FAQ for Tealium’s Customer Protection Package (“CPP”)

Thank you for taking the time to review this FAQ. It was designed to provide you with helpful information about Tealium’s Customer Protection Package (“CPP”) which are the documents that describe the protections and commitments that Tealium offers all its Customers as part of the MSA. We hope this FAQ will provide you with some helpful context as you review the CPP. This FAQ is provided for informational purposes only and will not form part of the contract being contemplated between the parties. Note, all liability issues for the DSS are addressed in the TOS.

What is the structure of the CPP?

Our CPP is made up of three documents:
The **Service Level Agreement (“SLA”)** contains our commitment to availability across all our Services, your remedies in the unlikely event we do not meet our commitment, and how we address support issues.
The **Acceptable Use Policy (“AUP”)** contains standard guidelines for your use of the Services, which really boil down to not being a bad actor on the internet.
The **Data Security Statement (“DSS”)** contains our formalization of our organizational and technical security measures designed to protect your data.

SLA

Our SLA is first-in-class in our industry, providing for 99.9% availability across all our Services. Tealium also provides a website for our Customers to subscribe to that will provide real-time status, as well as notifications for maintenance and emergency outages. We provide remedies in the unlikely event that we miss this availability, as well as a termination right for chronic outages. The SLA also includes information about how we address any support issue that might arise, and how to contact us in an emergency.

Since our SLA is being provided across all our products, and we are delivering a multi-tenant SaaS service, we are unable to alter our SLA for one Customer. We are confident that our SLA will more than address all our Customer’s issues.

AUP

Our AUP is a pass-through policy from Amazon Web Services (“AWS”), and contains restrictions on how people should use our Services over the internet, including related to SPAM, pornography and phishing. We are required to have all Customers agree to this policy as the Services rely on the AWS infrastructure.

Since our AUP is a pass-through policy, we are unable to agree to any modifications.

DSS

The DSS addresses all electronic data and information submitted by or for you to the Services, including enhancement and output derived from your use of the Services, which we call “Customer Data”. Our DSS reflects our security program for Customer Data, which applies to all of our customers equally. Please bear in mind that we do not access Customer Data unless you grant us access for a particular purpose (e.g., a support request). If you choose to grant us access, you control the access permissions and can terminate our access at any time.

There are specific reasons why we must use our DSS instead of using the data security documentation of customers.

1. The Services are provided to our customers using a “one-for-all” model, meaning the same Services are provided to all of our customers. We do not offer a “customized” service offering that would allow us to treat one customer (or its data), differently from other customers. Even our ancillary services (such as deployment or support) are provided in a uniform manner across our customer base.

2. Tealium has no visibility into the content of Customer Data, including whether or not it is pseudonymized, personal or sensitive, the particular manner in which you store or structure that Customer Data in your account, to whom the data relates, the purposes for which you process the data, the scope/volume of your processing, third parties you transmit the data to, and whether (or the degree to which) the particular data and/or processing poses risks to data subjects. As a result, we also will not have visibility necessary to determine which portions of the data may be subject to industry-specific or country-specific regulations.
3. All customers benefit uniformly from Tealium's rigorous security controls. Because the same Service is provided to all customers, you benefit from a set of shared technical and organizational security measures. Services provided in our private cloud environment have enhanced technical and organizational security measures such as an attestation of compliance with the US HIPAA regulations.

Since our DSS is being provided uniformly across all our products and customers, we are unable to alter our DSS for one Customer. We are confident that our DSS will more than address all our Customer's security issues. Note that while there is no customized offering, you are able to select the particular geographic hosting location(s) for your account, as further defined in the MSA.

Service Level Agreement (SLA)

This Service Level Agreement ("SLA") is incorporated into, and made a part of, the Master Services Agreement ("MSA"), Terms of Service or Service Order between Tealium Inc. and Customer that references this SLA, and constitutes a part of the MSA between Tealium and Customer (as identified in such Service Order).

1. **Definitions.** The following defined terms are used in this SLA Addendum:

"Available" or "Availability" means the Services are in an operable state, and the Service can be accessed through programmatic access (APIs, tags, HTTP requests/responses) or user interface access as applicable to the particular Service. Solely for Delivery Network performance, "Available" means Delivery Network servers are responding to requests for libraries.

"Delivery Network" means the content delivery network service providers used in connection with certain Services for the purpose of serving Tealium JavaScript or other Service related files ("Libraries") to Digital Properties.

"Force Majeure" means any cause beyond such Party's reasonable control, including but not limited to the weather, unavailability of utilities or communications services (including access to the Internet), civil disturbances, acts of civil or military authorities, or acts of God.

"Incident" means a P1, P2 or P3 problem with the Services.

