IBM Payments Gateway

This Service Description describes the Cloud Service IBM provides to Client. Client means and includes the company, its authorized users or recipients of the Cloud Service.

1. Cloud Service

The Cloud Service offering provided by IBM is described below. The applicable Quotation and Proof of Entitlement (PoE) are provided as separate Transaction Documents.

IBM Payments Gateway

IBM Payments Gateway provides connectivity with development, pre-production, and production environments. Functionality includes the following:

- Payment Card Industry (PCI) vault, a storage facility designed to provide security for sensitive payment information
- Payment gateway that performs routing, switching, and processing of payment transactions with third-party processors
- Virtual terminal which is a web tool designed for payment collection in call centers, credit management, and back-office payment operations
- Authentication designed with security features
- Fraud prevention tools
- Report generation capabilities
- Documentation

1.1 Additional Services

Client must purchase IBM Payments Gateway along with at least one (1) of the following Cloud Service Payment offerings:

a. IBM Payments Gateway API Payment

Functionality includes:

- Transactions are transmitted through an API that consists of a set of web services designed to facilitate integration with client systems. The API provides a single interface to global payments across banks and processors in a large number of countries and currencies.

b. IBM Payments Gateway Hosted-Page Payment

Functionality includes:

- Transactions are transmitted through the Hosted Payment Page (HPP), a payment collection and wallet management GUI that is designed to be integrated into websites, mobile commerce sites, Smart Phone apps, call center applications, and back-office collection systems. The Hosted Payment Page is designed to be delivered in an HMTL inline frame (iframe).

c. IBM Payments Gateway Advanced API Payment

Functionality includes:

- Transactions are transmitted through the JavaScript Object Notation (JSON) interface which is designed to facilitate development of payment functions in native smart phone applications.
- The JSON interface offers a set of payment APIs that are performed using HTTP methods on the related URL, with data delivered in the JSON format.

The following IBM Payments Gateway offering may be optionally purchased:

d. IBM Payments Gateway Settlement

Functionality includes:

- Transactions are transmitted from a seller to a buyer's financial institution that contain payment information to enable transaction settlement to be completed.

2. Security Description

2.1 Security Policies

IBM has an information security team and maintains privacy and security policies that are communicated to IBM employees. IBM requires annual privacy and security training for personnel. IBM security policies are revalidated annually based on industry practices and IBM business requirements. Security incidents are handled based on comprehensive incident response procedures. IBM maintains physical security standards designed to limit access to authorized personnel at IBM data centers, including limited and monitored access points. Visitors register upon entering and are escorted while on the premises.

2.2 Access Control

IBM authorized staff use two–factor authentication to an intermediate “gateway” management host. IP Blocking may be utilized to prevent access by known compromised Internet sites and users in U.S. embargoed countries. Access to Client data and transfer of data in or out of the hosting environment is logged. WIFI use is prohibited within the IBM data centers that support this Cloud Service.

The Cloud Service requires encryption of content during data transmission between the IBM network and Client's network access point. The specific encryption methods are specified by contractual agreement with the Client, and the encryption requires installation of SSL certificates at both IBM and Client's sites. Only personal information that is required for the payment processing is collected. The Cloud Service does encrypt that content when at rest awaiting data transmission.

2.3 Service Integrity and Availability

Modifications to operating systems, application software, and firewall rules are handled under IBM’s change management process. Changes to firewall rules are reviewed by the IBM security staff before implementation. IBM monitors the data center 24x7. Internal and external vulnerability scanning is conducted regularly by authorized administrators and third party vendors to help detect and resolve potential system security exposures. Malware detection systems (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) are used in all IBM data centers. IBM’s data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

2.4 Activity Logging

IBM maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time at central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to detect anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

2.5 Compliance

IBM performs industry standard ISAE3402 audits (or their equivalent) annually in production IBM Payments Gateway data centers for compliance with IBM information security policies. IBM's annual PCI DSS certification includes on site audits by external Qualified Security Assessor (Trustwave) in all IBM Payments Gateway data centers. The Attestation of Compliance (AoC) or Compliance Letter is available to Client and its auditors upon request.

