Program Guide

This Cribl Program Guide ("**Program Guide**") applies to the Subscription Services, purchased by Customer directly from Cribl, or from an Authorized Reseller. The Program Guide describes Support, Cribl Cloud availability, and the written program of policies, procedures, and controls governing information security.

The Subscription Services are made available by Cribl under the terms of this Program Guide as incorporated into the Cribl Subscription Services Agreement or other agreement that grants Customer the right to access and use the Subscription Services (collectively, the "**Agreement**," without regard to the name of the underlying agreement, or how it refers to its parties or identifies the Subscription Services). This Program Guide and the Agreement constitute the complete and exclusive agreement between Customer and Cribl relating to its subject matter and supersedes all prior oral and written agreements, understandings, representations, warranties, and communications regarding its subject matter. Capitalized terms defined in this Program Guide shall have the meanings set forth in this Program Guide. Capitalized terms not otherwise defined in this Program Guide shall have the meaning given to them in the Agreement. In the event of any conflict between the terms and conditions of this Program Guide and the Agreement, the Agreement will govern to the extent of such conflict.

This Program Guide may be updated from time to time, solely with prospective effect, upon posting the new version to Cribl's website. Updates to this Program Guide will retain the material commitments, protections, and overall level of service provided to Customer as described herein.

This Program Guide does not apply to any evaluation, trial, or other unpaid access to the Subscription Services, including Cribl's "Free Trial" online offering.

This Program Guide utilizes the following defined terms:

"**Defect**" means a reproducible failure of the Subscription Services to perform any material function outlined in the Documentation.

"**Support Portal**" means Cribl's online portal for support information and requests available at **https://cribl.io/support/** and its related and successor websites.

"**Technical Contact**" means a qualified individual designated by Customer to receive Support.

Support

During the Subscription Term, Cribl will provide to Customer the level of Support outlined below. Please refer to the Documentation and instructions posted on the Support Portal for more detailed information on Support procedures.

Scope of Support

Support is provided by Cribl to resolve Defects experienced by Customers. A resolution to a Defect may consist of a fix, workaround, or other relief, as Cribl deems reasonable.

Support does not include the following:

- Implementation, configuration, integration, or customization services
- Training or assistance with administrative functions
- Resolving immaterial defects
- Resolving Defects due to modifications of the Subscription Services made by any person other than Cribl or a person acting at Cribl's direction

Support Process

Cribl will answer Support requests regarding the operation of the Subscription Services once registered in the Support Portal by Customer's system administrator and supported by a Technical Contact. For any Defect, Customer may assign in the Support Portal a priority level based on the relative impact of the Defect on Customer's use of the applicable Subscription Services. Cribl may re-assign the priority level at its sole discretion. The level of Support is selected by Customer in the corresponding Order Form and is as described below:

	Standard	Enterprise
Support Availability	9am ET – 8pm ET (excluding U.S. public holidays)	24 hours per day, 7 days per week

Cribl will use commercially reasonable efforts to respond to and address any Defects, including through the application of updates to the Subscription Services, reported by Customer and confirmed by Cribl per the priority level assigned to the Defects in the Support Portal.

Priority levels and target initial response times for each priority level are described below.

Priority Level	Definition	Response Time	Target Level of Effort
P1	**Critical** - Production instance is unavailable.	1 hour	Continuously, 24 hours per day, 7 days per week
P2	**High** - Production instance is available; functionality or performance is severely impacted.	2 hours	As appropriate, Monday through Friday, 9am to 5pm Local Time
P3	**Medium** - Production instance is available and usable with partial, non-critical loss of functionality.	4 hours	As appropriate, Monday through Friday, 9am to 5pm Local Time
P4	**Low** - Cosmetic issues or requests for general information about the Subscription Services	24 hours	As appropriate, Monday through Friday, 9am to 5pm Local Time

Support responses may take the form of software or infrastructure updates, procedural solutions, correction of Documentation, or other remedial measures as Cribl may, in its sole discretion, determine to be appropriate. Support is provided to Customer only and not to third-party Authorized Users unless otherwise expressly agreed in an Order Form. Cribl will have no obligation to provide Support for preview, trial, beta or evaluation features, or Third-Party Components.

