Published date: March 25, 2024

Secureworks®

データ保護特約
DATA PROTECTION ADDENDUM

データ保護特約（Data Protection Addendum、「**DPA**」）及び**SCC**（以下に定義）は、該当する場合、Secureworksとお客様との間で締結された契約（「**CRA**」）の一部を構成します。別途明記される場合を除き、DPAは、Secureworksが本サービスに関連して、お客様のために「**個人データ**」(以下に定義)の処理をデータ処理者として行う場合に適用されます。別途明記される場合を除き、CRAに基づいて処理される個人データについて、お客様は「データ管理者」となり、Secureworksは「データ処理者」となります。DPAとCRAの条項が抵触する場合、DPAの範囲においてDPAが優先するものとします。
This Data Protection Addendum ("**DPA**") and the SCCs (as defined below), if applicable, are incorporated by reference into and form part of the CRA. Except as expressly stated, this DPA applies solely where Secureworks processes Personal Data (as defined below) as a processor on behalf of the Customer in connection with the provision of Services. Except as otherwise expressly stated, Customer is the controller and Secureworks is the processor (as defined below) of the Personal Data processed under the CRA. In the event of a conflict between this DPA and the CRA, this DPA shall control with respect to its subject matter.

1. **定義** DPAにおいて使用される「データ管理者」、「データ主体」、「パーソナルデータ」、「データ処理者」、「処理」(及びその派生語)及び「監督当局」という用語は、EU一般データ保護規則（General Data Protection Regulation 2016/679、「GDPR」）において定義された意味と同じ意味を有するものとします。「事業者」、「消費者」、「販売」、「事業目的」及び「商業目的」という用語は、カリフォルニア州消費者プライバシー法 (the California Consumer Privacy Act of 2018、「CCPA」) において定義された意味と同じ意味を有するものとします。DPAにおいて定義されていない用語は、CRAの定義に従うものとします。DPAにおいて参照される別紙は、DPAの別紙を指すものとします。 DPAにおいて：
Definitions: References in this DPA to "**controller**", "**data subject**", "**personal data**" (lower cased), "**processor**", "**processing**" (and its derivatives) and "**supervisory authority**" shall have the meanings ascribed to them under the General Data Protection Regulation 2016/679 (the "**GDPR**"). References to "**business**", "**consumer**", "**sell**", "**business purpose**" and "**commercial purpose**" shall have the meanings ascribed to them under the California Consumer Privacy Act of 2018 (the "**CCPA**"). Capitalized terms not defined in this DPA shall have the meaning set out in the CRA. References in this DPA to Schedules are to the Schedules to this DPA. In this DPA:

   1.1 「**データ侵害**」とは、SecureworksがDPAに基づくセキュリティ義務に実際に違反したことにより生じた、伝送、保管、その他の手段により処理された、偶発的又は不正な個人データの毀損、消失、変更、漏洩又はアクセスを意味します。
   "**Data Breach**" means an actual breach by Secureworks of the security obligations under this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored or otherwise processed.

   1.2 「**個人データ**」とは、特定の個人又は世帯を識別し、関連し、叙述し、関連付けることができ、又は直接的に若しくは間接的に合理的にリンクさせることのできる、Secureworksがお客様のデータ処理者として本契約上の義務の履行を見越して、関連して、又は偶発的に処理した情報を意味するものとします。個人データには、CCPA140条(o)(1)(A)-(K)項に列記されたデータ要素に限定されず、特定の個人又は世帯を識別し、関連し、叙述し、関連付けることができ、又は直接的に若しくは間接的に合理的にリンクさせることのできるものを含むものとします。
   "**Personal Data**" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, which is processed by Secureworks, acting as a processor on behalf of the Customer in anticipation of, in connection with or incidental to the performance of the CRA. Personal Data includes, but is not limited to, the data elements listed in section 140(o)(1)(A)-(K) of the CCPA, if any such data element identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household.

   1.3 「**プライバシー法**」とは、CRAの各当事者が規制の対象となる、又は、本サービスに係るすべてのデータ保護及びプライバシーに関する法律、法令、指令その他の規制（改正法を含む）を意味します。日本の個人情報の保護に関する法律、GDPR、英国データ保護法2018（「**英国DPA**」）、英国版GDPR（英国DPA第3条の定義に従う）及びCCPAを含みますが、これらに限られないものとします。
   "**Privacy Laws**" means any data protection and/or privacy related laws, statutes, directives, or regulations (and any amendments or successors thereto) to which a party to the CRA is subject and which are applicable to the Services including without limitation the GDPR, the United Kingdom Data Protection Act 2018 ("**UK DPA**"), the UK GDPR (as defined in section 3 of the UK DPA), and the CCPA.