2.6 Statement of Security Practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, or misappropriated or can result in misuse of your systems to attack others. Without a comprehensive approach to security, no IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

2.7 Data Privacy

IBM and Client are each responsible for complying with their respective obligations under the applicable data protection laws governing the personal data (as defined in the applicable data protection laws) that is stored or processed by IBM for Client under this Agreement ("Client Data"). By executing this Agreement, Client appoints IBM as a data Processor of Client Data. Client remains solely responsible for determining the purposes and means of IBM's processing of Client Data under this Agreement, including that such processing in accordance with Client's instructions will not place IBM in breach of the applicable data protection laws. IBM and Client each acknowledge that it is not investigating the steps the other is taking to comply with applicable data protection laws. Nothing in this Agreement prevents IBM or Client from taking the steps it deems necessary to comply with applicable data protection laws. If Client requests additional or different services to comply with the applicable data protection laws, such services shall be requested by using the Change Control Process described in Appendix C and using the Change Authorization for attached as Appendix E. Client acknowledges it is solely responsible for determining that the security measures specified in this Agreement constitute appropriate technical and organizational measures to protect Client Data as required by the applicable data protection laws. IBM is not required to perform or adhere to any security measures concerning Client Data other than those specified in this Agreement and as a Processor of Client Data; IBM will process Client Data as specified in this Agreement, and as IBM reasonably considers necessary or appropriate to perform the Services. Client is solely responsible for determining that any transfer by IBM or Client of Client Data across a country border under this Agreement complies with the applicable data protection laws.

3. Service Level Agreement

IBM provides the following service level agreement ("SLA") for the Cloud Service as specified in the Transaction Document. The SLA is not a warranty.

3.1 Definitions

a. "Service Credit" means the compensation IBM will provide for a validated Claim. The Service Credit will be applied in the form of a credit against a future invoice for the Cloud Service if acquired directly from IBM. If the Cloud Service is acquired from an IBM Business Partner, then IBM will make a rebate directly available to Client.

b. "Claim" means a claim Client submits to IBM that a service level has not been met during a Contracted Month.

c. "Contracted Month" means each full calendar month during the Cloud Service term measured from 12:00 a.m. Eastern US time on the first day of the month through 11:59 p.m. Eastern US time on the last day of the month.

d. "Downtime" means a period of time during which production system processing for the Cloud Service for which Client is entitled to use is not available. Downtime does not include the period of time when the Cloud Service is not available because of:

   (1) a scheduled or announced maintenance outage;

   (2) Events or causes beyond IBM's control (e.g., natural disaster, internet outages, emergency maintenance, etc.);

   (3) problems with content, equipment, or applications Client uses with the Cloud Service or any third party software, hardware, or other technology;

   (4) Client's failure to adhere to required system configurations and supported platforms or Client system administration, commands, or programming errors;

   (5) Client's caused security breach or any security testing performed by Client; or

   (6) IBM's compliance with any designs, specifications, or instructions that Client provides to IBM or a third party provides to IBM on Client's behalf.

e. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a service level.

f. "Response Time" means the time that elapses from the moment the CheckoutStartSession and/or CardAuthorize Web Services receive a request at the entry point to IBM's systems until IBM's web service response is sent back to the Client.

3.2 Service Credits

To submit a Claim, Client must log a Severity 1 support ticket (as defined below in the Technical Support section) for each Event with the IBM technical support help desk within 24 hours of first becoming aware that the Event has impacted use of the Cloud Service. Client must provide all necessary information about the Event and reasonably assist IBM with the diagnosis and resolution.

A Claim for a Service Credit must be submitted within three business days after the end of the Contracted Month in which the Claim arose.

IBM will measure internally total combined Downtime during each Contracted Month applicable to the corresponding service levels shown on the tables below. Credits will be based on the duration of the Downtime measured from the time you report that you were first impacted by the Downtime.

a. If Client reports Events of Web Services, Hosted Payment Page and Virtual Terminal Downtime occurring simultaneously, IBM will treat the overlapping periods of Downtime as a single period of Downtime, and not as two separate periods of Downtime.

b. If Client reports Events of CheckoutStartSession and CardAuthorize Web Services Response Time Downtime occurring simultaneously, then IBM will treat the overlapping periods of Response Time Downtime as a single period of Response Time Downtime, and not as two separate periods of Response Time Downtime.

