Tealium の顧客保護のパッケージ (「CPP」)に関する FAQ

当 FAQ をご覧いただきありがとうございます。当 FAQ は、Tealium の顧客保護のパッケージ (「CPP」) に関する便利な情報を提供するためにデザインされました。CPP は、基本サービス契約書（または MSA）の一部として Tealium がすべてのお客様に提供する保護とその達成のための努力を記載する文書です。 CPP をお読みいただきながら、当 FAQ によって有用な情報を提供できれば幸いです。当 FAQ は情報提供のみを目的とし、当事者が考慮の対象とする契約の一部を成すものではありません。 DSS および DPA のすべての責任に関する問題は、TOS に記載があります。

CPP の構成

CPP は 4 つの文書からなっています。:
サービス水準契約書(「SLA」) は、すべての本サービスを通して Tealium のサポートが利用可能であることを約束するための Tealium の努力、 極めて稀ではありますがその努力が達成されなかった場合のお客様の救済、また Tealium がどのようにサポートに関する問題に対応するかが含まれます。
承認利用規定（「AUP」）には、本サービスの利用に関して、インターネットを悪用しないための標準的なガイドラインが含まれます。
データセキュリティー規定 （「DSS」）には、顧客データを保護するため Tealium が形式化した組織的および技術的セキュリティー保護対策が含まれます。
データ処理契約書（「DPA」）は、適用されるプライバシー保護法および規律に則った Tealium のデータ処理の方針を反映します。

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 Master Services Agreement, or 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 and DPA are addressed in the TOS.

What is the structure of the CPP?

Our CPP is made up of four 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.
The **Data Processing Agreement ("DPA")** reflects our data processing policies in compliance with applicable privacy laws and regulations.

The 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

SLA

我々の SLA は、すべての本サービスが 99.9%の確率でご利用いただける業界最高峰レベルを誇っています。 Tealium はまた、お客様にリアルタイムのステータスおよびメンテナンスや緊急停止をお知らせするウェブサイトを提供します。Tealium は、極めて稀ではありますが、ご利用できない状態になった場合の救済、また長期に及ぶ停止状態になった場合の契約解除の権利を提供します。 SLA はまた、サポートに問題があった際の対応、また緊急時の連絡方法に関する情報を含みます。

SLA がすべての商品を通じて提供されていること、またマルチテナントの SaaS サービスを提供していることから、ここのお客様に合わせて SLA を変更することはできません。我々は SLA がお客様のすべての問題を網羅していると確信しています。

AUP

AUP は Amazon Web Services (「AWS」) から受け継がれたポリシーであり、インターネット上での本サービスの利用に関する制限が記載されています。その制限には、SPAM、ポルノ、およびフィッシングに関するものが含まれます。本サービスは AWS に準拠しているため、すべてのお客様に当ポリシーに同意していただく必要がございます。

AUP は既存のポリシーであり、一切の変更に同意することはできません。

DSS

DSS は本サービスに送信されるすべての電子データと情報に関する内容が示されます。すべての電子データと情報には、本サービスのご利用から派生した拡張および出力（これを「顧客データ」と呼びます）が含まれます。DSS は顧客データのためのセキュリティープログラムが示されます。これはすべてのお客様に平等に適用されま

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.

The 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.

The 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

す。サポートのリクエストなど、特別な目的のためにお客様からアクセスを許可されない限り、顧客データにアクセスすることはありません。我々にアクセスを許可された場合は、お客様にアクセスの範囲を設定していただき、またいつでもその追加アクセスを停止していただけます。 お客様のデータ保護に関する文書ではなく、我々の DSS を使用するのには、以下の理由があります。 **1.** 本サービスは「皆のための一つの」モデルを使ってお客様に提供されます。つまり、同じ本サービスがすべてのお客様に提供されることになります。ですので、あるお客様（またはそのデータ）に対し、別のお客様とは異なる方法でのサービス提供を可能にする「カスタマイズ」されたサービスは提供しておりません。実装やサポートなどの補助的サービスもまた、同等の方法ですべてのお客様に提供されます。 **2.** Tealium は、顧客データの内容を実際に見ることができません。Tealium が見ることのできないデータの内容には、データの匿名性、個人情報または秘密情報か否か、アカウント内の顧客データの特定の保存または構成の方法、 誰にデータが送られたか、データ処理の目的、処理の目的や量、データ送信先である第三者、およびあるデータまたは処理方法がデータの対象者にリスクを課すか否か（またはその程度）が含まれます。結果として、データのどの部分が業界特有の、または国特有の規定に準拠すべきなのかを判断するために必要な情報も、我々が見ることはできません。 **3.** Tealium の統一された厳格なセキュ	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

リティー制御は、すべてのお客様にとって同等に利益をもたらします。同じ本サービスがすべてのお客様に提供されているため、皆様に共有された技術的および組織的なセキュリティー保護をどなたでも受けることができます。我々のプライベートなクラウド環境下で提供されるサービスによって、 米国 HIPAA 規定準拠の認証など、技術的および組織的セキュリティー保護対策が強化されています。

DSS はすべての商品とお客様に同様に提供されているため、個々のお客様のためにDSS を変更することはできません。我々は DSS がお客様のすべてのセキュリティーに関する問題を網羅していると確信しています。カスタマイズされたサービスは提供できませんが、お客様のアカウントの地理的なホストロケーションをお選びいただけます（MSA に詳細を定義）。

データ処理補足条項(「DPA」)

DPA は、お客様が本サービスにアップデートするすべての個人データ（顧客データの一部）をカバーします。DPA は本サービスで処理される個人データのプライバシー保護対策を反映し、適用されるデータ保護法に基づく各当事者の特定の義務を示します。DPA はまた、欧州連合規制 2016/679 (「GDPR」)、1988 年オーストラリア連邦プライバシー法 (Cth.)、およびカリフォルニア州消費者プライバシー保護法 §§ 1798.100 修正(「CCPA」)の追加条件に言及しています。我々は、上記にある DSS を使用するのと同じ理由で、お客様のデータ処理に関する契約書ではなく DPA を使用しています。

DPA は、 GDPR 28(3)および 46 の条項を含む、適用法の条件を満たすために特別に作成されました。 我々はお客様の顧客デ

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.

The Data Processing Addendum ("DPA")

The DPA covers all personal data (a subset of Customer Data) you upload to our Services. Our DPA reflects our privacy program for personal data we process in the Services and addresses certain obligations each respective party has under applicable data protection laws. Our DPA also addresses additional requirements of the European Union's Regulation 2016/679 ("GDPR"), the Australian Privacy Act 1988 (Cth.), and the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. as amended ("CCPA"). We use our DPA instead of using our customers' data processing agreements for the same reasons that we use our DSS as stated above.

We drafted our DPA specifically to satisfy the requirements of applicable data protection laws, including those of Articles 28(3) and 46 of the GDPR. Because we do not have access or visibility to your Customer Data, you play an important role in how some of the requirements of GDPR

ータにアクセスできず、またその内容を見ることができないため、GDPR の条件が満たされているかの判断において、お客様が重要な役割を担っています。例えば、我々が、包括的な技術的かつ組織的対策（多くの監査の実行やサティフィケーションの提供を含む）を行なっていることはご存知の通りですが、本サービスがお客様の特定の使用に適しているか、また本サービスがお客様の特定の個人データに対する条件を満たすかどうかを判断するためには、最終的にお客様が不可欠な役割を果たすことになります。 同様に、もし EU からのデータ送信が GDPR の範疇にあると判断される場合、お客様にはその旨を我々にお知らせいただき、欧州標準的契約条項など、かかるデータ送信に関する代替条件を提供させていただけるようご協力が必要となります。 DPA はすべての商品とお客様に同様に提供されているため、個々のお客様のために DPA を変更することはできません。我々は DPA がお客様のすべてのセキュリティーに関する問題（適用法の準拠の可否を含む）を網羅していると確信しています。	are satisfied. For example, we are transparent about the comprehensive technical and organizational measures we implement, including the many audits and certifications we undergo and make available to you, but ultimately you play an indispensable role in determining whether the Services are appropriate for your specific use case and whether or not our Services meet requirements applicable to your particular personal data. Similarly, we rely on you to let us know if you believe you are in scope for the GDPR in terms of the data transfers from the EU and we can provide supplementary terms for those transfers such as the European Standard Contractual Clauses. Since our DPA is being provided uniformly across all our products and customers, we are unable to alter our DPA for one Customer. We are confident that our DPA will more than address all our Customer's privacy issues, including addressing compliance under applicable laws.

サービス水準契約書（SLA）

本サービス水準契約書(「SLA」)は、**基本サービス契約書**(MSA)、本サービス条件、または本 SLA 補足規定を参照する本サービス注文書に組み込まれまたその一部となり、Tealium と顧客間の MSA の一部を構成する（かかる本サービス注文書に示される通り）。

1. **定義。** 次に定義された語句は本 SLA 補足規定にて使用される。:

「利用可能な」または「利用可能性」とは、本サービスが機能する状態であり、また（API、タグ、 HTTP リクエスト/応答などの）プログラム、または特定の本サービスに適用可能なユーザーインターフェースを通じて本サービスへのアクセスが可能な状態をさす。 本配信ネットワークのパフォーマンスにおいてのみ、「利用可能な」とは、本配信ネットワーク（以下定義）のサーバーがライブラリ（以下定義）へのリクエストに応答している状態をさす。

「本配信ネットワーク」とは、 Tealium JavaScript ファイルまたはその他の本サービスに関連したファイル（以下「ライブラリ」という）を提供するための所定の本サービスに関連して使用されたコンテンツの配信ネットワーク・サービス・プロバイダをいう。

「**不可抗力**」とは、当事者が合理的に制御できない事由をいい、天候、公共施設もしくは通信サービス（インターネットへのアクセスを含む）が利用できないこと、市民による妨害、内乱、行政当局もしくは軍当局の行動、または天災を含むがこれに限らない。

「**インシデント**」とは、P1, P2 または P3 の本サービスの問題をいう。

「**月次加入額**」とは、本サービス期間の本サービスの契約金額を本サービス期間の月数で除算した金額（実装、管理および専門サービスの料金、また追加利用料金を除く）をいう。

「**月次使用可能時間率**」とは、ある暦月における本サービスが利用可能な時間の割合をいう。「利用可能な」または「利用可能」とは、本サービスが機能し利用可能な状態であり、また（API、タグ、 HTTP リクエスト/応答などの）プログラム、または特定の本サービスに適用可能なユーザーインターフェースを通じて本サービスへのアクセスが可能な状態をさす。 本配信ネットワークのパフォーマンスにおいてのみ、「利用可能な」と

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 Service.

