BigPanda

End User License Agreement

This End User License Agreement (the "Agreement") establishes the terms for the provision of an Enterprise SaaS Service (the "Service") to an End User who purchases via a Partner of the Provider. Entering into this Agreement does not, in itself, obligate the parties to provide or purchase the Service, but its terms will be applied to the ordering documents that establish such an obligation (each, an "Order").

The Service

The Elements of the Service

Enterprise SaaS. The Service is offered under a software-as-a-service model. Under this model, the core features and functionality provided by the Service are provided – not as software that is licensed to the End User and then either installed within the End User's IT environment (on-premise software model) or installed on the End User's behalf on the Provider's managed servers (an application service provider model) – but rather as a cloud-based site at which the End User accesses the features and functionality provided by the Service (the "SaaS").

Installed Access Points. The Service also includes software code (such as browser extensions or application plug-ins) that is installed within the End User's IT environment in support of the transfer of data between the End User's IT environment and the SaaS (an "Installed Access Point").

Performance of the Service

Documentation

Service documentation is provided as an online resource, available at docs.bigpanda.io (the "Documentation").

Performance Generally

General Performance Standard. For the full term of the End User's Order, the Service will perform as described in the Documentation (the "General Performance Standard").

Process and Remedy for Failure of the General Performance Standard. If the Service fails to meet the General Performance Standard, the End User may seek a remedy by providing a reasonably detailed notice of the failure, after which the Provider will have 30 days to correct the failure. If the Provider cannot do so, then the End User may terminate any or all Orders for the Service immediately upon notice and receive a prorated refund for its prepaid but unused fees, measured from the date of the failure notice.

Disclaimer of the UCC and Implied Warranties. The Parties agree that this Agreement is not a contract for the sale of goods, as those terms are defined under the Uniform Commercial Code, and that their intent is for the Uniform Commercial Code to not apply to this Agreement and the course of action it contemplates. THE PROVIDER DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTY OF MERCHANTABILITY AND THE IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE.

Uptime and Issue Management

Uptime and Issue Management. The Provider's obligations regarding uptime and issue management are established in the Service Level Agreement, provided as an exhibit to this Agreement.

Professional Services

Professional Services. The Service is complemented by professional services, such as implementation, End User support, End User success, and consulting services. All professional services will be provided according to industry standards.

Security and Privacy Controls

Security and Privacy Controls. The Service will be designed and maintained according to the Service Security Standards, provided as an exhibit to this Agreement.

Business Continuity and Disaster Recovery

Continuity and Recovery Investments. The Provider will maintain business continuity and disaster recovery plans, infrastructure, and processes that conform to the industry standards for enterprise SaaS providers.

Force Majeure. A party's failure to perform will be excused for up to 30 days when directly caused by an intervening event of a magnitude or unpredictability that renders performance impractical despite that party's continuity and recovery investments. Fees owed for days in which the Service is unavailable due to a force majeure event will be credited to the End User's account.

Protection Against Unwanted Code and Licenses

Protection Against Unwanted Code and Licenses. The Service will not expose the End User to (i) malicious software code, such as code that is designed to secretly penetrate End User's IT infrastructure or to create vulnerabilities within that infrastructure that can be exploited for such purpose or (ii) licensing terms that would require the End User's technology to be disclosed or distributed to the public (such as "copyleft" open source licensing terms).

Use of the Service by the End User

Use of the Service by the End User. The End User will only access the Service through its Documented access points and will only use the Service for its Documented purpose and subject to the limits established in the Orders (such as limits on Service scope, user counts, duration, or volume).

Future Functionality

Future Functionality. The Provider may make future improvements to the Service, which may include creating new features that are outside of the scope of End User's Orders or sunsetting features that are within the scope of End User's Orders. The End User will receive, at no additional charge, all future features and functionality that are sold to new End Users as an element of the SKU purchased by the End User. If the Provider sunsets material features within the scope of End User's Orders, it will provide any successor features at no additional charge.