   1.4 「**SCC**」又は「**標準契約条項**」とは、DPA別紙3で参照する、2021年6月4日付で欧州委員会から発行された標準契約条項（2021/914）（モジュール1: データ管理者からデータ管理者、モジュール2: データ管理者からデータ処理者）を意味するものとし、DPA別紙3の2022年3月21日付英国の個人データの移転に関する欧州委員会標準契約条項に対する国際データ移転特約及びスイスに関する特約によって (必要に応じて) 修正されるものとします。
   "**SCCs**" or "**Standard Contractual Clauses**" means Module One (controller to controller) and Module Two (controller to processor) of the Standard Contractual Clauses issued by the European Commission on 4 June 2021 (2021/914) as referenced in Schedule 3, and as amended (where appropriate) by the International Data Transfer Addendum to the EU

Commission Standard Contractual Clauses for UK transfers of Personal Data dated 21 March 2022 and/or the country specific provisions for Switzerland set out in Schedule 3.

1.5 「**セキュリティイベント・データ**」とは、本サービスの提供に関連してSecureworksが収集する、セキュリティイベントに関する情報を意味します。
"**Security Event Data**" means information related to security events which is collected during Secureworks' provision of Services.

1.6 「**復処理者**」とは、個人データの処理に関連してSecureworksに関与する、Secureworksの関連会社、委託先を含む、第三者を意味します。
"**Subprocessor**" means a third party engaged by Secureworks (including without limitation an Affiliate and/or subcontractor of Secureworks) in connection with the processing of Personal Data.

2. **処理の内容** CRA及びDPAに基づいて行われる処理の内容は、別紙1に記載の通りとします。
Description of processing: Schedule 1 sets out a description of the processing activities to be undertaken as part of the Services to be provided under the CRA and this DPA.

3. **法律の遵守** 両当事者は、プライバシー法に規定される各々の義務を遵守するものとします。特に、お客様は、自己又は（関係する場合は）各関連会社のために、Secureworksが、プライバシー法に従って、DPA及びCRAに基づいて本サービスを提供するために必要なすべての許可及び同意を取得し、それを維持することを表明し、保証します。
Compliance with laws: the parties agree to comply with their respective obligations under Privacy Laws. In particular, Customer warrants and represents (on its behalf and on behalf of each of its Affiliates where applicable) that it has obtained and will maintain all necessary authorizations and consents required to enable Secureworks to provide the Services and process the Personal Data pursuant to this DPA and CRA in accordance with Privacy Laws.

4. **Secureworksの義務**
Secureworks obligations

4.1 **指示** Secureworksは、（法令上の要請がない限り）個人データをお客様の適切で正当な指示に基づいて処理するものとします。お客様は、Secureworksに対して、本サービスを提供するために個人データを処理及び移転し、SecureworksのCRA及びDPAに基づく権利及び義務に従うよう指示するものとします。CRA及びDPAは、個人データの処理に関するSecureWorksに対するお客様のすべての指示を構成するものとします。両当事者間における指示の追加又は変更は、書面により合意されるものとし、指示に従うことによって追加の費用が生じる場合は、費用の取扱いについて取り決めるものとします。お客様は、お客様のSecureworksに対する指示が適用される法律（プライバシー法を含むが、これに限られない）を遵守していることを単独で保証し、当該指示にSecureworksが従ったことによって生じた結果について単独で責任を負うものとし、Secureworksは、このような行為によって債務不履行とはならないものとします。ただし、Secureworksが、お客様の指示が、適用されるプライバシー法の規定に反するという意見を有する場合、お客様に対して合理的に速やかにその旨をお客様に通知することにより、当該指示に従う義務を負わないものとします。
Instructions: Secureworks shall process the Personal Data only in accordance with Customer's reasonable and lawful instructions (unless otherwise required to do so by applicable law). Customer hereby instructs Secureworks to process and transfer the Personal Data in order to provide the Services and comply with Secureworks' rights and obligations under the CRA and this DPA. Any additional or alternate instructions must be agreed between the parties in writing, including the costs (if any) associated with complying with such instructions. Customer is solely responsible for ensuring its instructions comply with applicable law (including without limitation Privacy Law) and is solely responsible for the consequences of Secureworks complying with such instructions and Secureworks shall not be in default by doing so. However, if Secureworks is of the opinion that a Customer instruction infringes applicable Privacy Laws, Secureworks shall notify Customer as soon as reasonably practicable and shall not be required to comply with such instruction.