"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

は、本配信ネットワークのサーバーがライブラリーへのリクエストに応答している状態をいう。

「優先順位 1」または「P1」インシデントとは、Tealium の本サービスが顧客のデジタルプロパティーに破滅的な影響を持つ重大欠陥をいう。例えば、Tealium のタグが原因でデジタルプロパティーが機能しない、デプロイされたライブラリがデリバリーネットワークに送られず、主要コンテンツが表示されない、本サービスが広範囲で停止、またはアクセス不可になる、デプロイが元のバージョンに「巻き戻り」、デプロイ以前の問題が解決されないなど。不具合は顧客の顧客データの収集力に影響を与える。

「優先順位 2」または「P2」インシデントとは、本サービスは機能しているものの顧客が本サービスの物質部分を使用できない、物質的欠陥をいう。例えば、デリバリーネットワークがライブラリを継続的に送信するが本サービスの配信機能が利用不可になる、また物質要素が利用不可になるあるいは誤動作が起きるが回避策がないなど。

「優先順位 3」または「P3」インシデントとは、本サービスは機能するが、重要度の低いエラーまたはバグが、一つ以上の重要度の低い本サービスの機能に、意図された通り作動しない末梢的欠陥をもたらす状態をいう。例えば、拡張またはタグ内のバグで、回避可能なものなど。

「回答にかかる時間」とは、Tealium がインシデントを察知した、または顧客が Tealium にインシデントの通知をした時点から、Tealium がインシデントの通知を認め、インシデント解決のために解決策を講じるまでの時間をいう。

「本サービスクレジット」とは、以下定義された条件で計算される、顧客に発行する未来の請求書に対して Tealium が充当することができるクレジットをいう。

2. 本サービス使用可能性の誓約。Tealium は、いずれの月においても 99.9%以上の月次使用可能時間率で本サービスを利用可能にするように商業的に合理的な努力を払うものとする（以下「本サービスの誓約」という）。本サービスが本サービスの誓約を満たさない場合には、顧客は、以下で定める本サービスクレジットを受け取る資格を有する。

3. 本サービスクレジット。本サービスクレジットは、本サービスの誓約が以下のスケジュールに従って満たされなかった月の、特定の本サービスにかかる月次加入額の割合として計算される。Tealium は、将来の支払のみに本サービスクレジ

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,

ットを充当するものとする。顧客が MSA に基づきすべての本サービスに対して全額を前払いする場合は、MSA が満了するか更新されなければ、顧客は Tealium へ書面上の要請をすることで本サービスクレジットの分の返金を受け取る権利を有する。本サービスが本サービスの誓約を満たすことができなかった場合、顧客の単独のかつ唯一の救済は本 SLA の条件に従って本サービスクレジットを受け取ることである。本サービスクレジットは、その他の顧客のアカウントに移転または充当することはできない。

月次使用可能時間率が 99.9%を下回るが 99%以上であった場合は、本サービスクレジットは月次加入額の 10%に相当するものとする。

月次使用可能時間率が 99%を下回る場合は、本サービスクレジットは月次加入額の 20%に相当するものとする。

4. クレジットの要求および支払手続。 本サービスクレジットを受け取るために、顧客は、services@tealium.com に電子メールメッセージを送信して、要求書を提出しなければならない。クレジット受給の資格を満たすには、クレジットの要求が、（a）Tealium のある月における本サービスの誓約を満たさなかったことも証明する、合理的に詳細な機能停止状況のリストを含み、(b) 電子メールの本文に、顧客が経験したとする各インシデントの日付および時間を記載し、(c) 顧客が主張する機能停止を文書化し、Tealium がかかる機能停止を立証できる顧客の追加情報（サーバーのリクエストログなど）（当該ログの秘密情報または機密情報は、削除するか、またはアスタリスクに置き換えなければならない）を含み、(d) サービスの誓約が満たされなかった月の末日から 10 営業日以内に Tealium が受領しなければならない。クレジットを受け取るには、当セクション 4 に従って Tealium が単独で、顧客の主張する機能停止を認めることができることが条件となる。

5. SLA の除外。 本サービスの誓約は、（a）Tealium が合理的に制御できない要素（不可抗力事由、または本配信ネットワークの責任分界点を超えるインターネットへのアクセスの問題もしくは関連する問題を含む）によって生じるか、（b）顧客もしくは第三者の作為もしくは不作為に起因するか、（c）顧客の装置、ソフトウェアもしくは他の技術、および／もしくは第三者の装

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 Services Commitment does not apply to any Service 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

置、ソフトウェアもしくは他の技術（Tealium が直接管理する第三者の装置を除く）に起因するか、または（d）MSA に従って本配信ネットワークを使用する顧客の権利が停止し、終了したことから生じるか、(e) システムまたはネットワークのメンテナンスのために計画されたダウンタイムによる本サービスの利用停止または他の本配信ネットワークの性能の問題には適用されない。

6. 恒常的機能停止による契約解除の権利。上記のセクション 3 に示される本サービスクレジットの救済に加え、2 ヶ月連続で、または 4 ヶ月分（連続した 12 ヶ月の間いつでも）、月次使用可能時間率が 97%を下回る場合は、顧客は意図された通り機能しない本サービス欠陥による本サービス注文書を解約し、有効な解約日の後、影響のあった期間に対し事前に支払われた金額分の返金を受け取ることができる。かかる解約が有効となるためには、かかる解約の通知を、解約する権利が生じた月から Tealium が 30 日以内に受領しなければならない。

7. Tealium の技術上の回答にかかる時間および解決にかかる時間の目標タイムテーブル。 Tealium は以下の表に従ってインシデントに応答し、解決策を講じる。:

P1 重要度 – Tealium の回答にかかる時間は 2 時間である。Tealium は、インシデント修復のため 1 日 24 時間の（無休で）リソースを提供し、4 時間ごとに修復状況を報告する。

P2 重要度 – Tealium の回答にかかる時間は 4 時間である。Tealium は、インシデント修復のため少なくとも通常営業時間内中リソースを提供し、営業日ごとに修復状況を報告する。

P3 重要度- 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. の回答にかかる時間は 1 時間である。Tealium は、インシデント修復のため常営業時間内にリソースを提供し、修復状況は顧客が選択した担当アカウントマネージャーを通じて提供される。

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:

重要度の増加。インシデントの重要度は、顧客への影響の度合いを鑑みて、アカウントマネジャーの判断によって一つ上の重要度に上がることがある。	(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.
重要度の低下。以下の理由により、Tealium の判断でインシデントの重要度が下がることがある。	(c) A suitable workaround is provided, whether temporary or permanent, which reduces the impact of the issue to that of a lower severity category.
(a) 問題が再生できず、顧客への影響がなくなった時。	(d) Tealium determines Customer is not providing the required cooperation and access necessary to enable resolution of the issue.
(b) 顧客または Tealium の分析の結果、問題の重要度を下げるべきと判断された時。	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.
(c) 一時的、あるいは長期的に適切な回避策が提供され、下の重要度に相当するレベルまで問題が軽減された時。	**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.
(d) Tealium が、顧客が問題解決に必要な協力およびアクセスを提供しないと判断した時。	**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.
抜本的原因分析(「RCA」)。Tealium は、P1 インシデントが発覚してから 48 時間以内に内部 RCA を実施し、顧客の要請により、インシデント解決から 5 日以内に利用可能となる。	
Tealium 以外の商品; コネクター。コネクターに不具合があったとする通知を、Tealium がコネクターからのエラーメッセージを受けるか、またはその通知を顧客から受けた場合、Tealium は 5 営業日以内にかかるコネクターの不具合について調査を行う。 Tealium がコネクターを作成したところで、Tealium は商業的に道理的な努力を払い、第三者のコネクターの提供元と協力してコネクターの不具合を修復し、また合理的に適切な時間内に第三者の提供元による解決策またはパッチを行うものとする。この条項に基づく一切の問題は利用可能性から特別に除外される。	
8. カスタマーサクセスサポートサービス。Tealium は、P1 インシデントに関しては無休で（24×7）、P2 インシデントに関しては 営業時間内フルタイムで、サポートサービスを提供する。P3 およびその他のサポートサービスは、Tealium の通常営業時間（現地時間で月曜から金曜、8:00am – 6:00pm、祝日を除く）に利用できる。Tealium のオフィスはカリフォルニア州サン	

ディエゴ（太平洋時間）、およびイギリスのリーディング（グリニッジ平均時）にある。Tealiumのサポートホットラインの番号は+1.877.443.5276まで。カスタマーサクセスサポートサービスチームは、Tealiumのサポートポータル（https://support.tealiumiq.com/）からも連絡することができる。ある本サービスのサポートサービスの詳しい内容は本サービス注文書に示される。

9. Tealium チーム。 Tealiumは、各本サービス注文書の期間中、顧客と連絡を取り合い本サービスの適切な実行と作動を確かなものにするため、一人または複数の従業員を配属する。本サービスの初期デプロイ期間中、顧客はSOWに示されるサポートチームを割り当てられる。 アカウントマネージャーは、デプロイ後の主要コンタクトとして、顧客とともに、顧客が本サービス利用による利益を確信し、また相互の協働を促すために戦術的、戦略的なアドバイスを提供する。アカウントマネージャーはまた、推奨されるトレーニングの機会を紹介し、技術上のサポートが必要な時に連絡を取り次ぐ。

10. システムヘルスモニタリング。Tealiumは、Tealiumヘルスアンドステータスダッシュボードを提供し（https://status.tealium.com）、顧客はこれにアクセスすることができる。Tealiumは、顧客に適切なAPIインターフェイスを提供し、ヘルスアンドステータスダッシュボードに直接アクセスできるようサポートする。このダッシュボードは「緑」「黄色」「赤」のシステムを使う。緑はシステムが通常通り機能していることを示し、赤は使用中のTealiumのシステムの一部が重大な影響を受けていることを示すのに使われる。黄色は本サービスの機能低下が発生しているが、本サービスの機能停止を招く問題であると判断されるには至っていないことを示すために使われる。黄色は、赤のステータスにあった問題が正され、引き続き安定性をチェックされている状況を示すためにも使われる。計画的メンテナンスは、10日前に通知がある。本ページには緊急メンテナンスの通知も示され、必要とされる変更の性質によってなるべく早く事前に通知される。緊急変更通知の後にはインシデント経過が通知される。

11. 通知サービス。顧客はヘルスアンドステータスダッシュボードを直接利用し、またEmail通知を受け取ることができる。Email通知はすべての変更、ステータス更新、あるいは新しくスケジュ

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

ールされたメンテナンスウィンドウがある度に送信される。これらの Email はダッシュボードで閲覧可能な情報と同じものが送られる。 **12. 事業継続および災害復旧。**本サービス期間中、Tealium は、パフォーマンス不全から Tealium のシステムを防御し、また不可抗力を含むがこれに限らないパフォーマンス不全が生じた場合、可能な限り迅速に Tealium のシステムの全機能の回復はかるためにデザインされ、実行され、およびテストされた、商業的に合理的かつ業界の平均的な事業継続および災害復旧計画を確保する。	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 許容可能な利用規定 AUP

この許容可能な利用規定補足条項(「AUP 補足条項」)は、基本サービス契約書(MSA)、本サービス条件、または本 AUP 補足条項を参照する本サービス注文書に組み込まれまたその一部となり、Tealium と顧客間の MSA の一部を構成する。

許容可能な利用規定（「本規定」）は、本サービスの利用における禁止事項を規定する。本規程における例は全てを網羅するものではない。貴方が本規程に違反し、他者をして違反させ、または他者の違反を助長した場合、Tealium は貴方の当該本サービスの利用を停止しまたは終了させることができる。

1. 違法、有害または攻撃的な使用及びコンテンツの禁止

貴方は、本サービスにつき、あらゆる違法、有害または攻撃的な使用を行ってはならず、かつ、他者によるそのような使用を助長し、促進し、助力し、またはそそのかしてはならない。また、違法、有害または攻撃的なコンテンツを送信し、保存し、展示し、頒布し、その他利用可能にすることも禁止される。禁止される行動またはコンテンツは以下を含む。:

違法な行動。あらゆる違法な行動で、必要な同意を得ずに PII を収集し、または処理すること、違法な賭博サイトまたはサービスを宣伝し、送信し、その他利用可能にすること、もしくは、児童ポルノを拡散し、助長しまたは容易にさせることを含む。