Term and Termination

Term

Term. This Agreement is effective as of the effective date of the first Order for the Service (the "Effective Date"). This Agreement will terminate naturally 30 days after the last day of the term set on the End User's Orders.

Termination for Breach of the Agreement

Termination for Breach of the Agreement. If a party breaches this Agreement, and if the breach is capable of being cured and is not a breach of the Intellectual Property, Confidentiality, or Use of the Service by the End User provisions, then the non-breaching party, prior to terminating for breach, will provide notice of breach and intended termination. If the breach is not cured within 30 days of the date of such notice, then the intended termination will become automatically and immediately effective.

Survival of Terms

Survival of Terms. If the term of an Order extends beyond the term of the Agreement, then the Agreement will remain in effect for the limited purpose of providing continuity of terms for that Order until the end of that Order's current term. Rights and obligations established under this Agreement that must survive termination in order to have their customarily intended effect (such as rights and obligations related to confidentiality, indemnification, limitation of liability and damages, and data and intellectual property) will so survive.

Data Ownership and Use

End User Data. All data that is either (i) transmitted to the Service by or on behalf of the End User or (ii) is added to a End User-facing dataset within the Service through the use of the Service by or on behalf of the End User (collectively, "End User Data") is and will remain the property of the End User.

Anonymized Data. End User Data that has been modified so as to be attributable neither to the End User nor to any personally identified individual ("Anonymized Data") is and will remain the property of the End User, but the Provider may retain and continue to use Anonymized Data after the termination of this Agreement.

Usage Data. Data generated by the Service as a record of its use, such as system logs, is and will remain the property of the Provider, and the Provider may retain and continue to use Usage Data after the termination of this Agreement.

Intellectual Property

The SaaS. The SaaS (including, for example, its algorithms, calculations, organization, look and feel, and the underlying software code) is and will remain the sole property of the Provider, and the Provider is and will remain the sole owner of all intellectual property embodied or practiced by the SaaS. The End User is hereby granted a non-exclusive, limited license to access the SaaS through its documented access points and to use its documented functionality, for the duration of the term and to the limits of the scope described in an Order.

Installed Access Points. The Installed Access Points are and will remain the sole property of the Provider, and the Provider is and will remain the sole owner of all intellectual property embodied or practiced by the Installed Access Points. The Provider grants the End User a non-exclusive, limited license to use, copy, prepare derivative works of, display, transmit, perform, and distribute the Installed Access Points as may be necessary for the End User to use their documented functionality, for the duration of the term and to the limits of the scope described in an Order.

Reports. Documents generated by the Service and made available for download by the End User through the Service (each, a "Report") may be retained and used by the End User for any purpose, subject to the End User's confidentiality commitments. The Provider grants the End User a non-exclusive, limited, perpetual license to (with regard to copyrights embodied by the Report) copy, prepare derivative works of, display, transmit, perform, and distribute the Report and (with regard to patents practiced through use of the Report) to use the Report, in all instances only as may be necessary for the End User to utilize the Report.

Feedback. Suggestions for improvements to any element of the Service that are provided by the End User will be provided without restriction and will not operate to grant the End User an ownership interest in any intellectual property embodied or practiced by the Service. If a conveyance of intellectual property rights (such as an assignment or license) is required to achieve this result, the End User will grant such a conveyance.

Reservation of Rights. Each party reserves all intellectual property rights not expressly granted in this Agreement.

Confidential Information

Relationship to NDA. If the Parties have previously executed a nondisclosure agreement, then the terms related to confidential information established in this Agreement will supersede that nondisclosure agreement as of the Effective Date.

General Definition of Confidential Information. "Confidential Information" is defined to include all information, regardless of the medium through which it is conveyed, that is provided by one party to the other in relation to this Agreement and that a reasonable industry participant would deem likely to be confidential.

Exclusions from Confidential Information. Confidential Information is defined to exclude all information that is or becomes public knowledge, other than when the receiving party knew or should have known that such information became public knowledge through the breach of a confidentiality obligation owed to the disclosing party.