For each valid Claim, IBM will apply the highest applicable Service Credit based on the achieved service level during each Contracted Month, as shown on the tables below. IBM will not be liable for multiple Credits for the same Event(s) in the same Contracted Month.

If the Cloud Service was acquired from an IBM Business Partner, the Service Credit will be calculated on the monthly subscription fee for the then-current list price for the Cloud Service in effect for the Contracted Month which is the subject of a Claim, discounted at a rate of 50%.

The total Service Credits awarded with respect to any Contracted Month cannot exceed 10 percent or one twelfth (1/12th) of the annual charge for the Cloud Service.

3.3 Service Levels

IBM's Web Services, Hosted Payment Page and Virtual Terminal interfaces will be available to the Client at least 99.95% of the time during a Contracted Month.

Availability Percentage (during a Contracted Month)	Service Credit (% of Monthly Subscription Fee for Contracted Month that is the subject of a Claim)
< 99.95%	2%
< 99.80%	4%
< 99.60%	6%
< 99.30%	8%
< 99.00%	10%

Availability, expressed as a percentage, is calculated as: the total number of minutes in a Contracted Month that IBM's Web Services, Hosted Payment Page and Virtual Terminal are available and responding to Client's requests divided by the total number of minutes in a Contracted Month multiplied by 100.

3.4 IBM Web Service Response Time during a Contracted Month

IBM offers two Response Time SLAs as follows:

3.4.1 Median IBM Web Service Response Time

The median IBM Response Time for CheckoutStartSession and CardAuthorize Web Services will be less than 100 milliseconds.

The IBM Response Time for a given Web Service, is measured as the elapsed time from when the Web Service request is received at the entry point to IBM's system, until IBM's web service response is sent back to the Client, minus any time IBM's system has spent waiting for responses from downstream Third Party Processors.

The service level target is calculated as the median IBM Response Time for CheckoutStartSession and CardAuthorize Web Services respectively, across all such Web Service requests in a given Contracted Month.

Median Response Time (during a Contracted Month)	Service Credit (% of Monthly Subscription Fee for Contracted Month that is the subject of a Claim)
> 100 ms	2%
> 500 ms	6%
> 1 second	10%

3.4.2 99% IBM Web Service Response Time

99% of CheckoutStartSession and CardAuthorize Web Services will have an IBM response time of less than 1 second.

The IBM Response Time is calculated the same as defined above for the Median IBM Web Service Response Time.

The service level target is calculated as the 99 percentile IBM Response Time for CheckoutStartSession and CardAuthorize Web Services respectively, across all such Web Service requests in a given calendar month.

99% Response Time (during a Contracted Month)	Service Credit (% of Monthly Subscription Fee for Contracted Month that is the subject of a Claim)
> 1 second	2%
> 5 seconds	6%
> 10 seconds	10%

3.5 Other Information about this SLA

This SLA is available to the Client company and does not apply to claims made by a user of the Cloud Service or for any beta or trial services. The SLA only applies to the Cloud Services in productive use. It does not apply to non-production environments, including but not limited to test, disaster recovery, quality assurance, or development. IBM will not process Claims for Response Time Service Credit when an availability service level outage has been recorded for the same period of time .

4. Service Level Objectives

The following service level objectives are a goal and do not constitute a warranty to Client. There is no refund, credit, or remedy available to Client in the event IBM does not meet the service level objectives.

Service	Objective
Batch Processing Turn-Around-Time	90% of all transaction batches will be processed to completion in less than 60 minutes from receipt
E-Mail Responsiveness	95% of e-mail sent to IBM's shared support mailbox will be answered within 24 business hours
24x7 Help Desk Call Answer Response Tim4e	IBM's 24x7 Help Desk will answer phone calls in less than 60 seconds
Security Management	● IBM's PCI-DSS Level 1 Certification will be renewed at least once per annum ● IBM will remediate High severity security vulnerabilities within 10 days ● IBM will remediate Low severity security vulnerabilities within 30 days
Pre-Production system availability	● Available for client testing 24x7 ● Pre-Production system is unattended ouside normal Central European work hours ● Pre-Produciton system incidents will, by default, be handled as severity 3

5. Technical Support

Technical support for the Cloud Service is provided via email and telephone. Any enhancements, updates, and other materials provided by IBM as part of any such technical support are considered to be part of the Cloud Service and therefore governed by this Service Description. Technical support is included with the Cloud Service and is not available as a separate offering.