有害なまたは詐欺的行動。他の者に、または当社の業務運営もしくは名声を害する可能性のある行為をいう。この中には、詐欺的な物品、サービス、スキームまたは販促活動（例えば、メイク・マネー・ファスト・スキーム、出資金詐欺もしくは無限連鎖講、またはフィッシングもしくはファーミングなど）を提供し、もしくは拡散すること、またはその他の欺瞞的活動に従事することが含まれる。

権利侵害コンテンツ。他の者の知的財産権または専有財産権を侵害し、または不正使用するコンテンツをいう。

攻撃的なコンテンツ。名誉毀損の、わいせつな、

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 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

侮辱的な、プライバシーを侵害する、またはその他不快なコンテンツをいう。この中には、児童ポルノを構成する、性的倒錯に関係する、または合意のない性行為を描写するコンテンツが含まれる。 **有害なコンテンツ。**何らかのシステム、プログラムまたはデータを毀損し、妨害し、秘密裏に傍受し、または横取りする可能性のあるコンテンツまたはその他のコンピュータ・テクノロジーをいう。この中には、ウイルス、トロイの木馬、ワーム、時限爆弾、キャンセルボット、またはその他の有害なあるいは悪意のあるコードが含まれる。 **2. セキュリティ侵害の禁止** 貴社は、本サービスを利用して、いかなるネットワーク、コンピューターもしくはコミュニケーションのシステム、ソフトウェアアプリケーション、またはネットワークもしくはコンピューター機器（それぞれを「**システム**」という）のセキュリティまたは完全性も侵害してはならない。禁止される行為には、以下のものが含まれる。: **無許可のアクセス。**許可を得ることなく、いずれかのシステムにアクセスすること、または使用することをいう。 **インターセプション。**許可を得ることなく、システム上のデータまたは交信をモニターすることをいう。 **3. ネットワーク濫用の禁止** 貴社は、いかなるユーザー、ホストまたはネットワークとの間であっても、それらとの接続することについて許可を得ない限り、ネットワーク接続を行ってはならない。禁止される行為には、以下のものが含まれる。: **モニタリングまたはクローリング。**対象とするシステムを毀損し、または混乱させるシステムのモニタリングまたはクローリングをいう。 **故意の妨害。**システムの正常な動作を妨害する行為をいう。この中には、メール爆撃、ニュース爆撃、ブロードキャスト攻撃、またはフラッディング技術によってシステムに過重な負荷をかけようとするあらゆる意図的試みが含まれる。 **システムの制限の回避。**手動または電子的手段を	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.

用いて、アクセス制限や保存制限などシステムに課された使用上の制限を回避することをいう。

4. E メールまたはその他のメッセージの濫用禁止

貴社は、法令または規制に違反して大量の迷惑メールもしくはその他のメッセージ、宣伝、広告、または勧誘（例えば「スパム」など）を配信、公表または送信するために、本サービスまたはシステムを使用してはならない。

5. 当社によるモニタリングおよび執行

当社は、本規程の違反または本サービスの不正使用を調査する権限を有するが、義務を負わない。当社は、以下の措置を講じることができる。: (i) 本規程の違反もしくは本サービスの不正使用を調査すること、または (ii) 本規程、または当社が本サービスの利用について貴社と締結したその他の合意に違反するコンテンツもしくはリソースを除去し、アクセスを無効化し、または修正すること。

当社は、法令または規制に違反する疑いのあるあらゆる活動について、適切な法の執行官、取締官、またはその他の適切な第三者に通報することができる。当社の通報には、適切な顧客情報および顧客データを含めることができる。当社はまた、適切な法執行機関、取締官、またはその他の適切な第三者に協力して、本規程の違反と主張されている行為に関連するネットワークおよびシステムの情報を提供することにより、違法行為の調査および訴追に協力することができる。

6. 本規程違反の通報

貴社は、何らかの本規程違反を発見した場合には直ちに当社に通報し、当該違反行為を停止または是正するために当社の要請に応じて協力するものとする。本規程違反を当社に通報する場合は、legal@tealium.com にご連絡ください。

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

データセキュリティー規定(DSS)

本データセキュリティー規定(「DSS」)は、Tealiumと顧客間のMSAに組み込まれ、その一部となる。

1. 一般。

Tealiumは、顧客データに対するそのアクセス、利用および保有に関し、顧客データの偶発的または違法な破壊、消失、変更または不正な開示もしくはアクセスに対する少なくとも業界基準(ただし、いかなる場合も本補足条項に定める特定の保護の強度を下回ってはならない)と同等の、合理的に適切な技術的および組織的保護措置を提供するようデザインされた論理的で物理的なセキュリティー措置(「プロセス」)を実行し、維持する。Tealiumは、定期的にそのセキュリティー基準を再評価し、業界基準の変化、新しいテクノロジーまたは新しい脅威の出現に応じてそのセキュリティー基準を変更する。すべての顧客データ処理は、両当事者による別段の合意がない限り、論理的に区分制御されたマルチテナント環境下で行われなければならない。

Tealiumのデータセンターは Amazon Web Services Inc.(「AWS」)が所有し、運営する。AWSのセキュリティー基準およびプログラムの詳細は、https://aws.amazon.com/security/において参照することができる。

2. 定義。

「コンピュータ設備」とは、デスクトップ、ラップトップまたはノート型パソコン、モバイル機器(例えば、携帯電話またはタブレットなど)およびその他電話またはコンピュータ機能のために使用されるすべての機器をいう。

「ダイナミックアプリケーションセキュリティーテスト」または**「DAST」**とは、あるアプリケーションを生産環境下で、または当該アプリケーションが稼動する生産環境を想定したテスト環境下で稼動させて、そのセキュリティーの脆弱性を示す条件を探知するためにデザインされたアプリケーションのセキュリティーテストをいう。

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.

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.

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.

「**暗号化**」とは、データの機密性を保護するため、データをコード化された情報に変換するアルゴリズムを用いたプロセスをいう。	**"Firewall"** means an integrated collection of security measures used to prevent unauthorized electronic access to the Tealium Network.
「**ファイアウォール**」とは、Tealium のネットワークへの不正な電子アクセスを防止するために使用される統合的なセキュリティー措置の集合体をいう。	**"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.
「**業界基準**」とは、MSA が対象とする種類のサービスの主要な供給者たちが遵守している慣習および慣行であって、当該主要な供給者たちに期待される技術、注意力、慎重さおよび洞察力を反映するものいう。	**"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.
「**侵入探知プロセス**」または「IDP」とは、システムログおよびプロセスをほぼリアルタイムで、また、侵入の発生または侵入発生の可能性を示す動作パターンの増加をすみやかに、不合理に遅延することなく検知する方式をいう。	**"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.
「**最小限の権限**」とは、特定のコンピュータ環境（例えば、個々の処理、ユーザーまたはプログラムなど）の下にあるどのモジュールも、適法正当な目的のために必要な情報およびリソースに限りアクセスが可能であることをいう。	**"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.
「**悪意のあるコード**」とは、バックドア、ウイルス、トロイの木馬、ワーム、またはその他のソフトウェアルーチンもしくは機器要素であって、顧客のシステム運用を妨害するためにソフトウェア、機器またはデータを破壊し、変更し、消去し、またはその他の方法でこれを害するようにデザインされたものをいう。	**"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.
「**手動侵入テスト**」とは、自動化されたツールと公認のテスターまたは資格のある第三者との組み合わせにより実行されるアプリケーションの手動セキュリティーテストをいう。	**"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.
「**多要素認証**」とは、パスワードなどの「貴方が知っているもの」、トークンなどの「貴方が所有するもの」、または生体認証などの「貴方であるもの」のうち、少なくとも 2 つの要素を使う認証をいう。	**"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.
「**処理すること**」または「**処理**」とは、顧客データに作動するオペレーションまたはオペレーションの集合体の一切（自動装置によるものか否かに	**"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

限らない）をいう。その例として、収集、記録、編成、構成、ストレージ、適合または変更、入手、参照、使用、送信による開示、流布またはその他の方法による公開、同調または結合、制限、消去または破棄などが挙げられる。 「**リムーバブルメディア**」とは、顧客データを収納している、持ち運び可能なまたは取り外し可能なハードディスク、フロッピーディスク、USB メモリドライブ、ジップディスク、光ディスク、CD、DVD、デジタルフィルム、メモリーカード（例えば、セキュアデジタル（SD）、メモリースティック（MS）、コンパクトフラッシュ（CF）、スマートメディア（SM）、マルチメディアカード（MMC）、および xD-ピクチャーカード（xD）など）、磁気テープ、およびその他の取り外し可能なすべてのデータ保存メディアをいう。 「**セキュアソフトウェア開発ライフサイクル方式**」または「**SDLC**」とは、情報セキュリティー対策（特にデザイン、テスト、および開発の工程時の対策）を必要とする情報システムの、プランニング、作成、テスト、およびデプロイに関する文書化されたプロセスをいう。 「**セキュリティーインシデント**」とは、偶発的または違法な顧客データの破壊、損失、変更、無許可の開示あるいは顧客データへのアクセスに繋がる、無許可または違法なセキュリティーの侵害をいう。ただし未然のセキュリティー事故を除く。 「**職務の分離**」とは、一人の人間が重要な工程のセキュリティー管理方法を変えることができないよう、役割と責任を分割することをいう。 「**静的アプリケーションセキュリティーテスト**」または「**SAST**」とは、あるアプリケーションのコード内のセキュリティーの脆弱性を示す状態を検知するためにデザインされた、アプリケーションのソースコードのセキュリティーテストをいう。 「**Tealium の施設**」または「**施設**」とは、本サービスの提供に関係する施設をいう。この中には、Tealium の職員が勤務し Tealium のシステムを使用する場所、および/または、顧客データが収納されまたは処理される場所がすべて含まれる。 「**Tealium のネットワーク**」とは、Tealium またはそのサブプロセッサーの管理内にあり、かつ本サ	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

ービスを提供するために使用される、データセンター施設、ネットワーク環境、およびホストソフトウェア（仮想ファイアーウォールなど）をいう。 **「脅威モデル」**とは、すべて仮想の攻撃者の目線から、潜在的な脅威を特定し、列挙し、優先順位をつけることができるプロセスをいう。脅威モデルの目的は、潜在的攻撃者のプロフィール、最も可能性の高い攻撃経路、および攻撃者が最も欲する資産について、防御者に体系的分析を提供することである。 **「未然のセキュリティーインシデント」**とは、顧客データのセキュリティーの危殆化に至らない未然の試みまたは活動をいう。これには、ファイアウォールまたは端末サーバーへのピングおよびその他のブロードキャストの攻撃、ポートスキャン、未然のログインの試み、サービス攻撃の拒否、パケット盗聴（またはその他の、ヘッダーへのアクセスに至らないトラフィックへの無許可のアクセス）、もしくは同様のインシデントを含むがこれに限らない。 **「根本原因分析」**とは、セキュリティーインシデントを含む、セキュリティーイベントに関連する根本的原因を特定するための基本原理ベースのシステムアプローチをいう。 **3. インシデント管理およびセキュリティーインシデントの通知** **3.1 インシデント管理。** Tealium は、セキュリティー上の問題を適時に探知するため、文書化されたインシデント管理の方針および手続を整備し、脅威および顧客からの通知に対し連携した対応をする。手続には、特定された問題の修復に至るまでの追跡を含む根本原因分析、ならびに再発を防ぐための措置の評価および実行を含む。 **3.2 セキュリティーインシデントの通知と是正。** セキュリティーインシデントが発生した場合、Tealium は顧客に通知し、以下に定める方法によりセキュリティーインシデントを是正する。： **3.2.1 通知。** Tealium がセキュリティーインシデントを確認した場合、不当な遅延なしに、可能な場合、確認した時点から 48 時間以内に顧客にセキュリティーインシデントの通知をする。48 時間以内に顧客が通知を受けなかった場合、遅延の理	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. **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