4.2 **機密保持義務** Secureworksは、個人データをCRAに基づき機密情報として取り扱うものとし、個人データにアクセスする権限を持つ者（復処理者を含む）に対して、本条に定める義務と同等の義務を課すものとします。
Confidentiality: Secureworks shall maintain the confidentiality of the Personal Data in accordance with the CRA and shall require persons authorized to process the Personal Data (including its Subprocessors) to have committed to materially similar obligations of confidentiality.

4.3 **開示** Secureworksは、次の各号に定める場合、個人データを第三者（関連会社及び復処理者を含む）に開示することができるものとします。
Disclosures: Secureworks may only disclose the Personal Data to third parties (including without limitation its Affiliates and Subprocessors) for the purpose of:

(a) お客様の合理的で正当な指示に従う場合
complying with Customer's reasonable and lawful instructions

(b) 本サービスの提供に関連し、CRA及びDPAによって許諾されている場合
as required in connection with the Services and as permitted by the CRA and/or this DPA, and/or

(c) プライバシー法を遵守するために必要な場合、又はSecureworks及びSecureworksの関連会社もしくは復処理者に対して管轄権を有する裁判所、審判機関、規制当局、政府当局から開示を要求された場合。
to the extent required to comply with Privacy Laws, or an order of any court, tribunal, regulator or government agency with competent jurisdiction to which Secureworks, its Affiliates and/or Subprocessors is subject.

4.4 **データ主体の権利に関する支援** Secureworksは、本サービスに関して、データ主体が個人データに関して（アクセス、変更及び消去を含むがこれらに限定されない）プライバシー法に基づく権利を行使した場合に、お客様が要求に応じる上で、合理的な範囲において支援するものとします。Secureworksは、当該支援に費用が一定額以上を要する場合、お客様に対して請求する権利を有するものとします。Secureworksは、データ主体及び消費者からCRAの有効期間内に個人データに関連して適用されるプライバシー法に基づく権利の行使について要求を受けたときは、お客様に対して合理的に速やかに通知するものとします。
Assisting with data subject rights: Secureworks shall, as required in connection with the Services and to the extent reasonably practicable, assist Customer to respond to requests from data subjects and consumers exercising their rights under Privacy Laws (including without limitation the right of access, rectification and/or erasure) in respect of the Personal Data. Secureworks may charge Customer for such assistance if the cost of assisting exceeds a nominal amount. Secureworks shall forward to Customer as soon as practicable any data subject rights requests Secureworks receives from Customer's data subjects.

4.5 **セキュリティ** Secureworksは、業界標準、実施に掛かる費用、性質、範囲、文脈及び処理の目的、その他個人データの処理に関連する状況を考慮し、GDPR第32条（又は、その他のプライバシー法に規定された同等の条項）に定める措置を講じるものとします。両当事者は、別紙2（情報セキュリティ基準）の内容が、本条に定める個人データの適切なセキュリティ保護基準を満たすことを合意します。
Security: Taking into account industry standards, the costs of implementation, the nature, scope, context and purposes of the processing and any other relevant circumstances, Secureworks shall implement the measures required by GDPR Article 32 (or similar provision under other applicable Privacy Laws). The parties agree that the security measures described in Schedule 2 (Security Measures) provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause.

