly, manually or through robotic devices access or use (or allow any third party to access or use) the Payment Solutions for: (a) making transactions which are speculative, fictitious, duplicative, improper or fraudulent, or made solely to achieve minimum targets, minimum usage requirements or to otherwise obtain improper economic advantages; (b) engaging in any unethical or illegal activities; (c) whether knowingly or not, transmitting or disseminating any virus, trojan or other malicious, harmful or disabling data, work, code or program; or (d) interfering with, disrupting or attempting to gain unauthorised access to any computer, system or network.

7.1.2 Licence, transfer, assign, distribute, display, disclose or otherwise make any Payment Solutions available to any third party except as expressly permitted under this Agreement.

7.1.3 Access Outpayce Payment Platform or any Payment Solutions via third party products (e.g., robotic tools) that are not expressly authorized by Outpayce in writing; use any automatic device, software, application, program, browser plugins, algorithm, whether integrated in a browser or otherwise, or methodology having similar processes or functionality, or any manual process, to monitor, perform any transactions, frame, modify, add content or copy any part of the Payment Solutions.

7.1.4 Access all or any part of the Outpayce Payment Platform or Payment Solutions in order to build a product or service which competes with the Outpayce Payment Platform or any Payment Solution.

***