"Monthly Subscription Amount" means the contracted amount for the Services for the Service Term, divided by the number of months in the Service Term (excluding fees for implementation, managed, and professional services and Additional Usage Fees).

"Monthly Uptime Percentage" means the percentage of time within a given calendar month the Services are Available. "Available" or "Availability" means the Services are in an operable state, and the Services can be accessed through programmatic access (APIs, tags, HTTP requests/responses) or user interface access as applicable to the particular Services. Solely for Delivery Network performance, "Available" means Delivery Network servers are responding to requests for Libraries.

"Priority 1" or "P1" Incident means a critical defect in which the Services has a devastating impact on Customer's Digital Property. For example, the Digital Property is not rendering due to the Tealium tag, deployed Libraries are not being delivered by the Delivery Network directly causing business critical content to not display, the Services have widespread outages or are otherwise inaccessible, and the deployment has been "rolled back" to a previously published (and previously working) version which did not resolve the issue. Failure impacts Customer's ability to collect or retrieve Customer Data.

"Priority 2" or "P2" Incident means a material defect in which the Services are functioning but Customer is unable to use a material portion of the Services. For example, the Delivery Network is continuing to deliver Libraries but the Service's publish capability is unavailable, and a material component is unavailable or malfunctioning with no workaround available.

"Priority 3" or "P3" Incident means a minor defect in which the Services are functioning, however there is a non-critical error or bug that causes one or more non-critical functions of the Services not to work as intended. For example, a bug within an extension or tag that may be resolved using a workaround.

"Response Time" means the amount of time between Tealium's learning of an Incident or Customer's notification to Tealium of an Incident, and Tealium acknowledging notification of the Incident and assigning resources to commence resolution of the Incident.

"Service Credit" means a credit, calculated as set forth below, that Tealium may credit towards future invoices to Customer.

2. Service Uptime Commitment. Tealium will use commercially reasonable efforts to make the Services available with a Monthly Uptime Percentage of at least 99.9% during any month (the "Service Commitment"). In the event the Services do not meet the Service Commitment, Customer will be eligible to receive a Service Credit as described below.

3. Service Credits. Service Credits are calculated as a percentage of the Monthly Subscription Amount for the specific Service for the month in which the Service Commitment for a particular Service was not met in accordance with the schedule below. Tealium will apply any Service Credits only against future payments. If Customer has prepaid in full for all Services under the MSA, in the event the MSA expires and is not renewed, Customer will be entitled to a refund of the Service Credit amount upon written request to Tealium. Customer's sole and exclusive remedy for any failure of the Services to meet the Service Commitment is the receipt of a Service Credit in accordance with the terms of this SLA. Service Credits may not be transferred or applied to any other Customer account.

If the Monthly Uptime Percentage is less than 99.9% but equal to or greater than 99%, then the Service Credit will equal 10% of the Monthly Subscription Amount.

If the Monthly Uptime Percentage is less than 99%, then the Service Credit will equal 20% of the Monthly Subscription Amount.

4. Credit Request and Payment Procedures. To receive a Service Credit, Customer must submit a request by sending an e-mail message to services@tealium.com. To be eligible, the credit request must (a) include a reasonably detailed list of the instances of unavailability that together evidence Tealium's failure to meet Service Commitment in a given month; (b) include, in the body of the e-mail, the dates and times of each incident that Customer claims to have experienced; (c) include Customer's additional information (e.g. server request logs) that document and enable Tealium to corroborate Customer's claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and (d) be received by Tealium within ten (10) business days after the end of the month in which the Service Commitment was not met. In order for Credit to be awarded, Tealium must be able to independently verify the instances of unavailability reported by Customer pursuant to this Section 4.

5. SLA Exclusions. The Service Commitment does not apply to any Services unavailability or other performance issues: (a) caused by factors outside of Tealium's reasonable control, including any Force Majeure event or Internet access or related problems beyond the demarcation point of Tealium's network or the Delivery Network; (b) that result from any actions or inactions of Customer or any third party; (c) that result from Customer's equipment, software or other technology or third party equipment, software or other technology (other than third party equipment within Tealium's direct control); (d) arising from the suspension and termination of Customer's right to use a Service in accordance with the MSA; or (e) arising from scheduled downtime for system or network maintenance.

6. Chronic Outage Termination Right. In addition to the Service Credit remedies described in Section 3 above, if the monthly Uptime Percentage is less than 97% for (two) (2) consecutive months or any four (4) months in a rolling twelve (12) month period then Customer will have the right to terminate the Service Order for the adversely affected Services and receive a refund of any amounts paid in advance attributable to periods after the effective date of termination. In order for such termination to be effective, written notice of such termination must be received by Tealium with thirty (30) days following the month in which the right to termination arose.