Notwithstanding anything herein, the response times and priority levels set forth above will not modify any applicable security or privacy breach notification obligations as outlined in any data security or data privacy addenda, or other applicable terms in Customer's underlying Agreement.

Updates and Upgrades

Customer will have access to all updates and upgrades applicable to its purchased Subscription Services that are made generally available to all customers.

Customer Acknowledgments

Cribl's Support obligations are conditioned upon the following:

1. Customer must designate a limited number of Technical Contacts to make Support requests. Customer will use reasonable efforts to ensure that the individuals designated as Technical Contacts are qualified to support Customer's internal teams. Technical Contacts must provide reasonable assistance to resolve Support issues and provide updates to Cribl using the Support Portal or email.

2. Cribl may collect and use metrics, and other data derived from the operation of the Subscription Services, including the diagnostic bundle described in the Documentation (collectively, the "**Usage Data**") to operate, support, improve, and develop its products and services and for industry benchmarking and analysis. Cribl will not share Usage Data with any third party except: (a) in accordance with the Agreement; or (b) to the extent the Usage Data is aggregated and anonymized such that Customer and Authorized Users cannot be identified.

3. If Customer purchased access to the Subscription Services from an Authorized Reseller: (a) Customer agrees that this Program Guide will apply notwithstanding anything to the contrary in an agreement with the Authorized Reseller; and (b) if Cribl does not receive payment from Customer for the Subscription Services purchased directly, or indirectly through an Authorized Reseller, Cribl will have the right to suspend Support until payment is received without liability for such suspension. Cribl will not be liable for any contractual obligation made by the Authorized Reseller or any other third party beyond those set forth in this Program Guide.

4. Customer must be using the latest release of the Subscription Services.

Cribl Cloud Service Level Agreement

Cribl will provide Cribl Cloud with at least 99.9% Availability. "**Availability**" means the production instance of Cribl Cloud can be accessed by Customer and its Authorized Users during a calendar month. Availability is calculated monthly as the minutes a production instance of Cribl Cloud is accessible to Authorized Users in a month divided by the total minutes in that month, where the calendar and clock utilized will be that used by Cribl Cloud in its hosted location.

Cribl Cloud products that Cribl designates as free or that involve customer-managed components in a hybrid Cloud deployment do not have a minimum Availability requirement.

For any calendar month in which the Availability of a production instance of Cribl Cloud falls below 99.9%, excluding Service Level Exclusions (defined below) ("**Service Level**"), as Customer's sole and exclusive remedy for such downtime, Cribl will credit your Cribl Cloud account as follows ("**Service Level Credit**"):

Availability	Credits
99% to 99.89%	5% of previous month's total usage
98% to 98.9%	10% of previous month's total usage
Below 98%	20% of previous month's total usage

To request a Service Level Credit, Customer must submit a ticket to the Support Portal within 30 days from the end of the month in which the Service Level was not met and provide sufficient information and documentation to show the qualifying downtime. Cribl will review the request and decide, within thirty days of receiving your request and at its complete discretion, whether and the extent to which a qualifying downtime occurred. If Cribl determines that a qualifying downtime occurred, Cribl will issue appropriate Service Level Credits to Customer's Cloud account in accordance with the table above.

"**Service Level Exclusions**" means: (a) emergency maintenance provided with at least one hour prior written notice; (b) scheduled maintenance provided with at least 48 hours' prior written notice; (c) unavailability caused by Customer interference due to testing or audit, or Customer's integrations except as described in the Documentation; (d) unavailability caused by general internet problems or circumstances beyond Cribl's reasonable control, or arising from any of the following: data or software received in, or submitted to, Customer's instance of Cribl Cloud, Customer's or a user's equipment, Customer's authentication software, third-party acts, or unavailability to services or systems not provided by Cribl to Customer; (e) suspension as provided for in the Agreement; or (f) unavailability of evaluation, proof of concept, proof of technology, beta, Free Trial, or other non-production use or instances of Cribl Cloud. All notices provided for herein will be made to the administrator user(s), posted on the Support Portal, or displayed in a conspicuous on-screen message to the administrator user(s) in Cribl Cloud.