由がなければならない。

上記の通知には少なくとも以下の点が含まれなければならない。：

(1) セキュリティーインシデントの性質の説明

(2)データ保護担当者またはより多くの情報が得られるその他の者の氏名と連絡先の詳細。および

(3) Tealium がセキュリティーインシデントを是正するために講じた、または申し出た措置（悪影響が出る可能性がある場合、これを最低限に抑える適切な措置を含む）の説明。

情報の同時提供が不可能な場合、過度の遅延なく、段階ごとに情報を提供することができる。

Tealium は、あらゆるセキュリティーインシデント、セキュリティーインシデントに関する周辺事実、その影響および講じられた是正措置を文書化しなければならない。かかる文書は、顧客が当セクションへの準拠を確認することができるものでなければならない。

3.2.2 根本原因分析。 Tealium は本原因分析をすみやかに開始し、できるだけ早期の完了を目指す。

3.2.3 是正。Tealium は、顧客データおよび Tealium システムの安全性を回復するために必要な措置を速やかに講じる。　悪影響がさらに拡大するリスクを減じるため、当該措置により一切の情報または Tealium システムへのアクセスが一時的に制限される場合、Tealium は、当該制限に先立って、合理的に可能な時点で、アクセスの制限について顧客に速やかに通知をする。Tealium は、顧客と協力して、Tealium が漏洩に対処し、その影響を減じるために必要な追加的処置を特定する。

3.2.4 未然のセキュリティーインシデントの一切は当セクションの対象とならない。

4.　独立のリスク査定および監査。

4.1 サービス組織に関する報告。　Tealium は、少なくとも年に一度、その費用負担で ISO/IEC 27001、ISO/IEC 27018 および 国際監査保証基準 3402（SSAE16/ISAE 3402 タイプ II）、またはこれ

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

らの後継基準に従って監査を実施する。当該監査は、サービス組織として本サービスの提供に関連する管理体制をカバーするものとし、その範囲は業界基準の慣行に従うものとする。

4.2 第三者/ 下請業者の契約。 Tealium は、顧客データを処理する Tealium のサービス業者について詳細なリスク査定を行う。その査定結果は文書化され、顧客は要請すればこれを入手できる。

4.3 セキュリティーテスト。 Tealium は、少なくとも年に一度、その費用負担で、第三者サービス業者に委託して、本サービスの提供に関する Tealium システムのマニュアル侵入テストを行わせる。テストの採点および問題評価の方法は、アメリカ国立標準技術研究所（「NIST」）が公表する最新の共通脆弱性評価システム（「CVSS」）など、業界基準の慣行に従う。Tealium は、重大（危機的、優先度の高い、またはハイリスク）とみなされる発見があった場合には、当該発見の後、適時にこれを是正する。

4.4 AWS の査定。 Tealium のストレージおよびインフラストラクチャのプロバイダーである AWS は ISO 27001 に認定されており、また本サービスのために情報セキュリティープログラムを維持することに同意した。そのプログラムは、AWS に適用されるセキュリティー基準の設立、実行、管理および改良において、ISO 27001 の基準、またはその他の ISO 27001 と実質的に同等の代替基準に基準拠する。AWS は、AWS 自身のセキュリティー対策（Tealium が本サービスを提供する物理的なデータセンターのセキュリティーを含む）の適性を検証するため、外部の監査法人を使う。この監査は、(a)少なくとも年に一度、(b) ISO 27001 の基準またはその他の ISO 27001 と実質的に同等の代替基準に従って、また(c)独立した第三者のセキュリティー専門家によって行われる。

4.5 顧客の監査。 顧客は、自身または顧客選定の第三者の独立した業者によって、顧客の自己負担で、現地監査を行い、本サービスに関連して使用される Tealium のネットワークを審査することができる。かかる監査および審査は、多くて年に一度、30 日の事前通知を伴って行われなければならない（適用法に要求されるか、顧客データに影響を与えるセキュリティーインシデント後である場合を除く）。当セクションに示される監査はすべて、適切な時間内に、Tealium の通常業務を非合理

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

的に妨害せずに、また適切な技術的および秘密保護の制限に基づいて行われなければならない。顧客が第三者の独立した業者に監査をさせる場合、かかる独立業者は、Tealium の本秘密情報を保護する MSA に定義される条項と実質的に同類の秘密保護の条項を含む秘密保護契約を、監査前に締結していなければならない。顧客は、Tealium に、監査の過程で発見されたあらゆる違反に関する情報と報告書をすみやかに提出しなければならない。

5. セキュリティー業務。

5.1 セキュリティー担当者。Tealium は、すべての顧客データおよび Tealium ネットワークの継続的セキュリティー保護を図るため担当者を指定する。Tealium のセキュリティー担当者には、infosec@tealium.com で連絡をすることができる。

5.2 訓練。Tealium は、MSA において義務付けられる訓練に加え、少なくとも年に一度、本サービスに関係する責任を負うすべての Tealium の人員に対し、MSA の遵守が要求される Tealium のプロセスに関する適切な継続的訓練（この中には、Tealium の人員が実際のセキュリティーインシデントおよび・またはセキュリティーインシデントの恐れをすみやかに報告することを確認する手続が含まれるが、これに限定されない）を提供する。Tealium の SDLC 方式のいずれかの部分に関与するすべての人員は、アプリケーションセキュリティーの訓練を受けなければならない。Tealium は、かかるトレーニングが完了したことを示す記録を保管する。

6. データの管理。 Tealium のネットワークが処理する顧客データには、以下が適用される。:

6.1 データへのアクセス。顧客データは、その職務上アクセスする必要があり、最小限の権限の原則に従う Tealium の人員のみがアクセスすることができる。Tealium は、業界基準の認証慣行に従って顧客データに関わる全ての通信を保護する。

6.2 情報の暗号化。 Tealium は、本サービス提供において顧客データを保存し、処理しまたは送信する場合には、業界基準の暗号化の技術を用いる。かかる技術は、(i) 対称暗号化には 128 ビット以上のキーの長さ、および(ii)非対称暗号化には 2048 ビット以上のキーの長さを必要とする。

6.3 暗号化キーの管理。Tealium は、暗号化キーを

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

安全に管理し、文書化された業界基準の管理要件および手順を維持する。Tealium が公開鍵基盤（「PKI」）を使用する場合、Tealium は、基本ソフトを「強化」することによって、当該 PKI を不正アクセスから合理的に保護する。Tealium は、第三者のシステムにはベンダー推奨の強化ガイドラインを用いる。Tealium は、Tealium のシステムについては、米国インターネットセキュリティーセンター®のチェックリストなど、業界基準の強化ガイドラインを用いる。	guidelines. For Tealium's systems, Tealium will utilize Industry Standard hardening guidelines, such as checklists provided by the Center for Internet Security®.
6.4 リムーバブルメディア。 Tealium は、本サービスの提供にはリムーバブルメディアを使用しない。	**6.4 Removable Media**. Tealium does not use Removable Media in providing the Services.
6.5 データの消去および処理。顧客データを収納するハードウェア、保存メディア、または顧客データを含む文書を処分し、またはサービスのために移動する必要がある場合には:	**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 は、データの処分に関する文書化された方針および手続（受け渡しの管理の維持に関する規定を含む）を遵守し、	**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 は、当該ハードウェアおよび/またはメディアから、少なくとも NIST SP 800-88 Rev.1（または後継基準）が推奨する最低限のサニタイズの方法と同程度の保護の方法を用いて、当該顧客データをアクセス不能とし、除去し、または消去する。	**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 データの送信。Tealium が顧客データをインターネット、またはその他の公共もしくは共同ネットワークを通じて送信する場合、本 DSS 第 6 条(b)の要求に従い適切な暗号を用いてデータを保護する	**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 データの復元力。業界基準の保護機能を利用して顧客データを復元する。復元の方法としては、データベースのバックアップ、ファイルのバックアップ、サーバーのバックアップ、または管理された高可用性のサービス、耐障害性のデータ保存もしくは管理データベースサービスがあるが、これらに限定されない。Tealium のバックアップファイルの保管または保持は、すべて本 DSS の条件に従う。	**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. 物理的なセキュリティー - 施設。Tealium の施設は、出入口のアクセスの管理（例えば、入場	**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

証の使用など）のように不正のアクセス、毀損および妨害から防御された物理的環境を提供する周辺警備によって保護される。すべての Tealium の施設は、少なくとも、以下の警備関連の特性を備えなければならない。：	(“CCTV”) systems and CCTV recording systems to monitor and record access to Tealium Facilities. Logs must be retained for at least one (1) year.
7.1 Tealium は、人的および物理的警備方針を文書化し、実行し、維持する。この中には、「クリーンデスクポリシー」が含まれるが、これに限定されない。	**7.3** All Tealium personnel will be issued and will display to gain access an identification badge allowing electronic verification of bearer’s identity.
7.2 Tealium は、Tealium の施設へのアクセスを監視し、記録するために、有線テレビ（「CCTV」）システムおよび CCTV 録画システムを備え付ける。記録は、少なくとも 1 年間は保管されなければならない。	**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.
7.3 すべての Tealium の人員には個人認証バッジが発行され、アクセスする際にはバッジを見せて所持者の身分証明のため電子認証を受けることになる。	**8. Tealium Network Security.**
7.4 すべての施設所在地では、訪問者の本人確認、および施設への入場許可のための手続を維持する。この中には、身分証明の確認、認証バッジの発行、バッジ所持者の本人確認、訪問の目的および出入の記録が含まれるが、これらに限定されない。	**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. Tealium ネットワークセキュリティー。	**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.
8.1 **資産目録。** Tealium は、その現行のシステムのコンポーネント、ハードウェアおよびソフトウェア（バージョン番号および物理的所在地を含む）の包括的な目録を維持し、権限を付与された、またはサポートされたコンポーネントのみが顧客データを処理、保存または送信することを確実にする。Tealium は、少なくとも年に一度、システムコンポーネントの目録を見直し、更新する。	**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.
8.2 **Tealium のネットワークセキュリティー。** 外部ソース（インターネットを含むが、これに限定されない）から Tealium のネットワークに入るデータは、Tealium の内部ネットワークと外部のソース間の安全な接続を確保するため、ファイアウォールを通過しなければならない。当該ファイアウォールは、Tealium の事業運営に必要な最小限のデータ以外のデータを明確に拒否する。	**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