7. Tealium Technical Response Time and Resolution Time Objectives. Tealium will respond to Incidents and undertake resolution of Incidents in accordance with the following:

P1 Severity Level – Tealium Response Time is two (2) hours. Tealium will have assigned resources working twenty-four by seven (around the clock work) to resolve the Incident, and will provide resolution status updates every four (4) hours.

P2 Severity Level – Tealium Response Time is four (4) hours. Tealium will have assigned resources working, at least, full-time during normal business hours to resolve the Incident, and will provide resolution status updates every business day.

P3 Severity Level - Tealium Response Time is one (1) business day. Tealium will have resources working during normal business hours to resolve the Incident, and will have resolution status updates available via Customers assigned Account Manager.

Increasing Severity Level. Incidents may be raised one level of severity at the discretion of the Account Manager based on the severity of impact on Customer.

Decreasing Severity Level. Incidents may be downgraded by Tealium for any of the following reasons:

(a) The issue is not reproducible, and is no longer impacting Customer.

(b) Analysis by Customer or by Tealium determines that the severity of the issue is low enough to warrant the downgrade.

(c) A suitable workaround is provided, whether temporary or permanent, which reduces the impact of the issue to that of a lower severity category.

(d) Tealium determines Customer is not providing the required cooperation and access necessary to enable resolution of the issue.

Root Cause Analysis ("RCA"). Tealium will perform an internal RCA for P1 Incidents within 48 hours of a P1 Incident being detected, and will be available upon request by Customer within five (5) days after resolution of the Incident.

Non-Tealium Products; Connectors. Upon notification that there is a Connector failure, either from Tealium's receipt of error messages from the Connectors, or from Customer, Tealium will commence investigating such Connector failure within five (5) business days. Where Tealium has created the Connector, Tealium will make commercially reasonable efforts to work with the third-party provider of the Connector to remedy the Connector failure and to implement any solution or patch provided by the third-party provider in a reasonably timely manner. Any issues under this Section are specifically excluded from the Availability.

8. Customer Success Support Services. Tealium provides support services 24 hours a day, 7 days a week (24x7) for P1 Incidents, full-time assigned resources for P2 Incidents during normal business hours. P3 and other support services are available during Tealium's normal business hours: Monday – Friday, 8:00am – 6:00pm local time (excluding holidays). Tealium's offices are located in San Diego, CA (PST) and Reading, UK (GMT). Tealium's support hotline is +1.877.443.5276. The Customer Success support team may also be reached through Tealium's support portal at https://support.tealiumiq.com/. Further information about support services for a particular Service may be provided in the Service Order.

9. Tealium Team. Tealium will, throughout the Term of each Service Order, designate one or more employee(s) whose role is to liaise with the Customer and ensure successful implementation and operation of the Services. During the initial deployment of the Services, Customer will have a team assigned as described in an SOW. The Account Manager will be the main point of contact after deployment, and will partner with Customer and act as advisor on both tactical and strategic matters to help ensure Customer is seeing the benefit of the Services and help ensure mutual collaboration. The Account Manager will also advise on recommended training opportunities and act as a point of escalation when needed for technical assistance.

10. System Health Monitoring. Tealium provides, and Customer has access to, the Tealium Health and Status Dashboard available at https://status.tealium.com. Tealium will provide Customer the proper API interfaces to establish direct access into Heath and Status dashboard. This dashboard uses a "green", "yellow", and "red" system. Green is used to indicate the system is functioning as desired. Red is used to convey that an area of the Tealium system is being significantly impacted. Yellow is used to convey that a degradation of Services is occurring, but the issue has not been identified as causing a Service outage. Yellow is also used to indicate that a previously red status has been corrected, and is being monitored for continued stability. Planned maintenances are provided with 10-days advance notice. Emergency maintenances are posted as well, with as much advance notice as can be afforded based on the nature of the needed change. Emergency change notifications will follow the incident process.

11. Subscribing. Customer may use the Health and Status Dashboard directly, and may also subscribe to receive email notifications. Email notifications are sent for every posted change, status update, or newly scheduled maintenance window. These emails contain the same information as that available on the dashboard.

12. Business Continuity and Disaster Recovery. Throughout the Service Term Tealium will maintain a commercially reasonable and industry standard business continuity and disaster recovery plan designed, implemented and tested to guard the Tealium systems against performance failures and to return the Tealium systems to full functionality as soon as reasonably practicable in the event of performance failures including, without limitation, those arising from an event of Force Majeure.

Tealium Acceptable Use Policy “AUP”

This Acceptable Use Policy (“AUP”) is incorporated into, and made a part of, the Master Services Agreement (MSA), Terms of Service or Service Order that references this AUP Addendum, and constitutes a part of the MSA between Tealium and Customer.