Security

1. **Security Overview**.
   While providing the Subscription Services, Cribl will maintain a written information security program of policies, procedures, and controls aligned to ISO 27001 series, or a substantially equivalent standard, governing the processing, storage, transmission, and security of Customer Data (the "**Security Program**"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Cribl will update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

1.1 Security Organization. There will be a Chief Information Security Officer, or equivalent executive, who is designated as responsible for managing the Security Program.

1.2 Policies. Cribl's information security policies will be: (a) documented; (b) reviewed and approved by management, including after material changes to the Subscription Services; and (c) published and communicated to personnel and contractors with access to Customer's instance of Cribl Cloud, and will include appropriate remedies for non-compliance.

1.3 Risk Management. Cribl performs information security risk assessments as part of a governance, risk, and compliance program that is established to regularly test, assess, and evaluate the effectiveness of the Security Program. Such assessment will be designed to recognize and assess the impact of risks and implement identified risk reduction or mitigation strategies to address new and evolving security technologies, changes to industry-standard practices, and changing security threats.

2. Audits.

2.1 Procedure. Cribl allows for and contributes to audits that include inspections by granting Customer (either directly or through its representative(s)) access to all reasonable and industry-recognized documentation evidencing the applicable policies and procedures governing data security and privacy under its Security Program through a self-access trust portal at no additional cost to Customer ("**Audit**"). The information available includes documentation evidencing Cribl's Security Program, as well as copies of third-party attestation reports (including audits) listed above.

2.2 Output. Upon completion of the Audit, Cribl and Customer may schedule a mutually convenient time to discuss the output of the Audit. Cribl may in its sole discretion, consistent with industry and Cribl's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve Cribl's Security Program. The Audit and the results derived therefrom are deemed to be the Confidential Information of Cribl.

3. Physical and Environmental Security Measures.

3.1 Infrastructure. Cribl uses infrastructure-as-a-service cloud providers to support the application that processes Customer's instance of Cribl Cloud as further described in the Agreement or Documentation (each, a "**Cloud Provider**"). Cribl requires each Cloud Provider to have an SSAE 18/SOC 2 Type II attestation, ISO 27001 certification, or an industry-recognized equivalent security attestation or certification commensurate with the providers' risks, and will implement appropriate physical and environmental security measures, including: (a) physical access to the facilities controlled at building ingress points; (b) visitors required to present ID and be signed in; (c) physical access to servers managed by access control devices; (d) physical access privileges reviewed regularly; (e) utilization of monitoring and alarm response procedures at facilities; (f) use of CCTV; (g) fire detection and protection systems; (h) power back-up and redundancy systems; and (i) climate control systems.

3.2 Location. The hosting location of the Cribl Cloud instance is selected by Customer in the corresponding Order Form, or as Customer otherwise configures the location via Cribl Cloud or Support. Alternatively, if Cribl Cloud was purchased online such that no Order Form applies, then the location will be identified in the web form(s) applicable to the purchase.

3.3 Account Isolation. Each Customer is provisioned with a separate Amazon Web Services account and virtual private cloud (VPC) of Cribl Cloud that is logically separated from other customers.

4. Technical Security Measures.

4.1 Access Administration. Access to Cribl Cloud is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and non-production Cribl Cloud instances. Cribl employees are assigned a unique user account. Individual user accounts will not be shared. Access privileges are based on job requirements using the principle of least privilege and are revoked upon termination of employment. Access entitlements are reviewed by management semi-annually. Infrastructure access includes appropriate user account and authorization controls, which require use of secure remote access connections, complex passwords, account lock-out enabled, and a two-factor authenticated connection.