Use and Protection of Confidential Information. A receiving party will use the Confidential Information of the disclosing party only as necessary to perform its obligations and exercise its rights under this Agreement and will use reasonable care to protect such Confidential Information. At the termination of this Agreement, or upon the disclosing party's request, the receiving party will destroy the disclosing party's Confidential Information that is then in its possession.

Legally Compelled Disclosure. If the receiving party reasonably anticipates that it will be legally required to disclose Confidential Information, it will use its best efforts: (i) to timely notify the disclosing party; (ii) to limit the disclosure, such as by seeking a protective order in relation to the Confidential Information disclosed.

Trade Secrets. The receiving party's obligation to maintain the confidentiality of the disclosing party's trade secrets will survive the termination of this Agreement, enduring until such time as the information no longer satisfies the requirements of a trade secret.

Disputes

Insurance

Insurance. Upon the End User's reasonable request, the Provider will deliver to the End User a copy of its current certificates of insurance. And the Provider will maintain insurance that is at least commensurate with the coverage described in such certificates.

Indemnification

Definition of Indemnification. To "Indemnify" is defined to mean (i) to defend against all third-party claims (construed broadly, so as to include, for example, complaints and causes of action both when filed and when threatened) and regulatory actions (construed broadly, so as to include investigations and disciplinary actions by any government entity with the power to investigate or impose a penalty of any kind) and (ii) to pay all amounts (construed broadly, so as to include, for example settlements, judgments, fines, and attorneys fees awarded under all available theories of liability and damages) owed to such third-party claimants or regulators.

Procedure. A party seeking to be Indemnified will provide timely notice to the Indemnifying party, although untimely notice will relieve the Indemnifying party of its obligations only to the extent that the delay has prejudiced its ability to defend the claim. The Indemnifying party will have the right to control the defense, including the right to reach a settlement with the claimant; however, the Indemnified party will have a right to participate through its own counsel at its own expense and the Indemnifying party will not enter into a settlement that requires the Indemnified party to pay any amount or admit to any liability without the written consent of that Indemnified party.

The End User's Indemnifiable Claims. The Provider will Indemnify the End User for:

infringement of a patent or copyright, provided that the infringement arises through the End User's licensed use of the Service, either alone or (when the Provider would be liable for indirect or contributory infringement) in combination with other technology or processes

the Provider's breach of a Data Processing Agreement

the Provider's violation of law

the Provider's intentional misconduct or reckless conduct (even when not a breach of the Agreement)

Limitation of Liability

Standard Limitations on Types of Liability. Other than for the Exceptions to the Standard Limitation on Types of Liability (immediately below), each party will be liable to the other for direct damages only. As such, the following types of damages will be excluded, regardless of the underlying theory of recovery: indirect damages, consequential damages, special damages, punitive damages, lost profits, lost reputation, and the cost of replacement services.

Exceptions to the Standard Limitation on Types of Liability. The following liabilities will not be subject to the Standard Limitation on Types of Liability:

amounts owed under an obligation to Indemnify

amounts awarded for a breach of confidentiality obligations (other than as applied to a breach of a Data Processing Agreement) under this Agreement

amounts awarded for a party's intentional misconduct or reckless conduct

Standard Limitation on Total Amount of Liability. Other than for the Exceptions to the Standard Limitation on Amount of Liability (immediately below), neither party's total liability to the other (aggregated across all claims and causes of action) will exceed the fees paid or payable by the End User in the subscription year (or, if fees are assessed on a basis other than a subscription, the calendar year) in which transpired the events on which the claim is based.

Exceptions to the Standard Limitation on Total Amount of Liability. The following liabilities will not be subject to the Standard Limitation on Amount of Liability:

amounts owed under an obligation to Indemnify

amounts awarded for a breach of confidentiality obligations (other than as applied to a breach of a Data Processing Agreement) under this Agreement

amounts awarded for a breach of a Data Processing Agreement

amounts awarded for a party's willful or reckless conduct

Substantive Law and Forum for Disputes

Substantive Law. The Agreement will be interpreted according to the substantive law of the jurisdiction in which the End User is domiciled.