Acceptable Use Policy (this "**Policy**") describes prohibited uses of the Services. The examples described in this Policy are not exhaustive. If you violate the Policy or authorize or help others to do so, Tealium may suspend or terminate your use of the Services.

1. No Illegal, Harmful, or Offensive Use or Content

You may not use, or encourage, promote, facilitate or instruct others to use, the Services for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive. Prohibited activities or content include:

Illegal Activities. Any illegal activities, including collecting or processing PII without necessary consents, advertising, transmitting, or otherwise making available illegal gambling sites or services or disseminating, promoting or facilitating child pornography.

Harmful or Fraudulent Activities. Activities that may be harmful to others, our operations or reputation, including offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, ponzi, and pyramid schemes, phishing, or pharming), or engaging in other deceptive practices.

Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others.

Offensive Content. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.

Harmful Content. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots or other harmful or Malicious Code.

2. No Security Violations

You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "**System**"). Prohibited activities include:

Unauthorized Access. Accessing or using any System without permission.

Interception. Monitoring of data or traffic on a System without permission.

3. No Network Abuse

You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include:

Monitoring or Crawling. Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.

Intentional Interference. Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.

Avoiding System Restrictions. Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

4. No E-Mail or Other Message Abuse

You will not use the Services or any System to facilitate the distribution, publishing, or sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (e.g. "spam"), in violation of any law or regulation.

5. Our Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Services. We may: (i) Investigate violations of this Policy or misuse of the Services; or (ii) remove, disable access to, or modify any content or resource that violates this Policy or any other agreement we have with you for use of the Services.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information and Customer Data. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

6. Reporting of Violations of this Policy

If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this Policy, please contact us at legal@tealium.com

DATA SECURITY STATEMENT (DSS)

This Data Security Statement ("DSS") is incorporated into, and made a part of, the MSA between Tealium and Customer.

1. General.

1.2 Tealium will implement and maintain logical and physical security procedures with respect to its access, use, and possession of Customer Data ("Processes") that are designed to provide appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access of Customer Data at least equal to Industry Standards, but which in no event are less protective than the specific requirements of this DSS. Tealium will regularly re-evaluate and modify its security standards as Industry Standards evolve, new technologies emerge or new threats are identified. Unless otherwise agreed, all Customer Data Processing shall be in a multi-tenant environment with logical segmentation controls.

1.3 Tealium's data centers are owned and operated by Amazon Web Services Inc. ("AWS"). Details of AWS' security standards and programs are available at https://aws.amazon.com/security/.

2. Definitions.

"Computing Equipment" means desktop, laptop or notebook computers, mobile devices (e.g. cell phones or tablets) and any other devices used for computing functions.

"Dynamic Application Security Testing" or **"DAST"** means a security test of an application designed to detect conditions indicative of a security vulnerability in an application as it runs in a production environment, or in a test environment representative of the production environment in which such application will run.

"Encryption" means the process of using an algorithm to transform data into coded information in order to protect the confidentiality of the data.

"Firewall" means an integrated collection of security measures used to prevent unauthorized electronic access to the Tealium Network.

"Industry Standards" means customs and practices followed by, and representing the degree of skill, care, prudence and foresight expected from, leading providers of the types of services that are the subject matter of the MSA.

"Intrusion Detection System" or **"IDS"** means a method or system of reviewing system logs and processes in near real-time and escalating identified patterns of behavior that indicate an intrusion is occurring or is likely to occur soon without unreasonable delay.

"Least Privilege" means that, every module in a particular computing environment (such as a process, a user or a program) may only access the information and resources that are necessary for its legitimate purpose.

"Malicious Code" means any back door, virus, Trojan horse, worm or other software routines or equipment components) that are designed to disrupt, modify, delete, or otherwise harm software, equipment or data, to impede the operation of systems.

"Manual Penetration Testing" or **"PenTest"** means a manual security test of an application, executed by a combination of automated tools, a qualified tester or qualified third-party.

"Multifactor Authentication" means authentication using at least two (2) of the following factors:

“Something you know” such as a password, “Something you have” such as a token, or “Something you are” such as a biometric reading.

“Processing” or **“Process”** means any operation or set of operations which is performed on Customer 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.

“Removable Media” means portable or removable hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, memory cards (e.g., Secure Digital (SD), Memory Sticks (MS), CompactFlash (CF), SmartMedia (SM), MultiMediaCard (MMC), and xD-Picture Card (xD)), and magnetic tape.

“Secure Software Development Lifecycle Methodology” or **“SDLC”** means a documented process for planning, creating, testing, and deploying an information system that requires information security engagement, particularly with respect to the design, test, and deployment stages.

“Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data, but does not include any Unsuccessful Security Incident.