4.2 Service Access Controls. Cribl Cloud includes user-based and role-based access controls. Customer is responsible for configuring such access controls within its instance.

4.3 Session Management and Cookies. When providing Cribl Cloud, Cribl uses session tokens and cookies to: (a) validate user sessions and authorize requests; and (b) monitor Cribl Cloud application software and usage software. Customer will provide necessary notices to, and collect any necessary consents from, its users of Cribl Cloud for cookies used by Cribl Cloud.

4.4 Logging and Monitoring. The production infrastructure log activities are centrally collected, are secured in an effort to prevent tampering, and are monitored for anomalies. Cribl provides a logging capability in the platform that captures login and actions taken by users in Cribl Cloud. Customers can access user activity audit logs within its instance(s).

4.5 Data Encryption. Cribl uses industry-standard encryption to encrypt data in transit over public networks to Cribl Cloud. In addition, Cribl provides disk-level and storage-level encryption at rest capabilities. Cribl encrypts data at-rest using AES 256-bit or better encryption. Cribl uses Transport Layer Security (TLS) 1.2 or better for data in-transit over untrusted networks.

4.6 AWS Security Group. The AWS security group for all instances of Cribl Cloud are configured to prevent all inbound traffic from all resources except for ports enabled by Cribl to enable data ingestion or unless otherwise assigned to the security group by Customer. All outbound IPv4 traffic (and IPv6 as applicable) are allowed by default. Customer has the option to control traffic at the subnet level through a network access control list.

4.7 Vulnerability Management. Cribl monitors for and responds to security automated vulnerability alerts that are reviewed daily. Vulnerability alerts are triaged by Cribl's Security team and assigned and tracked centrally for remediation in accordance with Cribl's vulnerability management policy. Customer instances of Cribl Cloud are regularly updated to address known vulnerabilities. Self-hosted deployments of Cribl software must be kept updated to the latest monthly release to benefit from vulnerability patching as vulnerability patches are not backported to older versions. When software vulnerabilities are revealed and addressed by a vendor patch, Cribl will obtain the patch from the applicable vendor and apply it within an appropriate time frame per Cribl's then-current vulnerability management and security patch management standard operating procedure, and only after such patch is tested and appears to be safe for installation in all production systems.

4.8 Intrusion Detection Technology. Cribl uses an intrusion detection technology to monitor the Cribl Cloud network and systems for malicious activity and policy violations. Intrusion detection activity is collected using a security information and event management system.

4.9 Antivirus. Cribl runs antivirus and anti-malware software on Cribl-owned and managed endpoints (including employee laptops and desktops) and updates such software at regular intervals.

4.10 Malicious Code. The Cribl Cloud application is analyzed in an effort to detect, prevent, and remove viruses, Trojan horses, malware, worms, or similar harmful, malicious, or hidden procedures, routines, or mechanisms that may result in: (a) inoperability of Cribl Cloud; or (b) interruption or interference with the operation of Cribl Cloud (collectively, "**Malicious Code**"). If Cribl Cloud is found to contain any Malicious Code that adversely affects the performance of Customer's instance of Cribl Cloud or causes a material security risk to data received in Customer's instance of Cribl Cloud, Cribl shall, as Customer's exclusive remedy, use commercially reasonable efforts to remove the Malicious Code. Customer will be responsible for any security vulnerabilities, and the consequences of such vulnerabilities, including any Malicious Code in Customer Data, software, systems, or integrations that adversely affect the performance of the Subscription Services or cause a material security risk to Customer.

4.11 Change Control. Cribl evaluates changes to platform, applications, and production infrastructure to minimize risk and such changes are implemented following Cribl's change management standard operating procedure.

4.12 Configuration Management. Cribl implements and maintains standard hardened configurations for all system components within Cribl Cloud. Cribl evaluates and considers industry-standard hardening guides, such as guides from the National Institute of Standards (NIST) and Technology and Center for Internet Security, when developing standard hardening configurations.