More information about hours of availability, email addresses, online problem reporting systems, and other technical support communication vehicles and processes are described in the IBM Software as a Service Support Handbook.

Severity	Severity Definition	Response Time Objectives	Response Time Coverage
1	Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.	Notification of Client within 15 minutes.	24x7
2	Significant business impact: A service feature or function is severely restricted in its use or Client is in jeopardy of missing business deadlines.	Notification of Client within 15 minutes.	M-F local business hours
3	Minor business impact: Indicates the service or functionality is usable and it is not presenting a critical impact on operations.	No notification required	M-F local business hours
4	Minimal business impact: An inquiry or non-technical request.	No notification required	M-F local business hours

6. Entitlement and Billing Information

6.1 Charge Metrics

The Cloud Service is available under the charge metric specified in the Transaction Document:

a. Instance is a unit of measure by which the Cloud Service can be obtained. An Instance is access to a specific configuration of the Cloud Service. Sufficient entitlements must be obtained for each Instance of the Cloud Service made available to access and use during the measurement period specified in Client's Proof of Entitlement (PoE) or Transaction Document.

b. Thousand Events is a unit of measure by which the Cloud Service can be obtained. Thousand Events entitlements are based on the number of occurrences of a specific event related to the use of the Cloud Service, measured in packs of one thousand. Thousand Events entitlements are specific to the Cloud Service and the type of event may not be exchanged, interchanged, or aggregated with other Thousand Events entitlements of another Cloud Service or type of event. Sufficient entitlements must be obtained to cover every event that occurs during the measurement period specified in a Proof of Entitlement (PoE) or Transaction Document.

c. For this Cloud Service, an Event is defined as a Master Transaction, counted in packs of one thousand. A Master Transaction is a set of instructions initiated from an application external to the program (for example, business banking web channel or manual message entry channel) or triggered by an event in the program (for example, recurring payment or time of day to start bulk processing). The Master Transaction manages the related business activity and logical unit of work including all updates and events associated with the various processing steps and ending when the final instruction is sent to an external application or the processing lifecycle is complete. A Master Transaction will initiate underlying transactions during its processing lifecycle.

6.2 Partial Month Charges

A partial month charge as specified in the Transaction Document may be assessed on a pro-rated basis.

6.3 Overage Charges

If actual usage of the Cloud Service during the measurement period exceeds the entitlement specified in the PoE, Client will be charged for the overage as specified in the Transaction Document.

7. Term and Renewal Options

7.1 Term

The term of the Cloud Service begins on the date IBM notifies Client of their access to the Cloud Service, as documented in the PoE. Client may increase their level of use of the Cloud Service during the term by contacting IBM or their IBM Business Partner, and the increase will be confirmed in a Transaction Document.

7.2 Term Renewal Options

The Transaction Document will specify which of the following applies to renewal of the Cloud Service term.

7.2.1 Automatic Renewal

Where renewal is automatic, the Cloud Service will automatically renew for a term specified in the Transaction Document (either a one year term or the same duration as the expiring term) unless Client has provided written termination at least 90 days prior to the term expiration date.

7.2.2 Continuous Billing

Where billing is continuous, Client will continue to have access to the Cloud Service following the end of the term and will be billed for usage on a continuous basis. To discontinue use of the Cloud Service and stop the continuous billing process, Client must provide 90 days written notice of cancellation. Client will be billed for any outstanding access charges through the end of the month of cancellation.

7.2.3 Renewal Required

Where the renewal type is specified as “terminate”, the Cloud Service will terminate at the end of the term and Client access will end. To continue use of the Cloud Service beyond the term end date, Client must order a new subscription term.

8. General

Where applicable, taxes are based upon the location(s) receiving the benefit of the Cloud Service. IBM will apply taxes based upon the business address listed in Client’s order unless Client provides additional information to IBM. Client is responsible for keeping such information current and providing any changes to IBM.