“Separation of Duties” means dividing roles and responsibilities so that a single individual cannot subvert the security controls of a critical process

“Static Application Security Test” or “SAST” means a security test of an application’s source code designed to detect conditions indicative of a security vulnerability in an application’s code.

“Tealium Facilities” or **“Facilities”** means all locations where Tealium personnel work and use Tealium Network and/or where Customer Data is Processed.

“Tealium Network” means the data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within the control of Tealium or its sub-processors and are used to provide the Services.

“Threat Model” means a process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker’s point of view. The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker’s profile, the most likely attack vectors, and the assets most desired by an attacker.

“Unsuccessful Security Incident” means an unsuccessful attempt or activity that does not compromise the security of Customer Data, including (without limitation) pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

“Root Cause Analysis” means a principle-based, systems approach for the identification of the underlying causes associated with a security event, including a Security Incident. Incident Management and Security Incident Notification.

3. Incident Management and Security Incident Notification.

3.1 Incident Management. Tealium maintains a documented incident management policy and process to detect security events, and which provides coordinated response to threats and Customer notification. The process includes a Root Cause Analysis with identified issues tracked to remediation, and evaluation and implementation of actions to prevent recurrence.

3.2 Security Incident Notification & Remediation. In the event of a Security Incident, Tealium will notify Customer and remediate the Security Incident in the manner set forth below:

3.2.1 Notification if Tealium becomes aware of a Security Incident, Tealium will without undue delay and, where feasible, no later than 48 hours after having become aware of it, notify Customer of the Security Incident. Where the notification to Customer is not made within 48 hours, it shall be accompanied by reasons for the delay.

The notification referred to above shall at least:

(1) describe the nature of the Security Incident;

(2) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; and

(3) describe the measures taken or proposed to be taken by Tealium to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Tealium shall document any Security Incidents, comprising the facts relating to the Security Incident, its effects and the remedial action taken. That documentation shall enable Customer to verify compliance with this Section.

3.2.2 Root Cause Analysis. Tealium will promptly initiate and pursue to completion as quickly as possible a Root Cause Analysis.

3.2.3 Remediation. Tealium will promptly implement measures necessary to restore the security of Customer Data and Tealium Network. If such measures include temporarily restricting access to any information or Tealium Network in order to mitigate risks associated with further compromise, Tealium will promptly notify Customer of the restricted access, in advance of such restriction when reasonably possible. Tealium will cooperate with Customer to identify any additional steps required of Tealium to address the Security Incident and mitigate its effects.

3.2.4 Any Unsuccessful Security Incident will not be subject to this Section.

4. Independent Risk Assessments and Audits.

4.1 Service Organization Reports. Tealium will undertake at least annually, at its expense, an audit in accordance with ISO/IEC 27001, ISO/IEC 27018 and with the System and Organization Controls (SOC) Report under the SSAE-18 or their successor standard(s), covering controls related to Tealium's provision of the Services as a services organization, the scope of which will be in accordance with Industry Standard practice.

4.2 Third-Party/Subcontractor Agreements. Tealium will conduct a detailed risk assessment on its service providers who process Customer Data with results documented and made available to Customer upon request.

4.3 Security Testing. Tealium will, at least annually, engage, at its expense, a third-party service provider to perform Manual Penetration Testing of Tealium Network related to the provision of Services. The method of test scoring and issue ratings will follow Industry Standard practices, such as the latest Common Vulnerability Scoring System ("CVSS") published by the US National Institute of Standards and Technology ("NIST"). Tealium will remedy any validated findings deemed material (critical, high or medium risk) in a timely manner following such findings**.**

4.4 AWS Audits. Tealium's storage and infrastructure provider, AWS, is certified under ISO 27001 and has agreed to maintain an information security program for the Services that complies with the ISO 27001 standards or such other alternative standards as are substantially equivalent to ISO 27001 for the establishment, implementation, control, and improvement of the security standards applicable to AWS. AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which Tealium provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards which are substantially equivalent to ISO 27001; and (c) will be performed by independent third-party security professionals.

4.5 Customer Audits. Customer may conduct, either itself or through a third party independent contractor selected by Customer at Customer's expense, an on-site audit and review of the Tealium Network and procedures used in connection with the Services. Such audit and review shall be conducted no more frequently than one time per year, with 30 days' advance notice unless required to comply with applicable laws and regulations or following a Security Incident affecting Customer Data. Any audits described in this Section shall be conducted during reasonable times, shall be of reasonable duration, shall not unreasonably interfere with Tealium's day-to-day operations, and be conducted in accordance with appropriate technical and confidentiality restrictions. In the event that Customer conducts an audit through a third-party independent contractor, such independent contractor shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the MSA to protect Tealium's Confidential Information. Customer must promptly provide Tealium with information and reports regarding any non-compliance discovered during the course of an audit.