4.13 Secure Software Development. Cribl implements and maintains secure application development policies and procedures aligned with industry-standard practices, such as NIST SSDF (or a substantially equivalent standard). All personnel responsible for secure application design and development will receive appropriate training regarding Cribl's secure application development practices. Cribl performs a combination of static and dynamic testing and analysis of code before the release of such code to Customers.

5. Organizational Security Measures.

5.1 Cribl Access Limitations. Cribl employees or contractors will not do any of the following to data uploaded by Customer to Cribl Cloud without Customer's prior consent or unless as part of functionality of Cribl Cloud initiated by or for Customer (e.g., data integrations or data transferability between instances): (a) access the data; (b) move the data outside Customer's tenant (except as initiated by Customer or for Customer by a third party); or (c) screen-capture, copy, or record the data in video or other formats.

5.2 Cloud Provider Review. Cribl performs routine reviews of Cloud Providers to confirm that the Cloud Providers continue to maintain appropriate security controls necessary to comply with the Security Program.

5.3 Personnel Security. Cribl performs background screening on all employees and contractors who have access to Customer's instance of Cribl Cloud per Cribl's then-current applicable standard operating procedure and subject to applicable laws. Background screening may include the following, as permitted by applicable law: (a) social security verification; (b) prior employment verification; and (c) criminal history.

5.4 Security Awareness Training. Cribl maintains a security and privacy awareness program that includes appropriate training and education of Cribl personnel, including, as applicable, any contractors that may access Customer's instance of Cribl Cloud. Such training is conducted at the time of hire and at least annually throughout employment at Cribl.

5.5 Vendor Risk Management. Cribl maintains a vendor risk management program that assesses certain vendors for appropriate security and privacy controls and business disciplines.

5.6 Software Inventory. Cribl maintains an inventory of all software components (including open-source software) used in Cribl Cloud.

6. Service Continuity.

6.1 Disaster Recovery. Cribl (a) maintains a disaster recovery ("**DR**") plan for Cribl Cloud that is consistent with industry standards; (b) tests the DR plan at least once per calendar year; (c) makes available summary test results to Customers upon request (which will include the actual recovery point and recovery times); and (d) documents any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent Cribl Cloud from being recovered per the DR plan.

6.2 Business Continuity. Cribl maintains a business continuity plan ("**BCP**") to minimize the impact to its provision and support of Cribl Cloud from an event. The BCP (a) includes processes intended to protect personnel and assets and restore functionality per the time frames outlined in the BCP; and (b) is tested annually and updated based on any deficiencies identified and recognized by Cribl during such tests.

7. Monitoring and Incident Management.

7.1 Incident Monitoring and Management. Cribl will monitor, analyze, and respond to security incidents in a timely manner per Cribl's incident management policy. Cribl's security group will escalate and engage response teams as Cribl deems necessary to address a security incident.

7.2 Breach Notification. Cribl will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "**Breach**") without undue delay following the determination by Cribl that a Breach has occurred.

7.2.1 Report. The initial Breach report will be made to Customer security contact(s) designated by Customer to Cribl (or if no such contact(s) are designated, then to the primary Technical Contact designated by Customer). As information is collected or otherwise becomes available, Cribl will provide without undue delay any further information learned by Cribl regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected individuals, government agencies, and data protection authorities in accordance with all applicable data protection and privacy laws regulating the Processing of Personal Data, including where applicable, the European Union's General Data Protection Regulation and the United Kingdom's General Data Protection Regulation. The Breach report will include the name and contact information of the Cribl contact from whom additional information may be obtained. Cribl shall inform Customer of the measures that Cribl will adopt to mitigate the cause of the Breach and to prevent future Breaches.