4.6 **復処理者** お客様は、以下の各号に従うことを条件に、Secureworksが本サービスの個人データを処理する復処理者（お客様ポータル又はクラウドサービス・ポータルに掲載され、随時更新されるリストにより特定される委託先）を指名し、利用することに同意します。ただし、Secureworksは、(a) 復処理者が行う業務の内容において、(b) DPAに基づいてSecureworksが負う義務と同等の義務を復処理者に課す内容の契約を復処理者との間で書面により締結するものとします。Secureworksが新しい復処理者の指名を提案する場合、Secureworksは、お客様に通知し（電子メール又はお客様ポータルもしくはクラウドサービス・ポータルに通知を掲載することを含みますが、これに限定されません）、当該通知がなされてから30日以内にお客様が当該指名に異議を申し立てられるようにするものとします。お客様は、合理的なデータ保護関連の理由でのみ、新しい復処理者の指名に異議を唱えることができるものとします。お客様が異議を申し立てた場合、両当事者は代替案に合意する合理的な努力をするものとします。両当事者が合意できない場合、お客様は、新しい復処理者の指名の影響を受けるすべての本サービスを終了することができるものとします。ただし、お客様は、Secureworksに30日前に書面で通知し、終了日以前に提供された本サービスについて支払うべきすべての料金を（CRAに準拠した支払条件で）Secureworksに支払うものとします。両当事者は、該当する場合、通知期間をより短くすることを合意できるものとします。 お客様がSecureworksの通知に対して、通知がなされてから30日以内に異議を唱えなかった場合、お客様は新しい復処理者の追加に同意したものとみなされます。
Subprocessors: Customer agrees that Secureworks may appoint and use Subprocessors (which are identified on the subprocessor list posted on the customer portal or the Cloud Services portal, as updated from time to time) to process the Personal Data in connection with the Services PROVIDED THAT Secureworks puts in place a contract in writing with each Subprocessor that imposes obligations that are (a) relevant to the services to be provided by the Subprocessors and (b) materially similar to the rights and/or obligations granted or imposed on Secureworks under this DPA. If Secureworks proposes to appoint a new Subprocessor, Secureworks shall notify Customer (including without limitation by email or by posting a notification on the customer portal or the Cloud Services portal) and allow Customer to object to such appointment within 30 days of such notification being made. Customer may only object to the appointment of a new Subprocessor on reasonable data protection related grounds. If Customer objects, the parties shall use reasonable endeavours to agree alternative arrangements. If the parties cannot agree then Customer may terminate all Services affected by the appointment of the new Subprocessor subject to providing thirty (30) days written notice to Secureworks and making payment to Secureworks of any and all fees that are due and owing for any Services supplied prior to the termination date (on payment terms in accordance with the CRA). The parties may agree a shorter period of notice if applicable. Failure by Customer to object to Secureworks' notification within thirty (30) days from the notification being made will be deemed to be Customer's agreement to the addition of the new Subprocessor.

4.7 **個人データの消去**（理由の如何を問わず）本サービスが終了し、お客様から書面による要求があった場合、Secureworksは合理的に速やかに個人データを消去するものとします。ただし、Secureworksは、(a) 法律、規制、司法、監査、社内コンプライアンスの要請に基づき、必要な範囲で１部の複製物を保持できるものとし、(b) 個人データ又はその複製物をSecureworksのシステムから消去することが合理的かつ実務上できない場合、当該期間、消去を延期することが出来るものとします。本条 (a) 又は (b) に基づいて消去を延期している間、DPAの規定が引き続き適用されるものとします。(i)SCCモジュール2 第8.5条 (処理の期間及びデータの消去又は返却) 、及び(ii)SCC第16(d)条（標準契約条項の非遵守及び解除）において、お客様は、本サービス又はDPAが（理由を問わず）終了したとき、個

人データが削除される（お客様に返却されない）ことを選択するものとし、Secureworks は、お客様から書面で要求された場合にのみ、個人データの削除を証明するものとします。

Deletion of Personal Data: Upon termination of the Services (for any reason) and if requested by Customer in writing, Secureworks shall as soon as reasonably practicable delete the Personal Data, PROVIDED THAT Secureworks may: (a) retain one copy of the Personal Data as necessary to comply with any legal, regulatory, judicial, audit or internal compliance requirements; and/or (b) defer the deletion of the Personal Data to the extent and for the duration that any Personal Data or copies thereof cannot reasonably and practically be expunged from Secureworks' systems. The provisions of this DPA shall continue to apply to Personal Data that is retained by Secureworks pursuant to this clause. For the purpose of (i) the SCCs, Module Two, Clause 8.5 (*Duration of processing and erasure or return of data*) and (ii) the SCCs, Clause 16(d) (*Non-compliance with the Clauses and termination*), the Customer elects that upon termination (for any reason) of the Services or this DPA, the Personal Data will be deleted (and not returned to Customer) and Secureworks will only be required to certify the deletion of the Personal Data if requested in writing by Customer.