5. Security Function.

5.1 Security Officer. Tealium will designate a point of contact to coordinate the continued security of all Customer Data and Tealium Network**.** The Tealium Security Officer can be contacted at infosec@tealium.com.

5.2 Training. In addition to any training obligations in the MSA, Tealium will, at least annually, provide all Tealium personnel with responsibilities related to the Services with appropriate ongoing training regarding Tealium's processes for which compliance is required under the MSA, including, without limitation, procedures to verify all Tealium personnel promptly report actual and/or suspected Security Incidents. All personnel involved in any part of Tealium's SDLC are required to receive application security training. Tealium will retain documentation that such training has been completed.

6. Data Management. The following will apply to the Tealium Network Processing Customer Data:

6.1 Data Access. Customer Data will be accessible only by Tealium personnel whose responsibilities require such access and follow the principle of Least Privilege. Tealium will use Industry Standard authentication practices and secure all communications involving Customer Data.

6.2 Encryption of Information. Tealium will use Industry Standard Encryption techniques for Customer Data being stored, processed, or transmitted by Tealium in the course of providing Services. Such techniques will require (a) key length of 128 bits or more for symmetric Encryption and (b) key length of 2048 bits or more for asymmetric Encryption.

6.3 Cryptographic Key Management. Tealium will securely manage cryptographic keys and maintain documented Industry Standard control requirements and procedures. If Tealium uses public key infrastructure ("PKI"), Tealium will protect such PKI by 'hardening' the underlying operating system(s) to reasonably protect against unauthorized access. For third party systems, Tealium will use vendor-recommended hardening guidelines. For Tealium's systems, Tealium will utilize Industry Standard hardening guidelines, such as checklists provided by the Center for Internet Security®.

6.4 Removable Media. Tealium does not use Removable Media in providing the Services.

6.5 Data Disposal and Servicing. In the event that any hardware, storage media, or documents containing Customer Data must be disposed of or transported for servicing, then:

6.5.1 Tealium will maintain documented policies and procedures concerning data disposal that include provisions to maintain chain of custody; and

6.5.2 Tealium will render such Customer Data inaccessible, cleaned, or scrubbed from such hardware and/or media using methods at least as protective as the minimum sanitization recommendations outlined by NIST SP 800-88 Rev.1 (or successor standard).

6.6 Data Transmission. When Customer Data is transferred by Tealium across the Internet, or other public or shared network, Tealium will protect such data using appropriate cryptography as required by Section 6(b) of this DSS.

6.7 Data Resiliency. Utilize Industry Standard safeguards to provide resiliency of Customer Data. Resiliency will be achieved by use of services or methods such as, but not limited to, database backups, file backups, server backups, or managed highly available services, fault tolerant data storage or managed database services. Any Tealium storage or retention of backup files will be subject to all terms of this DSS. Tealium will test data resiliency periodically to protect the integrity and availability of Customer Data.

7. Physical Security – Facilities. Tealium Facilities will be protected by perimeter security such as barrier access controls (e.g., the use of entry badges) that provide a physical environment secure from unauthorized access, damage, and interference. At a minimum, all Tealium Facilities are required to have the following security related characteristics:

7.1 Tealium will document, implement and maintain administrative and physical security policies, including, without limitation, a “clean desk” policy.

7.2 Tealium will install closed circuit television (“CCTV”) systems and CCTV recording systems to monitor and record access to Tealium Facilities. Logs must be retained for at least one (1) year.

7.3 All Tealium personnel will be issued and will display to gain access an identification badge allowing electronic verification of bearer’s identity.

7.4 Each location will maintain procedures for validating visitor identity and authorization to enter the premises, including but not limited to, an identification check, issuance of an identification badge or escorted, validation of host identity, purpose of visit, and recorded entry.

8.Tealium Network Security.

8.1 Asset Inventory. Tealium will maintain a comprehensive inventory of its current Tealium Network components, hardware, and software (including version numbers and physical locations) to ensure only authorized and supported components Process Customer Data. Tealium will, at least annually, review and update its system component inventory.

8.2 Tealium Network Security. All data entering the Tealium Network from any external source (including, without limitation, the Internet), must pass through Firewalls to enforce secure connections between internal Tealium Network and external sources. Such Firewalls will explicitly deny all data other than the minimum required to support Tealium business operations.

8.3 Intrusion Detection System. Intrusion Detection Systems will run on individual hosts or devices on the Tealium Network to monitor the inbound and outbound connections and will alert administrators if suspicious activity is detected. IDS will monitor file integrity of the Tealium Network and, if critical system files are modified, the IDS will log the event in Tealium's security information and event management systems.