Forum: Disputes will be decided in the state and federal courts of the jurisdiction in which the End User is domiciled. Any state or federal court with jurisdiction may be used to (i) seek preliminary injunctive relief or (ii) enforce a judgment.

Attorneys Fees and Costs

Attorneys Fees and Costs. An authority that decides a dispute between the End User and the Provider will have discretion to award the prevailing party attorneys fees and costs.

No Waiver

No Waiver. A party's delay in exercising its rights under this Agreement will not be deemed a waiver of its rights, and a party's waiver of any right under this Agreement will not be deemed a waiver of any other right.

Interpretation of the Agreement

Complete Agreement. This Agreement and the attachments to this Agreement (such as exhibits and addenda), contain the complete agreement between the Parties in relation to its subject matter, superseding all prior or contemporaneous written or oral contracts. Neither party enters into this agreement based on any representation not stated herein. This agreement may only be amended in a writing that references it and states the Parties' intent that it be amended through such writing.

Severability. If any part of this Agreement (including entire provisions or any part thereof) is determined to be unenforceable (for any reason) but the remainder of the Agreement contains lawful distinct objects, then the unlawful part of the Agreement will be severed and the lawful objects will remain enforceable.

Conflicts Between Documents. The Agreement and the attachments to this Agreement (such as exhibits and addenda) will be interpreted as a single agreement, such that, for example, silence on a topic in any one document will not be interpreted as a conflict with an explicit statement on that same topic in another document. For example, the absence of a limitation of liability provision in a Data Processing Agreement will not be interpreted as an intention to prevent the application of a limitation of liability provision stated in the Agreement to claims arising from a breach of that Data Processing Agreement. If explicit statements in different documents are in conflict with one another, then the order of precedence will favor (i) a document that explicitly notes the conflict and states an intention to control or (ii) if no such note and statement exists, then an attachment to this Agreement, followed by this Agreement.

BigPanda

SERVICE LEVEL AGREEMENT

The BigPanda Service is designed and managed to a 99.9% monthly uptime expectation.

There is no deduction from that uptime expectation for most updates, which are designed to be deployed without requiring downtime.

Major updates and emergency maintenance may require downtime. BigPanda will provide no less than 30 days advance notice of major updates and will use best efforts to provide prior notice of emergency maintenance. BigPanda will also take all commercially reasonable efforts to schedule such efforts to minimize their impact on End User. The uptime calculation will allow for up to 6 hours of such downtime annually.

Despite BigPanda's adherence to industry standards for infrastructure resiliency, events beyond BigPanda's reasonable control – such as widespread failures of core internet infrastructure – may disrupt the BigPanda service. The uptime calculation will allow for a reasonable amount of downtime for such events.

End User will receive a service credit for a failure of the BigPanda Service to achieve the monthly uptime expectation:

Achieved Uptime	**Service Credit** as % of annual fee allocated to the month
Less than 99.9% but at least 99.5%	2%
Less than 99.5% but at least 99.0%	4%
Less than 99.0% but at least 98.0%	6%
Less than 98.0% but at least 97.0%	10%
Less than 97%	40%

If the BigPanda Service fails to achieve the monthly uptime expectation for 3 consecutive months or for any 4 months within a subscription year, End User may terminate the Agreement upon written notice delivered at any point within 3 months after the last day of the last month of uptime failure. Upon such termination, End User will receive a refund of prepaid subscription fees, prorated to the date of termination.

Real-Time status, incident, and maintenance notices are available at status.bigpanda.io and by push notification through the subscription functionality provided at that URL.

BigPanda

SECURITY STANDARDS

This Security Standards document describes the technical, administrative, and physical safeguards BigPanda takes to safeguard End User Data.

Technical Safeguards

Network Security. BigPanda's production environment, including the Platform and all End User Data, is hosted by Amazon Web Services (AWS) in BigPanda's logically isolated Virtual Private Cloud. Networks are protected against unauthorized access using firewalls, segmentation into different security groups, and private IP addresses. BigPanda's AWS Security Groups are configured to "Deny All First" which is equivalent to "Least Privilege" for Security Groups settings.