4.8 **DPA遵守状況の報告** Secureworksは、お客様から合理的な書面による要請を受けた場合（ただし12か月に1度の頻度を超えないものとします）、SecureworksがDPAに基づく義務を遵守していることを証明するために合理的に必要な情報をお客様に提供します。

Demonstrating compliance: Secureworks shall, upon reasonable prior written request from Customer (such request not to be made more frequently than once in any twelve-month period), provide to Customer such information as may be reasonably necessary to demonstrate Secureworks' compliance with its obligations under this DPA.

4.9 **監査及び検査** お客様は、第4.8条に基づいてSecureworksが提供した情報がSecureworksのDPA遵守状況の証明として十分ではないと合理的に判断する場合、関連するSecureworksの処理に関するDPAの遵守状況を監査又は検査する目的で、次の各号に従い、関連するSecureworksの処理に関する活動への合理的なアクセスを要請することができるものとします。

Audits and inspections: Where Customer reasonably believes the information provided under clause 4.8 above is not sufficient to demonstrate Secureworks' compliance with this DPA, Customer may request reasonable access to Secureworks' relevant processing activities in order to audit and/or inspect Secureworks' compliance with this DPA PROVIDED THAT:

(a) お客様は、Secureworksに対して、監査又は検査の30日以上前に合理的な書面による通知を行うものとします（ただし、プライバシー法、監督当局の命令、両当事者間の合意、データ侵害が発生した場合に、本項の定めより短い期間が適用される場合は、この限りではないものとします。）
Customer gives Secureworks reasonable prior written notice of at least thirty (30) days before any audit or inspection (unless a shorter notice period is required by Privacy Laws, an order of a supervisory authority, otherwise agreed between the parties, or in the event of a Data Breach);

(b) 監査又は検査は、12 か月に1 回という頻度を上回る頻度で行われないものとします。（ただし、プライバシー法、監督当局の命令、両当事者間の合意、データ侵害が発生した場合に、当該頻度を上回る場合は、この限りではないものとします。）
audits or inspections may not be carried out more frequently than once in any twelve-month period (unless required more frequently by Privacy Laws, an order of a supervisory authority, otherwise agreed between the parties, or in the event of a Data Breach);

(c) お客様は、Secureworksに対し、監査希望日の2週間以上前に、監査の範囲、監査期間、監査開始日を記載した詳細な監査計画書を提出するものとします。Secureworksは、当該監査計画書を確認し、重要な懸念や質問事項を遅滞なくお客様に連絡するものとし、その後、両当事者は、最終的な監査計画を合意するものとします。
Customer submits to Secureworks a detailed audit plan at least two (2) weeks in advance of the proposed audit date describing the proposed scope, duration and start date of the audit. Secureworks shall review the audit plan and provide Customer with any material concerns or questions without undue delay. The parties will then reasonably cooperate to agree a final audit plan;

(d) Secureworksは、調査を実施しつつ、法令及び第三者との秘密保持義務に違反しない目的で、情報へのアクセスを制限することができるものとします。（セキュリティー・オペレーション・センターの見学者用スペースからガラス越しに見学することはできますが）、お客様及びお客様の監査人による、他のお客様のお客様データを取り扱っている機密性が高く立ち入りが制限されている区域へのお客様のアクセスは、法令により厳しく制限されます。お客様は、Secureworksのポリシー、管理基準、手続に関する機密性の高い資料又は内容を、監査又は検査が行われたSecureworksのオフィスに（電子的であるか物理的であるかを問わず）放置しないものとし、自己の監査人が当該条件に従うことを保証するものとします。
Secureworks may restrict access to information in order to avoid compromising a continuing investigation, violating law or violating confidentiality obligations to third parties. Any access to sensitive or restricted facilities by Customer is strictly prohibited due to regulatory restrictions on access to other customers' data, although Customer and/or its auditor shall be entitled to observe the security operations center via a viewing window). Customer shall not (and must ensure that its auditor shall not) allow any sensitive documents and/or details regarding Secureworks' policies, controls and/or procedures to leave the Secureworks location at which the audit or inspection is taking place (whether in electronic or physical form);

(e) お客様は、監査又は検査をSecureworksの通常の業務時間中に実施するものとし、Secureworksの業務を中断させないものとします。
Customer carries out the audit or inspection during normal business hours and without creating a business interruption to Secureworks;