8.4 Scan Incoming Files. Tealium will use Industry Standard security tools including IDS to scan incoming files on any servers on which Customer Data may be Processed**.**

8.5 Protect Against Malicious Code. Tealium will implement appropriate technical measures designed to protect against transferring Malicious Code to Customer systems via email or other electronic transmission. Anti-malware tools are deployed on all Tealium Network providing or supporting Services to Customer, and such tools are updated to provide protection against current threats.

8.6 Vulnerability Management. Tealium will have a documented process to identify and remediate security vulnerabilities affecting Tealium Network containing Customer Data. Tealium will remediate any identified security vulnerabilities within a reasonable amount of time.

8.7 Electronic Communications. All electronic communications related to the provision of Services, including instant messaging and email services, will be protected by Industry Standard processes and technical controls.

9. Change and Patch Management.

9.1 Change Management. Changes to applications, any part of the Tealium's information technology infrastructure, Tealium Network will be tested, reviewed, and applied using a documented change management process and adhere to the principle of Separation of Duties.

9.2 Emergency Changes. Tealium uses an emergency change approval process to implement changes and fixes to Tealium Network and Services on an accelerated basis when necessary. Tealium will notify Customer in advance if any such emergency changes could affect the functionality of the Services during normal business hours.

9.3 Software Updates. Tealium will:

9.3.1 use anti-malware and other security software in support of the delivery of Services;

9.3.2 use only supported versions of software required for the delivery of Services; and

9.3.3 where Services may be impacted, implement emergency software fixes within a reasonable time, unless in Tealium's reasonable opinion this introduces higher business risks. All changes are undertaken in accordance with Tealium's approved change management process.

10. Logical Access Controls.

10.1 User Authentication: Tealium will implement processes designed to authenticate the identity of all users through the following means**:**

10.1.1 User ID. Access to applications containing Customer Data must be traceable to one (1) user. Shared accounts accessing Customer Data are prohibited by Tealium.

10.1.2 Passwords. Each user on Tealium Network will use a unique password to access applications containing Customer Data. Passwords will be at least eight (8) alphanumeric characters. The use of passwords that are easily discerned will be avoided (i.e., passwords matching or containing User ID, users' birthdays, street addresses, children's names, etc.). Tealium will require users to use Multifactor Authentication for access to applications or systems containing Customer Data**.**

10.1.3 Multifactor Authentication. Multifactor Authentication will be required for entry on all Tealium Network access points designed to restrict entry to authorized personnel.

10.2 Session Configuration. Sessions will be configured to timeout after a maximum of 60 minutes of user inactivity. Re-authentication will be required after such timeouts or periods of inactivity.

10.3 Unsuccessful Logon Attempts. The number of unsuccessful logon attempts will be limited to a maximum of five (5). User accounts will be locked for at least ten (10) minutes after the maximum number of permitted unsuccessful logon attempts is exceeded.

10.4 Remote Access. Remote access to Tealium Network containing Customer Data will be restricted to authorized users, will require Multifactor Authentication and will be logged for review.

10.5 Deactivation. User IDs for Tealium personnel with access to Customer Data will be deactivated immediately upon changes in job responsibilities that render such access unnecessary or termination of employment.

10.6 Privileged Access. Tealium will use Industry Standard methods to provide that:

10.6.1 Users with access to Tealium Network containing Customer Data will be granted the minimum amount of privileges necessary;

10.6.2 Privileged access will be restricted to authorized individual users and non-repudiation will be maintained;

10.6.3 Privileged user accounts will be used exclusively for privileged operational use and not for business as usual activities;

10.6.4 Developers will not receive privileged access to production environments; and

10.6.5 All privileged access will require Multifactor Authentication.

11. Logging & Monitoring.

11.1 Tealium Network Monitoring. Tealium will actively monitor the Tealium Networks supporting the Services where Customer Data is Processed (using Industry Standard IDS) to detect deviation from access control policies and actual or attempted intrusions or other unauthorized acts.

11.2 Event Logging. For Tealium Networks Processing Customer Data Tealium will:

11.2.1 maintain logs of key events, including access events, that may reasonably affect the confidentiality, integrity, and availability of the Services to Customer and that may assist in the identification or investigation of Security Incidents occurring on Tealium Network. Copies of such logs will be made available to Customer upon written request;

11.2.2 protect logs against modification or deletion. Tealium's Information Security team will review the logs on a regular basis; and

11.2.3 retain logs for at least twelve (12) months.

12. Software Security Assurance.

12.1 Development Methodology. For software used in the course of providing Services, Tealium will:

12.1.1 carry out in-house development activities in accordance with a documented SDLC policy, which will be shared with Customer upon request;

12.1.2 deploy new applications and changes to existing applications to the live production environment strictly in accordance with the SDLC policy; and

12.1.3 maintain documented SDLC practices including the definition, testing, and deployment of security requirements.