8.3 侵入検知システム。 侵入検知システムは、対内および対外コネクションを監視するため Tealium のネットワーク上の個々のホストまたは機器に対して実行され、不審なアクティビティーが検知されると管理人に警告する。IDS は Tealium のネットワークのファイルの生合成を監視し、重要なシステムファイルが変更された場合、IDS は Tealium のセキュリティー情報およびイベント管理システム内にかかるイベントを記録する。	supporting Services to Customer, and such tools are updated to provide protection against current threats.
8.4 着信ファイルの監視。 Tealium は、顧客データが処理されるすべてのサーバーに IDS を含む業界基準のセキュリティーツールを使用する。	**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.
8.5 無権限のコードからの保護。Tealium は、 悪意のあるコードの送信に対する保護を目的としてデザインされた適切な技術措置を、 顧客のシステムに、email またはその他の電子送信によって実施する。マルウェア対策ツールは、顧客にサービスを提供するすべての Tealium のシステムにデプロイされ、更新されて、現行の脅威に対する保護を提供する。	**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.
8.6 脆弱性の管理。Tealium は、顧客データを収納する Tealium のネットワークに影響を与える脆弱性を発見し、修復する文書化されたプロセスを備える。Tealium は、発見されたすべてのセキュリティー脆弱性を、合理的な時間内に修復する。	**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.
8.7 電子コミュニケーション。本サービスの提供に関連するすべての電子コミュニケーション（インスタントメッセージおよび Email サービスを含む）は、業界基準の処理方法および技術管理によって保護される。	**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. 変更およびパッチ管理。 **9.1 変更の管理。**アプリケーション、Tealium の情報技術基盤のあらゆる部分、Tealium のネットワークの変更は、文書化された変更管理プロセスを用いてテスト、検査および実行され、職務の分離の原則に従う。	**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.
9.2 緊急変更。Tealium は、 Tealium のネットワークの変更および修復を実行するため、必要に応じて緊急変更の許可のプロセスを迅速に行う。Tealium は、かかる緊急変更が本サービスの機能に影響を与える場合、通常の営業時間内に、顧客に事前に通知する。	**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

9.3 ソフトウェアのアップデート。 Tealium は、：	Customer Data must be traceable to one (1) user. Shared accounts accessing Customer Data are prohibited by Tealium.
9.3.1 本サービスの提供のため、マルウェア対策およびその他のセキュリティーソフトウェアを使用し、	**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.
9.3.2 本サービス提供に必要なソフトウェアは、サポートされるバージョンのみを使用し、	**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.
9.3.3 本サービスが影響を受ける場合、Tealium が事業リスクがより高まると合理的に判断しない限り、合理的な時間内にソフトウェアの緊急修復を行う。すべての変更は、Tealium が承認した変更管理プロセスに従って行われなければならない。	**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. 論理的なアクセスコントロール。	**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.
10.1 ユーザー認証： Tealium は、以下の方法により、すべてのユーザーについて、本人確認のためにデザインされた手続を実行する。：	**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.
10.1.1 ユーザーID。 顧客データを収納するアプリケーションへのアクセスは、ユーザー1 名に限定される。Talium は、顧客データにアクセスできるアカウントの共用を禁止する。	**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.
10.1.2 パスワード。Tealium ネットワークの各ユーザーは、一意的なパスワードを使って顧客データを収納するアプリケーションにアクセスする。パスワードは、少なくとも 8 桁の英数字とする。容易に解析可能なパスワード（ユーザーID、ユーザーの誕生日、住所、子供の名前と同じまたはそれを含むパスワードなど）は拒否される。Tealium は、ユーザーに対し、顧客データを収納するアプリケーションまたはシステムへのアクセスに多要素認証を使用することを要求する。	**10.6 Privileged Access**. Tealium will use Industry Standard methods to provide that:
10.1.3 Tealium 多要素認証。 多要素認証は、承認された人物のみに進入を制限するようデザインされたすべての Tealium のネットワークアクセスポイントにおいて、進入する際に必要とされる。	**10.6.1** Users with access to Tealium Network containing Customer Data will be granted the minimum amount of privileges necessary;
10.2 セッション設定。 セッションは、最大 60 分ユーザーが操作しないとタイムアウトになるように設定される。かかるタイムアウトまたは操作のない時間経過後は、再認証が必要となる。	**10.6.2** Privileged access will be restricted to authorized individual users and non-repudiation will be maintained;
10.3 ログインの失敗回数。 ログインの試みの失敗	**10.6.3** Privileged user accounts will be used

回数は、最大 5 回に制限される。許される最大のログイン失敗回数を超えると、ユーザーアカウントは少なくとも 10 分間ロックされる。 **10.4 遠隔アクセス。** 顧客データを収納する Tealium のネットワークの遠隔アクセスは、承認されたユーザーに限定され、多要素認証を必要とし、また検査のため記録される。 **10.5 効力停止。** 顧客データへアクセスできる Tealium の人員のユーザーID は、職務の変更に伴いかかるアクセスが不要になった場合、または雇用が終了した場合には、直ちに効力が停止される。 **10.6 特権アクセス。** Tealium は、業界基準の方法により、以下を提供する。: 10.6.1 顧客データを収納する Tealium のネットワークにアクセスできるユーザーは、本サービスの提供に必要最小限の特権を付与される。 10.6.2 特権アクセスは、権限を付与された個人ユーザーに制限され、否認不能は維持される。 10.6.3 特権ユーザーアカウントは、特権的操作のためにのみ使用され、事業のための通常活動には使用されない。 10.6.4 開発担当者は生産環境への特権アクセスを付与されない。 10.6.5 すべての特権アクセスには、多要素認証が要求される。 **11. ログ記録と監視。** **11.1 Tealium のネットワークの監視。** Tealium は、顧客データが処理される本サービスをサポートする Tealium のネットワークを積極的に監視し（業界 k 順夫 IDS を使用する）、アクセスコントロールポリシーからの逸脱および実際の侵入もしくは侵入未遂、またはその他の不正行為を探知する。 **11.2 イベントのログ記録。** Tealium のネットワークによる顧客データの処理のため、Tealium は以下を行う。 11.2.1 顧客に提供される本サービスの秘密保持、	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:

完全性、および利用可能性に影響を与える可能性があると合理的に判断され、かつ、Tealium のネットワーク上で発生しているセキュリティーインシデントの特定または調査に役立ちうる重要なイベント（アクセスイベントを含む）のログ記録を維持する。顧客は、書面上の要求によって、かかるログ記録のコピーを入手することができる。 11.2.2 ログ記録を修正または削除から保護する。Tealium の情報セキュリティーチームは定期的にログ記録を再検討する。 11.2.3 ログ記録を少なくとも 12 ヶ月間保管する。 **12. ソフトウェアセキュリティーに関する保証。** 12.1 **開発手法。** 本サービス提供の過程において使用されるソフトウェアについて、Tealium は以下を実行する。 12.1.1 文書化された SDLC の方針に従って内部開発活動を実施する。顧客は、要求によりこれを共有することができる。 12.1.2 SDLC に厳格に従って、新しいアプリケーションおよび既存のアプリケーションの変更を現行の生産環境にデプロイする。 12.1.3 セキュリティー要件の定義付け、テスト、およびデプロイを含む、文書化された SDLC を維持する。 12.2 **開発環境。** 本サービス提供の過程において使用されるソフトウェアについて、Tealium は以下を実行する。 12.2.1 生産環境から隔離され、かつ、不正開示から顧客データを保護する特別な環境下において、システム開発およびテストを行う。 12.2.2 顧客データを、顧客の事前の書面による承諾を得ることなく、かつ、当該情報の保護に必要な文書化された管理なしに、テスト環境で使用しない。 12.3 **容量および機能のプランニング。** Tealium は、Tealium のネットワーク不良または停止の可能性および影響を最小限に抑えるようにデザインされた、容量および機能のプラニングの手	**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

順に従う。 Tealium は、定期的に容量プランおよび機能の監視情報を検討する。

テストプロセス。 本サービスの提供の過程において 、Tealium は以下を実行する。

12.3.1 アプリケーションが正式なコードレビュープロセスを受けるように設定する。Tealium は、 顧客から書面上の要求があった場合、正式なプロセス実行の証拠を顧客に提供する。

12.3.2 アプリケーションが四半期ごとのダイナミックアプリケーションセキュリティーテスト(DAST)、および静的アプリケーションセキュリティーテスト(SAST)を受けるように設定する。 テストの採点および問題評価の方法は、アメリカ国立標準技術研究所（「NIST」）が公表する最新の共通脆弱性評価システム（「CVSS」）など業界の慣行に従う。 Tealium は、 重大な発見については、顧客の書面上の要求があった場合、要旨認証書の書式を用いて、かかるテスト結果および修復活動を顧客に報告する。当該証明書には、実行されたテスト、その日付、およびテスト結果の要約が含まれる。

12.3.3 アプリケーションが少なくとも年に一度、脅威モデル分析を受けるように設定する。 脅威モデルについて正式に結果を報告しおよび重大な瑕疵を修復するプロセスを実行する。Tealium は、顧客の書面上の要求があった場合、脅威モデルの要旨を共有することにより、かかる活動を証明する。

13. データセンターの管理。

13.1 **基本要件。** 本サービスをサポートするすべてのデータセンターは、以下の最低要件を備えるものとする。 :

13.1.1 本 DSS 第 6 条および第 7 条に定める適切な物理的セキュリティーおよびアクセスコントロール

13.1.2 専門的 HVAC および環境管理

13.1.3 専門的ネットワーク/ケーブルの環境

13.1.4 専門的火災探知/消化機能

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

13.1.5包括的事業継続プラン 14. 事業継続プラン(BCP)。 14.1 BCP プランおよびテスト 14.1.1Tealium のプランニング機能には、MSA に基づく Tealium の義務の履行に必要なすべてのハードウェア、ソフトウェア、通信機器、ならびにデータおよびファイルの現行のコピーをから成るデータ回復システムが含まれる。 14.1.2Tealium は、Tealium が所有する、または Tealium が運営するデータセンターにおいて本サービスの適時回復のプロセスを実行する。 14.2 BCP プラン。 このプランは、すべての重要な点において、以下の追加的またはこれと同等の基準を取り扱う。 : 14.2.1プランは、規制およ業界慣行を反映する。 14.2.2Tealium の影響を受けるスタッフの 1 つまたは複数の他の代替地への移転、および当該移動が有効になるまでの間、同様の機能を果たすその他の場所への職務の移転。 14.2.3Tealium の通常業務、システムおよびプロセスの中断、または損失が発生した場合に発生すると Tealium が確信し、予想する影響および効果の包括的業務影響度の分析。 14.2.4本サービス提供のため、および MSA に基づく Tealium の義務を履行するために Tealium が使用する主要な場所およびシステムと遜色のない能力を有する代替場所および代替システムの設立と維持。 14.2.5大事故発生後に実施される復旧手順の詳細であって、事業の継続を維持するために必要な、Tealium の事業運営、システムおよびプロセス、ならびに重要な人員、リソース、サービスおよび活動の復旧を確実にするための緊急時の準備の詳細を示すもの。 14.2.6大事故発生後に Tealium の事業運営、システムおよびプロセスが復旧する目標時間を示すスケジュール。Tealium は、復旧手順および BCM プランが、修復時間目標 (「RTO」) を 4 時間、復旧時	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.

点目標（「RPO」）を 24 時間に設定することに同意する。 **14.3 明確な準備計画。**明確なプランが特定の Tealium 所在地に適用される場合、Tealium が本サービスの重要部分を履行する各所在地のプランは、少なくとも年に一度、包括的なシナリオの下でテストされ、テストの結果が Tealium の経営陣に報告される。 **14.4 通知。** MSA に基づく Tealium の義務遂行能力、または本サービスに影響が出ると Tealium が合理的に判断する大事故が発生した場合、Tealium は、当該大事故について速やかに顧客に通知する。かかる通知には、詳細が明らかになり次第、以下の事項が含まれる。 **14.4.1** 問題の大事故の内容、およびどのように探知されたか **14.4.2** 大事故が本サービスに及ぼすと予想される影響 **14.4.3** Tealium が利用する代替運営方法およびバックアップシステム、ならびにそれらの利用のタイムテーブル **14.4.4** 大事故が解決し Tealium が通常業務に戻るのにかかると予測される時間 **14.5 下請業者。** Tealium は、本サービスのいずれか一部（本サービスを円滑にするための補助サービス（例えば、文書の倉庫保管および検索、プリントサービスなど）を除く）を提供するその下請業者が、取締規定および業界の最良の慣行に従った、商業的に合理的な事業継続プログラムを準備し、維持することを要求する。 Tealium による下請業者の利用は、その利用の理由および顧客への通知の如何にかかわらず、MSA に基づき提供するすべての本サービスのために、上記に従い事業継続可用性を提供する Tealium の義務を消滅させるものではない。	**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.