(f) 監査又は検査は、Secureworksの関連する施設におけるポリシー及び手続に従って行われるものとします。
the audit or inspection is carried out in compliance with Secureworks' relevant on-site policies and procedures;

(g) お客様のために第三者が監査を実施する場合、当該第三者はCRAと同等の秘密保持義務に服するものとし、かつ、SecureWorksの直接の競合ではないものとします。Secureworksは、当該第三者が監査を実施する前に、直接当該第三者との間で機密保持に関する契約書を締結する権利を留保するものとします。
where the audit is carried out by a third party on behalf of the Customer, such third party is bound by similar obligations of confidentiality to those set out in the CRA and is not a direct competitor of Secureworks. Secureworks reserves the right to require any such third party to execute a confidentiality agreement directly with Secureworks prior to the commencement of an audit or inspection; and

(h) 当該監査又は検査によりSecureworksがDPAに定める義務に違反していたことが判明した場合を除き、お客様は、Secureworksが第4.9条の定めに従うために発生した合理的な費用（Secureworksが監査に対応した時間に対し、Secureworks、社員及び専門家に対して発生した費用を含む）を負担するものとします。
except where the audit or inspection discloses a failure on the part of Secureworks to comply with its material obligations under this DPA, Customer shall pay all reasonable costs and expenses (including without limitation any charges for the time engaged by Secureworks, its personnel and professional advisers) incurred by Secureworks in complying with this clause 4.9.

お客様は、適用される法令により禁止されていない限り、第4.9条に基づいて実施した監査報告書の写しを一部Secureworksに提出するものとします。お客様は、当該監査報告書を、プライバシー法上の基準を満たす目的又はDPAの要件を満たすことを確認する目的で使用することができるものとします。当該監査報告書は両当事者間の機密情報に該当するものとします。
Customer shall provide to Secureworks a copy of any audit reports generated in connection with an audit carried out under this clause 4.9, unless prohibited by applicable law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of applicable Privacy Laws. The audit reports shall be Confidential Information of the parties.

お客様は、SCC、モジュール2、第8.9(c)条並びに第8.9(d)条において、DPA第4.9条の規定がお客様による監査の要求に組み込まれることに同意するものとします。
For the purpose of the SCCs, Module Two, Clauses 8.9(c) and 8.9(d), Customer agrees that the provisions of clause 4.9 of the DPA shall be incorporated into any audit request made by the Customer.

5. 国際的な移転
International transfers

5.1 Secureworksは、本サービスの提供に関連し、又は通常の業務の一環において、第5条に基づき、個人データ及びセキュリティイベント・データを自己の関連会社及び復処理者に移転する可能性があります。Secureworksは、プライバシー保護と個人データの国際流通についてのOECDガイドラインを考慮するものとします。
Secureworks may, in connection with the provision of the Services, or in the normal course of business, make international transfers of the Personal Data and Security Event Data to its Affiliates and/or Subprocessors subject to the terms of this clause 5. Secureworks takes into consideration the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

5.2 本サービスの提供及びSecureworksによるセキュリティイベント・データの処理が、(a)欧州経済領域、イギリス及びスイスから、(b)第三国(以下に定義)に所在するSecureworks(又はSecureworksの関連会社及び復処理者)へのパーソナルデータの移転を伴う場合、両当事者は、別紙3において参照されるSCCが当該移転に適用されることに同意するものとします(イギリス又はスイスからの移転については、必要に応じて、別紙3の国別条項によって修正されます)。本条における「**第三国**」とは、GDPR第45条（又はイギリス若しくはスイスのプライバシー法における同様の規定）に基づく十分性認定の対象となっておらず、かつプライバシー法によりパーソナルデータの移転が制限又は禁止される国を意味します。SCC、DPA、プライバシー法の間で矛盾が生じた場合は、(1)プライバシー法、(2)SCC、(3)DPAの順に優先されます。
Where the provision of the Services and/or Secureworks' processing of Security Event Data involve a transfer of personal data from (a) the European Economic Area, the United Kingdom and/or Switzerland to (b) Secureworks or any of Secureworks' Affiliates and/or Subprocessors located in a Third Country (as defined below), the parties agree that the SCCs as referenced in Schedule 3 shall apply to such transfer (as amended (where applicable) by the country specific provisions also referenced in Schedule 3 for transfers from the UK and/or Switzerland). "**Third Country**" in this clause means a country that is not subject to an adequacy decision pursuant to Article 45 of the GDPR (or a similar provision in the Privacy Laws of the United Kingdom and/or Switzerland) and to which a transfer of personal data would be restricted or prohibited by Privacy Laws. In the event of a conflict between the SCCs, this DPA or Privacy Law, the order of priority will be (1) Privacy Law, (2) the SCCs and (3) this DPA.