12.2 Development Environments. For software used in the course of providing the Services, Tealium will:

12.2.1 perform system development and testing in distinct environments segregated from the production environment and protected against unauthorized disclosure of Customer Data; and

12.2.2 not use Customer Data within non-production environments without Customer's prior written approval and without the documented controls required to protect such information.

12.3 Capacity and Performance Planning. Tealium will use capacity and performance planning practices and/or processes designed to minimize the likelihood and impact of Tealium Networks failures or outages. Tealium will review capacity plans and performance monitoring information on a regular basis.

12.4 Testing Process. Tealium will in the course of providing Services:

12.4.1 provide that applications undergo a formal code review process. Upon Customer's written request, Tealium will provide evidence of this formal process to Customer.

12.4.2 provide that applications undergo a quarterly Dynamic Application Security Test (DAST) and Static Application Security Test (SAST). The method of test scoring and issue ratings will follow Industry Standard practice, such as the latest Common Vulnerability Scoring System (CVSS) published by NIST. Upon written request, Tealium will provide Customer the results of such testing with respect to any material findings, and any applicable remediation activities in the form of an executive summary attestation letter containing the testing performed, the date, and a summary of the results.

12.4.3 provide that applications undergo a Threat Model analysis at least annually. Tealium has a process to formally report the results of the Threat Model and to remediate material findings. Upon request, Tealium will evidence this activity by sharing the Threat Model executive summary.

13. Data Center Controls.

13.1 Base Requirements. Any data center supporting the Services will possess the following minimum requirements:

13.1.1 Adequate physical security and access controls as set forth in Sections 6 and 7 of this DSS;

13.1.2 Professional HVAC & environmental controls;

13.1.3 Professional network/cabling environment;

13.1.4 Professional fire detection/suppression capability; and

13.1.5 A comprehensive business continuity plan.

14. Business Continuity Plan (BCP).

14.1 BCP Planning and Testing

14.1.1 Tealium's plan capabilities will include a data resiliency system containing all hardware, software, communications equipment, and current copies of data and files necessary to perform Tealium's obligations under the MSA; and

14.1.2 Tealium will maintain processes for timely recovery of Services at Tealium-owned and/or hosted data centers.

14.2 BCP Plan. The plan will address the following additional standards or equivalent in all material respects:

14.2.1 The plan will reflect regulatory requirements and Industry Standards;

14.2.2 The relocation of affected Tealium personnel to one or more alternate sites and the reallocation of work to other locations that perform similar functions until such relocation is effected;

14.2.3 A full business impact analysis of the expected impacts that Tealium believes are likely to arise in the event of a disruption to or loss of Tealium's normal operations, systems and processes;

14.2.4 The establishment and maintenance of alternate sites and systems, the capacity of which will be no less than the primary sites and systems that Tealium uses to provide the Services and perform its other obligations under this MSA;

14.2.5 A description of the recovery process to be implemented following the occurrence of a disaster. The description will detail the contingency arrangements in place to ensure recovery of Tealium's operations, systems and processes and also the key personnel, resources, services and actions necessary to ensure that business continuity is maintained; and

14.2.6 A schedule of the objective times by which Tealium's operations, systems and processes will be recovered following the occurrence of a disaster. Tealium agrees that its recovery processes and BCP plans provide a Recovery Time Objective (RTO) of four (4) hours and a Recovery Point Objective (RPO) of 24 hours.

14.3 Distinct Plans. If distinct plans apply to specific Tealium locations, the plans for each location from which a material part of the Services are performed by Tealium will be tested at least annually against a comprehensive scenario and the results made known to senior management of Tealium.

14.4 Notification. In case of a disaster that Tealium reasonably believes will impact its ability to perform its obligations or affect the Services under the MSA, Tealium will promptly notify Customer of such disaster. Such notification will, as soon as such details are known, describe:

14.4.1 The disaster in question and how it was detected;

14.4.2 The impact the disaster is likely to have on the Services;

14.4.3 The alternative operating strategies and the back-up systems Tealium will utilize and the timetable for their utilization; and

14.4.4 The expected timeframe in which the disaster will be resolved and Tealium expects to return to business as usual.

14.5 Subcontractors. Tealium will require its subcontractors that perform any part of the Services (other than auxiliary services that facilitate the Services (e.g., document warehousing and retrieval, print services, etc.)) to have in place and maintain a commercially reasonable business continuity program that complies with regulatory and industry best practices. Tealium's use of subcontractors does not diminish its obligation to provide business continuity capabilities as described above for all Services provided under the MSA, regardless of their origin and regardless of notice to Customer.