TEALIUM INC. データ処理補足条項
(補足条項 DPA-2)

本データ処理補足条項(「DPA」)は、顧客による Tealium からの本サービスの購入に関する Tealium と顧客間の MSA、またはその他の、書面上あるいは電子上の、本 DPA を参照するサービス条件もしくは購入契約書（「MSA」）の一部を構成し、その対象となる。本 DPA は、欧州連合と米国間に個人データの移動がない場合に適用される。

1. 定義。 本 DPA の目的のため、GDPR および CCPA で使用される語句と定義（ここに定義する）が適用される。さらに、MSA にベット定義されない限り、DPA で使用されるすべての大文字の語句は、**以下に定められた意味を持つものとする。**:

「**AWS**」 とは Amazon Web Services, Inc.をいう。

「**CCPA**」とは、 California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.（**カリフォルニア州プライバシー保護法民法** 1798.100）**をいう。**

「**データエクスポータ**」 および 「**データインポータ**」は標準契約条項で与えられた意味を持つ。

「**データ保護法および規制**」とは、MSA に基づく個人データ処理時における役割にに関して各当事者に適用されるすべての法律および規制をいい、 GDPR、プライバシー保護法、また CCPA が含まれる場合がある。

「**データセキュリティー規定**」 または「**DSS**」とは、Tealium の技術的かつ組織的セキュリティー対策に関する規定をいう。

「**EEA**」 とは、本 DPA の目的上、欧州経済領域および英国をいう。

「**GDPR**」 とは、個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、 並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679 をいう。

「**極秘データ**」**とは、その不正開示または不正使**

TEALIUM INC. DATA PROCESSING ADDENDUM
(Addendum DPA-2)

This Data Processing Addendum ("DPA") forms part of, and is subject to, the Master Services Agreement or other written or electronic terms of service or subscription agreement between Tealium and Customer for Customer's purchase of Services from Tealium that references this DPA (the "MSA"). This DPA applies where there is no transfer of Personal Data between the European Union and the USA.

1. Definitions. For the purposes of this DPA, the terminology and definitions as used by the GDPR and the CCPA (as defined herein) shall apply. In addition, unless otherwise defined in the MSA, all capitalized terms used in this DPA will have the meanings given to them below:

"AWS" means Amazon Web Services, Inc.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.

"Data Exporter" and **"Data Importer"** have the meanings given them in the Standard Contractual Clauses.

"Data Protection Laws and Regulations" means all laws and regulations applicable to each respective Party in its role in the Processing of Personal Data under the MSA, including where applicable, the GDPR, the Privacy Act, and the CCPA.

"Data Security Statement" or **"DSS"** means Tealium's statement of its technical and organizational security measures.

"EEA" means, for the purpose of this DPA, the European Economic Area and the UK.

"GDPR" means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"Highly Sensitive Data" means personal data whose unauthorized disclosure or use could

用により、データ対象の潜在的な重大なセキュリティーまたはプライバシーのリスクが合理的に発生するおそれがある個人特定可能な情報（国民保険番号、パスポート番号、運転免許証番号、もしくは類似の識別番号などの政府発行の識別番号、クレジットカード番号やデビットカード番号、医療または財務情報、生体情報、および／または財務、医療、あるいはその他のアカウント認証データ（パスワードや個人識別番号など）含むが、これらに限らない）をいう。

「個人データ」は、特定可能な個人に関する情報の収集、使用、保管または公開に関連した適用法または法令に定義された意味を持ち、かかる定義がない場合、特定の個人を識別し、連絡しまたは所在地を確定するために使用されうる個人に関する情報、またはその他の情報と組み合わせることによって特定の個人を識別し、連絡しまたは所在地を確定するための特定の個人に関連付けられる情報をいう。DPA の目的上、個人データは、添付書類 1 に記載のある「処理」の範囲に示される通りである。

「プライバシー法」とは、1988 年オーストラリア連邦プライバシー法(Cth.)をいう。

「処理すること」または**「処理」**とは、顧客データに作動するオペレーションまたはオペレーションの集合体の一切（自動装置によるものか否かに限らない）をいう。その例として、収集、記録、編成、構成、ストレージ、適合または変更、入手、参照、使用、送信による開示、流布またはその他の方法による公開、同調または結合、制限、消去または破棄などが挙げられる。

「サービスプロバイダー」は、 CCPA に定義される意味を持つものとする。

「セキュリティーインシデント」とは、偶発的または違法な顧客データの破壊、損失、変更、無許可の開示あるいは顧客データへのアクセスに繋がる、無許可または違法なセキュリティーの侵害をいう。ただし未然のセキュリティー事故を除く。

「Tealium のネットワーク」とは、Tealium またはそのサブプロセッサーの管理内にあり、かつ本サービスを提供するために使用される、データセンター施設、ネットワーク環境、およびホストソフトウェア（仮想ファイアーウォールなど）をいう。

reasonably entail a serious potential security or privacy risk for a data subject, including but not limited to government issued identification numbers such as national insurance numbers, passport numbers, driver's license numbers, or similar identifier, or credit or debit card numbers, medical or financial information, biometric data, and/or financial, medical or other account authentication data, such as passwords or PINs.

"Personal Data" has the meaning set forth in Data Protection Laws and Regulations relating to the collection, use, storage or disclosure of information about an identifiable individual, or if no definition, means information about an individual that can be used to identify, contact or locate a specific individual, or can be combined with other information that is linked to a specific individual to identify, contact or locate a specific individual. For purposes of the DPA, Personal Data is as described in the scope of Processing described in Appendix 1.

"Privacy Act" means the Australian Privacy Act 1988 (Cth.).

"Processing" or **"Process"** means any operation or set of operations which 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.

"Service Provider" shall have the meaning set forth in the CCPA.

"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 Personal Data, but does not include any Unsuccessful Security Incident.

"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.

"Unsuccessful Security Incident" means an unsuccessful attempt or activity that does not compromise the security of Personal Data, including (without limitation) pings and other

「未然のセキュリティーインシデント」とは、顧客データのセキュリティーの危殆化に至らない未然の試みまたは活動をいう。これには、ファイアウォールまたは端末サーバーへのピングおよびその他のブロードキャストの攻撃、ポートスキャン、未然のログインの試み、サービス攻撃の拒否、パケット盗聴（またはその他の、ヘッダーへのアクセスに至らないトラフィックへの無許可のアクセス）、もしくは同様のインシデントを含むがこれに限らない。

「ユーザーデータ」とは、本サービスの使用を認められたユーザーのログイン情報の詳細および連絡先をいい、個人データとみなされる。

より詳しい定義は本 DPA を通じて示される。

2. データ処理。

2.1 **範囲および役割。** 本 DPA は、MSA に基づき本サービスを提供する過程において Tealium がデータプロセッサーまたはサービスプロバイダーとして顧客を代表して個人データを処理する場合においてのみ適用される。Tealium は、以下セクション 10 で定められる下請業者の要件に従って、下請業者を雇用する。

2.2 **法への準拠。** 各当事者は、MSA に基づく本サービスの受領過程において、自身に適用される、または自身に課されるすべてのデータ保護法および規制（データ保護に関するすべての法廷要件を含む）に準拠する。

2.3 **顧客による個人データの処理。** 顧客は、いかに同意する。(a) すべての通知を終了し、ならびに Tealium が個人データを合法的に処理するために必要なすべての事前同意、許可、および権利を収得していること。 (b) 顧客が、Tealium に極秘データを送信せず、また Tealium にその処理を要求しないこと。(c) 顧客が、個人データの正確性、質、および合法性について、また顧客が個人データを得た方法について、単独で責任を負わなければならないこと。

2.4 データ処理の指示。

2.4.1 Tealium は、顧客の文書化された指示を代表し、またそれにのみ従って個人データを処理する。これには第三国または国際組織への個人デー

broadcast attacks of 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.

"User Data" means the login details and contact information of the authorized users of the Services and will be deemed Personal Data.

Further definitions are provided throughout this DPA.

2. Data Processing.

2.1 Scope and Roles. This DPA applies where and only to the extent that Tealium Processes Personal Data on behalf of Customer as a data processor or Service Provider in the course of providing Services pursuant to the MSA. Tealium will engage sub-processors pursuant to the requirements for subcontractors set forth in Section 10 below.

2.2 Compliance with Laws. Each party will comply with all Data Protection Laws and Regulations applicable to it and binding on it in the provision or receipt of Services under the MSA, including all statutory requirements relating to data protection.

2.3 Customer Processing of Personal Data. Customer agrees that: (a) it has provided all notices and obtained all consents, permissions and rights necessary under Data Protection Laws and Regulations for Tealium to lawfully process Personal Data; (b) Customer will not transmit to Tealium nor require Tealium to process any Highly Sensitive Data; and (c) Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.4 Instructions for Data Processing.

2.4.1 Tealium will Process Personal Data on behalf of and only in accordance with Customer's documented instructions, including with regard to transfers of Personal Data to a third country or an international organization, unless otherwise required by Data Protection Laws and Regulations to which Tealium is subject; in such a case, Tealium shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of

タの転送に関する事項が含まれるが、Tealium が対象となるデータ保護法および規制に要求される場合はこの限りでなく、その場合 Tealium は、処理を行う前に、顧客にかかる法律要件を通知しなければならない（かかる法が重要な公共の利益を理由に当該情報提供を禁止する場合を除く）。Tealium は個人データを販売しない。

2.4.2 顧客は次の目的のために Tealium の個人データの処理を指示する。：(a) MSA に基づく処理、(b) 本 DPA に基づく処理、(c) 顧客の、MSA および DPA に抵触しない、合理的な書面上のあらゆる要求に基づく処理。 特に、Tealium は、本サービスの実行という特別な目的のためにのみ、個人データを取得し、使用し、あるいは開示する。本 DPA を締結することによって, Tealium は契約上の制限を理解し、またこれに従うことを保証する。 当セクション 2.4 の範囲外の処理については、かかる処理における追加指示に関して、Tealium と顧客間の事前の書面合意（Tealium が追加指示を実行する際にかかる追加費用の一切を、顧客が Tealium に支払う合意を含む）が必要となる。

2.4.3 顧客は、顧客の処理に関する指示が合法であること、個人データの処理が適用されるデータ保護法および規制に違反しないこと、あるいは Tealium がデータ保護法および規制に違反する事態を招かないことを確実にしなければならない。ある指示がデータ保護法および規制のあらゆる条項に抵触していると Tealium が判断した場合、Tealium は顧客に直ちに通知しなければならない。 その場合、顧客がかかる指示を確認するか、その指示を変更するまで、Tealium は指示に従う必要がないものとする。

2.5 **開示。** Tealium は、 MSA の条件によって明示的に許可される場合、ならびに適用法および規制あるいは法務執行機関の有効で拘束力のある命令（召喚命令や裁判所命令など）に従う必要がある場合を除いて、個人データを第三者に開示しない。法務執行機関が Tealium に個人データの開示命令を送った場合、Tealium は、法務執行機関が直接顧客に当該データの開示を再要求するよう試みる。この試みの一部として、Tealium は法務執行機関に顧客の基本連絡情報を提供することができる。法務執行機関に個人データを開示する必要がある場合、顧客が秘密保持命令またはその他の適切な救済を求めることができるよう、Tealium は顧客にかかる要求の合理的な通知をする

public interest. Tealium will not sell Personal Data.