5.3 SCCがパーソナルデータの移転に対する有効な法的根拠とならなくなった場合、両当事者は、適用されるプライバシー法に従って当該移転を確実に継続できるよう、代替となる移転方法の利用ついて誠意をもって合意するために、遅延なく協議するものとし、合意された代替手段を合理的に実行可能な限り速やかに実施するものとします。 これには、利用可能かつ適切な場合に、両当事者が代替的なデータ移転手段の締結に合意することも含まれます。第5.3条に従って代替の移転手段に合意できなかった場合、唯一かつ排他的な救済措置は、該当する本サービスの終了とします。このような状況において、お客様は、当該終了前の期間に発生した、関連する取引文書に記載された未払いのサービス料金を、第三者製品（CRAの定義に従う）に関連する料金とともに、Secureworksに支払う義務を負うものとします。
If the SCCs cease to provide a valid legal basis for the transfer of personal data, the parties shall without undue delay meet to agree in good faith what alternative transfer methods are available to ensure such transfers can continue in accordance with applicable Privacy Law and implement an agreed alternative method as soon as reasonably practicable. This may include the parties agreeing to enter into an alternative data transfer method where available and appropriate. The sole and exclusive remedy for failure to agree an alternative transfer method in accordance with this clause 5.3 shall be the termination of the affected Services. In such circumstances Customer shall remain liable to pay to Secureworks all unpaid Services fees as set forth in the relevant Transaction Document accrued as of, and attributable to the period prior to, such termination together with any applicable fees associated with Third Party Products (as defined in the CRA).

5.4 両当事者は、SCCが特定の条項に関して最大限の努力を払うことを求めている場合、関連する当事者が、自らの利益のためにその結果を達成することを求めているかのように、誠実に、勤勉に、断固として、熟慮して、かつ合理的な方法で行動する義務を意味すると解釈することに同意します。
The parties agree that where the SCCs require the use of best efforts in respect to a specific provision this will be interpreted to mean an obligation on the relevant party to act in good faith, in a diligent, determined, prudent and reasonable manner, as if that party were seeking to achieve the result of that provision for its own benefit.

6. **データ侵害** Secureworksは、DPAに基づく自らの債務不履行に起因してデータ侵害が発生した場合、次の対応を取るものとします。
Data Breaches: Where a Data Breach is caused by Secureworks' failure to comply with its obligations under this DPA, Secureworks shall:

6.1 Secureworksは、データ侵害の発生を確認した場合、遅滞なくお客様に通知し、Secureworksが把握している範囲でデータ侵害の概要、連絡先、当該データ侵害への実施済みの対策及び今後の対策に関する情報を提供するものとします。
notify Customer without undue delay after establishing the occurrence of the Data Breach and shall, to the extent such information is known or available to Secureworks at the time, provide Customer with details of the Data Breach, a point of contact and the measures taken or to be taken to address the Data Breach; and

6.2 Secureworksは、データ侵害に関する調査及び復旧に関して、お客様に合理的な協力を提供します。（プライバシー法に基づく規制当局及び影響を受けた個人に対する通知を含みますが、これらに限定されません。）
reasonably cooperate and assist Customer with any investigation into, and/or remediation of, the Data Breach (including, without limitation and where required by Privacy Laws, the provision of notices to regulators and affected individuals).

お客様が、監督当局、その他の規制当局又は司法機関に対してデータ侵害に関する通知を行うことを意図する場合、（適用される法律により禁止されている場合を除き）Secureworksに対して当該通知内容を確認する機会を与えるものとし、Secureworksが提示した合理的な意見及び修正を反映させるものとします。
In the event Customer intends to issue a notification regarding the Data Breach to a supervisory authority, other regulator, or law enforcement agency, Customer shall (unless prohibited by applicable law) allow Secureworks to review the notification and Customer shall have due regard to any reasonable comments and/or amendments proposed by Secureworks.