7.2.2 Customer Obligations. Customer will cooperate with Cribl by providing any information that is reasonably requested by Cribl to resolve any security incident, including any Breaches, identify its root cause(s), and take measures intended to prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted data subjects (identified or identifiable natural persons) and for providing such notice.

7.2.3 Limitations. Customer acknowledges that because Cribl personnel do not review data processed by Customer in Cribl Cloud, it may be unlikely that Cribl can provide information as to the nature of that data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of Cribl with Customer in connection with a Breach will not be construed as an acknowledgment by Cribl of any fault or liability with respect to such Breach. As used in this Program Guide, "**Personal Data**" means any information relating to an identified or identifiable natural person uploaded to Cribl Cloud by or for Customer or Customer's agents, employees, or contractors; and "**Processing**" means any operation or set of operations that is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

8. Penetration Tests.

8.1 By a Third Party. Cribl contracts with third-party vendors to perform penetration tests on Cribl's product application code at least three times per year to identify risks and remediation options that help increase security. Cribl shall make executive summary reports from the penetration testing available to Customer on demand.

8.2 By Customer. Customer shall not perform penetration tests on Cribl Cloud without Cribl's express written authorization. Penetration testing information is available pursuant to an Audit as described in Section 2.1 (Audit).

9. Sharing the Security Responsibility.

9.1 Product Capabilities. Cribl Cloud is designed to provide Customer with the option to: (a) authenticate users before accessing Customer's instance; (b) integrate with industry-standard federation solutions; (c) allow users to manage passwords; (d) prevent access by users with an inactive account; and (e) select data for exclusion from processing. Customer is solely responsible for: (i) managing its users' access to, and use of, Cribl Cloud by assigning to each user a credential and role that controls the level of access to Cribl Cloud; (ii) its decision to process data containing sensitive information, including any Personal Data, and Cribl will have no liability to the extent that damages would have been mitigated by Customer's decision not to mask such sensitive information; (iii) protecting the confidentiality of administrative credential information, including each user's login and password, and managing roles, rights, maintaining user logins for each individual person, and granting each user's access to Cribl Cloud; and (iv) reviewing Cribl's Security Program and making an independent determination as to whether it meets Customer's requirements, taking into account the type and sensitivity of the data that Customer processes using Cribl Cloud.

9.2 Industry-Specific Regulations. Customer acknowledges that the Subscription Services are not intended for any industry-specific use and Cribl does not review data or assess regulatory impacts. Customer is solely responsible for compliance with regulations, laws, rules, or other requirements applicable to its industry and for managing data in Cribl Cloud to comply with such requirements. Customer acknowledges that Cribl is not a Business Associate and should not process patient, medical, or other protected health information regulated by the U.S. Health Insurance Portability and Accountability Act unless the parties have expressly agreed otherwise in a Business Associate Addendum.

9.3 High-Risk Activity. Customer understands that the Subscription Services are intended for routing, searching and enhancing certain types of data, including logs, metrics and traces, and Customer must use the Subscription Services within the intended business purposes described in the Documentation and not for any purpose that requires fail-safe processing performance, or applications for which failure could result in death, personal injury, or severe physical or environmental damage ("**High Risk Activity**"). Cribl, its licensors and suppliers expressly disclaim all warranties of fitness for any such use and Customer releases and holds Cribl, its licensors and suppliers harmless from liability arising out of use of the Subscription Services for or in relation to any High Risk Activity.

9.4 Security Contact. In accordance with this Program Guide, Customer will identify and maintain within the Support Portal appropriate security contact(s) for all information security incidents and information security-related communication.

9.5 Limitations. Notwithstanding anything to the contrary in this Program Guide or other parts of the Agreement, Cribl's obligations herein are only applicable to the Subscription Services. This Program Guide does not apply to: (a) information shared with Cribl that is not data processed using the Subscription Services; (b) data in Customer's VPC or a third-party network, data stored in Customer's environment, or data hosted for Customer by its third-party providers; and (c) data processed by Customer or its Authorized Users in violation of the Agreement or this Program Guide.