2.4.2 Customer instructs Tealium to process Personal Data for the following purposes: (a) processing in accordance with the MSA; (b) processing in accordance with this DPA; and (c) processing to comply with any reasonable written request from Customer that are consistent with the terms of the MSA and this DPA. In particular Tealium will retain, use or disclose Personal Data only for the specific purpose of performing the Services. By entering into this DPA, Tealium certifies that it understands its contractual restrictions and shall comply with them. Processing outside the scope of this Section 2.4 (if any) will require prior written agreement between Tealium and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to Tealium for carrying out such instructions.

2.4.3 Customer shall ensure its processing instructions are lawful and that the processing of Personal Data in accordance with such instructions will not violate applicable Data Protection Laws and Regulations or cause Tealium to be in breach of Data Protection Laws and Regulations. Tealium shall immediately inform Customer if, in its opinion, an instruction infringes any provision of Data Protection Laws and Regulations. In such case, Tealium is not obliged to follow the instruction unless and until Customer has confirmed or changed such instruction.

2.5 Disclosure. Tealium will not disclose Personal Data to any third party other than as expressly permitted by the terms of the MSA, and except as necessary to comply with applicable laws and regulations or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Tealium a demand for Personal Data, Tealium will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Tealium may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then Tealium will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Tealium is legally prohibited from doing so.

3. Tealium Personnel.

3.1 Confidentiality, Reliability, and Limitation

（Tealium が法的に禁止される場合を除く）。

3. Tealium の人員。

3.1 **秘密保持、信頼性、およびアクセスの制限。** Tealium は、個人データを処理する権限を与えられた Tealium の人員が、秘密保持およびデータ保護とデータセキュリティーに関する関連義務を含む適切な契約的義務を果たすこと、またはかかる人員が適切な秘密保護の法定義務に拘束されていることを保証する。Tealium は、個人データの処理に携わる Tealium の人員の信頼性を保証するため合理的な措置を講じる。Tealium は、データセキュリティー規定に示される通り Tealium が承認しない限り、Tealium の人員による個人データの処理を制限する。

3.2 **訓練。** Tealium は、Tealium の人員が個人データに関する責務における適切な訓練を受けていることを保証する。

3.3 **データ保護担当者。** Tealium はデータ保護担当者を指定した。指定された担当者には、dpo@tealium.com から連絡することができる。

4. Tealium のその他の義務。 Tealium は、以下を実行する。:

4.1 最新鋭の技術水準、実装にかかる費用、処理の性質・範囲・コンテキストおよび目的、ならびに自然人の権利および自由に係る可変的可能性と重大性を考慮し、かかるリスクに見合ったレベルのセキュリティーを提供するためにデザインされた適切な技術的かつ組織的措置を講じる。かかる措置は、最低でも、データセキュリティー規定に定義される条件を満たす。

4.2 サブプロセッサーの雇用において本 DPA セクション 10 に参照される条件を尊重する。

4.3 処理の性質を考慮し、本 DPA セクション 5 に示される通り、データ保護法および規制に基づく、データ主体の権利に関する要求に対する顧客の応答義務の履行のため、可能な限り、技術的かつ組織的措置によって顧客を補助する。

4.4 処理の性質および Tealium に開示された情報を考慮し、データ保護法および規制に基づく顧客の義務（処理時のセキュリティー、データ漏洩の通知、プライバシー影響評価、および監督当局へ

of Access. Tealium will ensure that its personnel authorized to Process Personal Data have committed themselves to appropriate contractual obligations, including relevant obligations regarding confidentiality, data protection and data security, or are under an appropriate statutory obligation of confidentiality. Tealium will take reasonable steps to ensure the reliability of Tealium personnel engaged in the Processing of Personal Data. Tealium restricts its personnel from Processing Personal Data without authorization by Tealium as described in the Data Security Statement.

3.2 Training. Tealium will ensure that its personnel have received appropriate training on their responsibilities concerning Personal Data.

3.3 Data Protection Officer. Tealium has appointed a data protection officer. The appointed person can be reached at dpo@tealium.com.

4. Other obligations of Tealium. Tealium will:

4.1 take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risk. Such measures shall, at a minimum, meet the specifications set forth in the Data Security Statement;

4.2 respect the conditions referred to in Section 10 of this DPA for engaging a sub-processor;

4.3 take into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to requests regarding data subject rights under Data Protection Laws and Regulations as described in Section 5 of this DPA;

4.4 take into account the nature of processing and the information available to Tealium, assist Customer in ensuring compliance with its obligations under Data Protections Laws and Regulations with regard to security of processing, data breach notification, conducting privacy impact assessments and cooperation with supervisory authorities.

5. Customer Controls and Data Subject rights.

の協力に関する義務）の履行を補助する。

5. 顧客の制御権およびデータ主体の権利。

5.1 **顧客の制御権。** 本サービスは、顧客が、個人データを収得し、修正し、削除し、もしくはブロックし、またデータ主体の要求（以下定義）に応答する権限を与える。Tealium は、顧客が使用すると決めた場合に利用可能な、特定のセキュリティー機能と機能性を **提供する。顧客は、以下の適切な実行に責任を負う。**(a)本サービスのコンフィギュレーション、(b) 本サービスに関連して可能な制御権（セキュリティーコントロールを含む）の使用、(c) 個人データの適切なセキュリティー、保護、およびバックアップのために、顧客が適切であると判断した措置（不正アクセスから個人データを保護するための暗号化技術の使用、および個人データの定期的アーカイブも含まれうる）の実行。

5.2 **データ主体の権利。** Tealium が、顧客に関連していると Tealium が知るところのデータ主体に要求を受けた際には、データ主体の（情報へ）アクセスする権利・改正する権利・処理の制限・削除（「忘れられる権利」）・データポータビリティ・処理の拒否・または自動処理による個人に関する決定を行使するため、Tealium は、法的に許される限りすみやかに顧客に通知する（「データ主体の要求」）。さらに、本サービスを使用している顧客がデータ主体の要求にアクセスできない場合、（Tealium が法的に許される限り、またデータ保護法および規制に基づいてかかるデータ主体の要求への応答が必要である限り、）Tealium は、顧客の要請を受けて、データ主体の要求への顧客の回答を援助する。

6. 個人データの転送。

リージョン。 顧客は、以下のリストに挙げられる Tealium のネットワーク内の、個人データ（ユーザーデータを除く）がホストされる場所を選ぶことができる（かかるリストは Tealium によって随時更新される）。(i) 米国カリフォルニア州(ii) 米国バージニア州 (iii) アイルランド　ダブリン(iv)ドイツ　フランクフルト(v)日本　東京 (vi)オーストラリア　シドニー (それぞれ「**リージョン**」という)。顧客が本サービスを適切に設定してリージョンをいったん決めると、顧客の追加指示なしに、または、セクション 2.5 に示される通り法律あるいは法務執行機関の有効で拘束力のある命令（召

5.1 Customer Controls. The Services provide Customer with controls to enable Customer to retrieve, correct, delete, or block Personal Data and to respond to Data Subject Requests as defined below. Tealium makes available certain security features and functionalities that Customer may elect to use. Customer is responsible for properly (a) configuring the Services, (b) using the controls available in connection with the Services (including the security controls), and (c) taking such steps as Customer considers adequate to maintain appropriate security, protection, deletion and backup of Personal Data, which may include use of encryption technology to protect Personal Data from unauthorized access and routine archiving of Personal Data.

5.2 Data Subject Rights. Tealium shall, to the extent legally permitted, promptly notify Customer if Tealium receives a request from a data subject known to Tealium to be associated with Customer, to exercise the data subject's right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, object to the processing, or its right not to be subject to an automated individual decision making (**"Data Subject Request"**). In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Tealium will upon Customer's request provide assistance to Customer in responding to such Data Subject Request, to the extent Tealium is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations.

6. Transfers of Personal Data.

Regions. Customer may specify the location(s) where Personal Data, not including User Data, will be hosted within the Tealium Network from the following list, as updated by Tealium from time to time: (i) California, USA; (ii) Virginia, USA; (iii) Dublin, Ireland; (iv) Frankfurt, Germany; (v) Tokyo, Japan; and (vi) Sydney, Australia (each a **"Region"**). Once Customer has made its choice, by properly configuring the Services, Tealium will not transfer the hosting of Personal Data from Customer's selected Region(s) except under Customer's further instructions or as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order) as described in Section 2.5. User Data will be hosted in California, USA in all cases.

喚命令や裁判所命令など）に従う必要がある場合を除いて、Tealium は、顧客の選定したリージョンから個人データのホストを転送しない。ユーザーデータは、すべてのケースにおいて米国カリフォルニア州にてホストされる。	
7. Tealium のセキュリティー責任。	**7. Security Responsibilities of Tealium.**
7.1 **継続的評価。** 本 DPA セクション 4.1 に基づく義務に加え、Tealium は、自身のインフラストラクチャ、アプリケーション、および関連する本サービスのセキュリティーを定期的に評価する。Tealium の情報セキュリティープログラムの適性は、業界のセキュリティー基準、および Tealium の方針と手順への準拠に対して評価される。Tealium は、Tealium のネットワークおよび関連する本サービスのセキュリティーを継続的に評価し、新しいセキュリティーの脅威、または定期的な審査によって明らかになる発見に対応するために、セキュリティーの措置の追加または緩和の必要性があるかどうかを決定する。**Tealium は、継続的脆弱性のテストおよび年次の侵入テストによって、欠陥を検知し、また欠陥があった場合その修復を行う。Tealium のネットワークおよび関連する本サービスは、セキュリティーインシデントの発生または発生の可能性において継続的に監視される。Tealium はまた、少なくとも年に一度、または環境に重大な変化が起きた場合にリスク査定を行う。これらの措置は、情報セキュリティープログラムの継続的改良のために講じられる。**	**7.1 Continued Evaluation**. In addition to its obligations under Section 4.1 of this DPA, Tealium will conduct periodic reviews of the security of its infrastructure, applications, and associated Services. The adequacy of Tealium's information security program is measured against industry security standards and compliance with Tealium's policies and procedures. Tealium will continually evaluate the security of the Tealium Network and associated Services to determine whether additional or mitigating security measures are required to respond to new security risks or findings generated by the periodic reviews. Tealium conducts ongoing vulnerability scans and annual penetration tests to identify and then remediate identified deficiencies. The Tealium Network and associated Services are continuously monitored for events and potential Security Incidents. Tealium also conducts risk assessments at least annually or when significant changes to the environment occur. These activities provide for a continually improving information security program.
7.2 **顧客の独自の審査。** 顧客は、以下の点について単独で責任を負う。：データセキュリティーに関して Tealium に開示された情報を審査し、また本サービスが顧客の要求を満たすかどうかを独自に判断すること、および顧客の人員と相談役がデータセキュリティーに関して提供されたガイドラインに従うことを保証すること。	**7.2 Customer Independent Review**. Customer is solely responsible for reviewing the information made available by Tealium relating to data security and making an independent determination as to whether the Services meet Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security**.**
8. サティフィケーションおよび監査。	**8. Certifications and Audits.**
8.1 **Tealium の監査。** Tealium は、少なくとも年に一度、自身のセキュリティー対策の監査を行う。これらの監査は、ISO 27001、ISO 27018 、および SOC 2 タイプ II の基準、またはこれらの基準に実質的に同等の、その他のだいたい基準に基づいて行われる。これらの監査は、Tealium の選定と費用負担によって、第三者のセキュリティー専門家によって行われる。	**8.1 Tealium Audits.** Tealium audits its security measures at least annually. These audits: will be performed according to ISO 27001, ISO 27018 and SOC 2 Type II standards or such other alternative standards that are substantially equivalent to such standards. These audits will be performed by independent third party security professionals at Tealium's selection and expense.
	8.2 Audit Reports. At Customer's written request, Tealium will provide Customer with a confidential report so that Customer can reasonably verify Tealium's compliance with its obligations under this DPA. The report constitutes Tealium's Confidential Information.