Encryption. BigPanda uses industry-standard encryption methods and products to protect End User Data at rest and during transmission between End User's and BigPanda's systems.

Encryption in Transit. End User Data is encrypted in transit between BigPanda and End User's systems over public networks using HTTPS/TLS 1.2 or better.

Encryption at Rest. End User Data at rest is encrypted using AES-256 or better.

Encryption Key Management. Encryption keys are managed according to industry best practices, including with hardware security modules that have been validated under FIPS 140-2.

Access Control. BigPanda enforces "separation of duties" and "least privilege" principles by restricting use based on unique custom roles, and access permissions are reviewed at least quarterly. User permissions are adjusted when job responsibilities change and promptly revoked upon termination. Two-factor authentication is required for employees to access BigPanda's systems and applications. Access to the production environment is further restricted with additional layers of protection, including SSH key authentication, connection to BigPanda's VPN, and multi-factor authentication.

Vulnerability Detection and Management. BigPanda continuously monitors its networks and systems for threats, including by regularly scanning for vulnerabilities, conducting internal penetration tests, and employing an intrusion detection system to detect malicious activity. An independent third-party performs penetration tests annually, which test BigPanda's Platform and APIs against common and advanced security vulnerabilities using direct and indirect attacks. BigPanda remediates identified vulnerabilities based on risk and severity, consistent with industry standards.

Secure Coding. BigPanda applies secure coding and privacy by design principles in its software development lifecycle. Changes to the production environment can be made only through a centralized configuration management system, and every change is logged and undergoes a security review, vulnerability scan, code review, and other testing before deployment. End User Data is never used for development or testing purposes, and all development and testing are conducted in a non-production environment.

Logging and Monitoring. BigPanda collects and monitors log data from all systems that process End User Data, using industry-standard tools and configuration. Logs are reviewed and analyzed at least monthly. All audit logs are exported to a dedicated "Security" AWS account restricted to authorized BigPanda employees.

ADMINISTRATIVE SAFEGUARDS

Security Program. BigPanda maintains a comprehensive security program designed to comply with data protection laws, prevent and recover from security incidents, and maintain the confidentiality, integrity, and availability of End User Data. The security program is reviewed at least annually and updated as necessary to address changes to BigPanda's business and products, applicable laws, and the threat landscape.

BigPanda Employees. All employees must complete security training as part of the new hire onboarding process and on an ongoing basis, and employees with access to End User Data or personal data must complete additional role-based training. All BigPanda employees must sign a commitment to maintain the confidentiality of End User Data and other Confidential Information during and after their employment with BigPanda and to comply with BigPanda's security policies and requirements. Employees who do not comply with these requirements are subject to discipline and potentially termination.

Service Providers. BigPanda conducts security due diligence before onboarding new service providers, contractually obligates service providers to maintain the security standards necessary to satisfy BigPanda's commitments to End User, and monitors service providers for compliance on an ongoing basis.

Incident Response. BigPanda has a security incident response policy, which is updated annually and designed to respond to, contain, and remediate security incidents. BigPanda will notify End User within 24 hours of confirming any unauthorized access or disclosure of End User Data and will provide additional information as it becomes known or as is reasonably requested by End User. BigPanda will assist End User with its breach notification obligations and will take reasonable steps to mitigate and, where possible, remedy the effects of a security incident.

PHYSICAL SAFEGUARDS

Data Centers. Physical access to AWS data centers is strictly controlled at the perimeter and at building entry points by professional security staff and are monitored and protected using video surveillance, state of the art intrusion detection systems, biometric access controls, and other electronic means. AWS data centers are designed to withstand adverse weather and other reasonably predictable natural conditions and are supported by on-site back-up generators.

BigPanda Offices. Physical access to BigPanda's offices is controlled at all entry points, access is restricted to authorized employees, and visitors must be escorted at all time.