8.2 **監査の報告。** 顧客の要請を受けた場合、顧客が、本 DPA に基づく Tealium の義務を果たしているかを合理的に検証することができるよう、Tealium は、顧客に機密報告書を提出する。かかる報告書は Tealium の本秘密情報を構成する。	**8.3 AWS and Customer Audits.** Customer audits rights are as set forth in the DSS.
8.3 **AWS および顧客の監査。**顧客の監査に関する権利は、DSS に定義される。	
9. セキュリティーインシデントの通知。	**9. Security Incident Notification.**
9.1 **Tealium の通知。** Tealium がセキュリティーインシデントを確認した場合、不当な遅延なしに、可能な場合、確認した時点から 48 時間以内に顧客にセキュリティーインシデントの通知をする。48 時間以内に顧客が通知を受けなかった場合、遅延の理由がなければならない。	**9.1 Tealium Notification.** If Tealium becomes aware of a Security Incident, Tealium will without undue delay and, where feasible, not later than 48 hours after having become aware of it, notify Customer of the Security Incident. Where the notification to the Customer is not made within 48 hours, it shall be accompanied by reasons for the delay.
9.2 セクション 9.1 にある通知には少なくとも以下の点が含まれなければならない。:	**9.2** The notification referred to in Section 9.1 shall at least:
9.2.1 セキュリティーインシデントの性質の説明	**9.2.1** describe the nature of the Security Incident;
9.2.2 データ保護担当者またはより多くの情報が得られるその他の者の氏名と連絡先の詳細、および	**9.2.2** communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
9.2.3 Tealium がセキュリティーインシデントを是正するために講じた、または申し出た措置（悪影響が出る可能性がある場合、これを最低限に抑える適切な措置を含む）の説明。	**9.2.3** 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.
9.3 情報の同時提供が不可能な場合、過度の遅延なく、段階ごとに情報を提供することができる。	**9.3** 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.
9.4 Tealium は、あらゆるセキュリティーインシデント、セキュリティーインシデントに関する周辺事実、その影響および講じられた是正措置を文書化しなければならない。かかる文書は、顧客が当セクションへの準拠を確認することができるものでなければならない。	**9.4** 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.
9.5 **Tealium のサポート。**データ保護法および規則に基づいて顧客が要求される、あらゆる個人データ漏洩の通知に関して顧客をサポートするため、Tealium は、セクション 9.1 に基づき、Tealium が顧客に合理的に開示できる情報を通知に含む。その際 Tealium は、本サービスの性質、Tealium が知ることができる情報、および機密情報など情報開示のあらゆる制限を考慮する。	**9.5 Tealium Assistance.** To assist Customer in relation to any personal data breach notifications Customer is required to make under the Data Protection Laws and Regulations, Tealium will include in the notification under section 9.1 such information about the Security Incident as Tealium is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Tealium, and any restrictions on disclosing the information, such as confidentiality.
	9.6 Limitations. Customer agrees that:
	9.6.1 An Unsuccessful Security Incident will not be subject to this Section; and

9.6 **制限。**顧客は以下の点に合意する。:	**9.6.2** Tealium's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Tealium of any fault or liability of Tealium with respect to the Security Incident.
9.6.1 未然の**セキュリティーインシデントは当セクションの対象にならないこと。**	**9.7 Delivery.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any reasonable means Tealium selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information with Tealium all times.
9.6.2 当セクションに基づく Tealium の**セキュリティーインシデントの報告または応対は、かかるセキュリティーインシデントに関する** Tealium の過失または責任の一切を、Tealium が認めたことにはならず、将来的にもそうならないこと。	**10. Sub-Processing.**
9.7 **送達。 セキュリティーインシデントの通知は、email を含む、**Tealium が選択するあらゆる合理的な方法によって、一人または複数の顧客の運営者に届けられる。Tealium に顧客の運営者の正しい連絡先を常に知らせておくことは、顧客の単独の責任である。	**10.1 Authorized Sub-processors.** Customer agrees that Tealium may use AWS as a sub-processor to fulfill certain of its contractual obligations under this DPA or to provide certain services on its behalf. Tealium will inform Customer of any intended changes concerning the addition or replacement of sub-processors, thereby giving Customer the opportunity to object to such changes.
10. サブプロセス。	**10.2 Obligations in respect of sub-processors.** Where Tealium authorizes any sub-processor as described in this Section 10:
10.1 **権限を付与されたサブプロセッサー。** 顧客は、Tealium が本 DPA に基づく特定の契約的義務を果たすため、また Tealium を代表して特定のサービスを提供するため、Tealium がサブプロセッサーとして AWS を利用できることに同意する。Tealium は、サブプロセッサーの追加または変更を意図する場合、顧客がその変更に異議を申し立てることができるよう、顧客にその意図を通知する。	**10.2.1** Tealium will restrict the sub-processor's access to Personal Data only to what is necessary to maintain the Services or to provide the Services to Customer and Tealium will prohibit the sub-processor from accessing Personal Data for any other purpose;
10.2 **サブプロセッサーに関する義務。** 当セクション 10 に示される通り、Tealium がサブプロセッサーに権限を与える場合、Tealium は以下を実行する。:	**10.2.2** Tealium will impose appropriate contractual obligations in writing upon the sub-processor that are no less protective than this DPA, including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights; and
10.2.1 Tealium は、サブプロセッサーの個人データへのアクセスを、本サービスの維持または顧客に本サービスを提供するのに必要なアクセスのみに制限し、サブプロセッサーによるその他のあらゆる目的のための個人データへのアクセスを禁止する。	**10.2.3** Tealium will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processor that cause Tealium to breach any of Tealium's obligations under this DPA.
10.2.2 Tealium は、サブプロセッサーに 、書面による、本 DPA と同等かそれ以上の保護力のある、適切な契約義務を課す。かかる契約義務は、秘密保持、データ保護、データセキュリティーおよび監査の権利を含む関連した契約義務を含む。	**10.3 Objection to Sub-Processor.** If Customer has a reasonable basis to object to Tealium's use of a new sub-processor, Customer shall notify Tealium promptly in writing within ten (10) business days after receipt of Tealium's notice. If Customer objects to a new sub-processor(s)
10.2.3 Tealium は、本 DPA の義務の Tealium の履行、およびサブプロセッサーの作為または不作為	

を原因とする、本 DPA に基づく Tealium の義務の違反の一切に、継続的に責任を持つものとする。

10.3**サブプロセッサーへの異議。** 顧客が、Tealium による新しいサブプロセッサーの採用に対し、合理的な理由を持って異議を唱える場合、顧客は、Tealium の通知から 10 営業日以内に、すみやかに、Tealium にその旨書面通知しなければならない。顧客が新しいサブプロセッサーに反対する場合、Tealium は、合理的な努力を払って、影響のある本サービスの変更を顧客に申し出るか、あるいは顧客に非合理的な負担をかけずに、反対された新しいサブプロセッサーによる個人データの処理を避けるため、影響のある本サービスの顧客のコンフィギュレーションまたは使用の、商業上合理的な変更を推奨する。Tealium が、かかる変更を合理的な期間内（60 日を超えないものとする）に提供できなかった場合、顧客は、Tealium に書面通知することで、反対された新しいサブプロセッサーの使用なしに Tealium が提供できなかった本サービスに関してのみ、本サービス注文書を解約することができる。顧客は、かかる解約された本サービスに関して、解約成立日後の期間分、前払いした料金を返金されるものとする。

11. 通知義務。 破産または債務超過の手続き上、または第三者による同様の措置の過程で、個人データが Tealium の処理中に没収対象になった場合、Tealium は、不当な遅延なしに顧客に通知する。Tealium は、不当な遅延なしに、かかる手続きにおけるすべての関連当事者（債権者や破産管財人など）に、かかる手続きの対象となる個人データの一切が、顧客の財産かつ責任範囲であり、また個人データは顧客の単独に処分されることを通知する。

12. DPA の解約。本 DPA は、 MSA の解約日（「本解約日」）まで 有効である。

13. 顧客の個人データの返却および消去。 本サービスは、顧客に、個人データの収得または消去のために使用されうるの制御権を付与する。本解約日まで、顧客は、当セクションに従って個人データを収集または削除することができる。顧客が、本サービスの利用を通じて自力で個人データの収集または削除ができなかった場合、Tealium は、顧客の書面上の要請により、顧客によるかかる収集または削除をサポートする。Tealium は、本解約日から 180 日以内に個人データを消去する。

Tealium will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's configuration or use of the affected Services to avoid Processing of Personal Data by the objected-to new sub-processor without unreasonably burdening Customer. If Tealium is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Service Order in respect only to those Services that cannot be provided by Tealium without the use of the objected-to new sub-processor, by providing written notice to Tealium. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

11. Duties to Inform. If Personal Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by Tealium, Tealium will inform Customer without undue delay. Tealium will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Personal Data subjected to those proceedings is Customer's property and area of responsibility and that Personal Data is at Customer's sole disposition.

12. Termination of the DPA. This DPA shall continue in force until the termination of the MSA (the "Termination Date").

13. Return and Deletion of Customer Personal Data. The Services provide Customer with controls that Customer may use to retrieve or delete Personal Data. Up to the Termination Date, Customer will continue to have the ability to retrieve or delete Personal Data in accordance with this Section. To the extent Customer is unable to retrieve or delete Personal Data itself through its use of the Services, Tealium will assist Customer in such retrieval or deletion upon Customer's written request. Tealium will delete Personal Data within 180 days following the Termination Date.

14. Fees and Expenses. To the extent legally permitted, Customer shall be responsible for any costs and fees arising from a request by Customer to change the Region originally chosen by Customer during configuration of its account(s) pursuant to Section 6.1 above.

14. 料金および費用。法で許される限り、上記セクション 6.1 に従って、顧客は、自身のアカウントのコンフィギュレーション中に最初に選定したリージョンの変更を顧客が要請した場合に発生する、あらゆる費用と料金を負うものとする。 **15. 非開示。** 顧客は、本 DPA は公開されたものではなく、本 DPA がまた MSA の秘密保護の条項に基づく Tealium の本秘密情報を構成することに同意する。 **16. 抵触。** 本 DPA で修正されない限り、MSA は有効に存続する。MSA と本 DPA に抵触がある場合、の条件が優先する。 **17. 副本、電子署名または Email による送達。** 本 DPA は、二部またはそれ以上の副本をもって締結されうる。それらのいずれについても原本とみなされ、かつ、当該副本のすべては、一個の、かつ同一の契約を構成する。両当事者は、電子署名または email の通信によって、本 DPA に署名し、送達することができる。	**15. Nondisclosure.** Customer agrees that the details of this DPA are not publicly known and constitute Tealium's Confidential Information under the confidentiality provisions of the MSA. **16. Conflict**. Except as amended by this DPA, the MSA will remain in full force and effect. If there is a conflict between the MSA and this DPA, the terms of this DPA will control. **17. Counterparts; Electronic Signature or Email Delivery**. This DPA may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties may sign and deliver this DPA by electronic signature or email transmission.