7. **セキュリティイベント・データ** Secureworksは、本サービスの提供に関連してセキュリティイベント・データを処理するものとします。お客様は、顧客に提供されるセキュリティサービス、製品、サービスの開発、機能向上、改良目的でセキュリティイベント・データが処理されることに同意します。Secureworksは、セキュリティイベント・データに含まれるパーソナルデータについてはデータ管理者に該当し、Secureworksは、適用されるプライバシー法を遵守する責任を負います。DPAに定める個人データの開示及び移転に関する制約は、本条に定める利用目的に沿ったセキュリティイベント・データの処理には適用されないものとします。ただし、DPA又はCRAで許諾されている場合、又は当該開示が適用される法律又は司法手続において要求されない限り、お客様を追跡し得るセキュリティイベント・データを、（関連会社及び復処理者を除く）第三者に開示しないものとします。Secureworksは、本サービスの終了時に（いかなる理由においても）セキュリティイベント・データを返却又は消去するようお客様から要求されないものとします。お客様が、（管轄権を有する裁判所又は規制当局等による）法的に拘束力を有する命令に基づき、セキュリティイベント・データを消去せざるを得ない場合、Secureworksは法律上の要求に従い、拘束力のある命令の対象であるセキュリティイベント・データを、当該拘束力のある命令の謄本の写しの受領後、実務上可能な限り速やかに消去することに同意します。
Security Event Data: Secureworks will process Security Event Data as part of its provision of Services. Customer acknowledges that Security Event Data may also be processed in order to develop, enhance and/or improve security services

and the products and services offered and provided to customers. Secureworks shall be the controller in respect of any personal data in the Security Event Data and, as such, is responsible for processing the Security Event Data in accordance with applicable Privacy Laws. Restrictions on the disclosure and transfer of Personal Data in this DPA shall not apply to Security Event Data processed for the purposes described in this clause PROVIDED THAT Secureworks shall not disclose any Security Event Data that is traceable to Customer to any third parties (other than Affiliates and Subprocessors) unless permitted under this DPA and/or the CRA, or the disclosure is required in order to comply with applicable law or legal process. Secureworks shall not be required by Customer to return or delete Security Event Data upon termination of the Services (for any reason). If Customer is compelled by a legally binding order (e.g. of a court or regulatory authority of competent jurisdiction) to have the Security Event Data deleted, then Secureworks agrees, as legally required, to delete the Security Event Data that is the subject of the binding order as soon as practicable following receipt of a certified copy of such binding order.

8. **プライバシー影響評価** お客様が、本サービスにおけるSecureworksが行う個人データの処理の範囲で、監督当局への事前相談を含む、SecureWorksが行う個人データの処理に関連するデータ保護影響評価を実施する場合、Secureworksは、合理的な範囲でこれに協力するものとします。ただし、Secureworksは、当該協力に掛かる合理的な費用を請求する権利を留保するものとします。

Privacy Impact Assessments: Secureworks shall provide reasonable cooperation and assistance to Customer, to the extent applicable in relation to Secureworks' processing of the Personal Data and within the scope of the agreed Services, in connection with any data protection impact assessment(s) which the Customer may carry out in relation to the processing of Personal Data to be undertaken by Secureworks, including any required prior consultation(s) with supervisory authorities. Secureworks reserves the right to charge Customer a reasonable fee for the provision of such cooperation and assistance.

9. **CCPAに関する特則** 本条は、本サービスの提供においてカリフォルニア州の居住者の個人データが処理されるときに限り適用されます。Secureworksは、本サービスを提供する、又は、DPA及びCRAにおいて明確に規定された目的を含む事業目的以外の目的のために、消費者の個人データを保持し、使用し又は開示することを含む、商業目的のために個人データを保持し、使用し又は開示することが禁止されていることを認識し、同意します。また、Secureworksは、本サービスを提供する、又は、DPA及びCRAにおいて明確に規定された目的を含む事業目的に必要な場合を除き、消費者の個人データをさらに収集し、販売し又は使用しないものとします。Secureworksは、消費者の個人データの取扱いに関する本条及びその他のDPAの規定の制約を理解し、自らに課される義務を遵守することを保証します。両当事者は、お客様がSecureworksに提供する消費者の個人データが、金銭又はその他の価値のある対価のために提供されるものではないことを明確に確認し、同意します。

CCPA-Specific Requirements: To the extent that Personal Data of California residents is processed in the provision of the Services, this clause 9 shall apply. Secureworks understands and agrees that it is expressly prohibited from retaining, using, or disclosing Personal Data of consumers for any purpose, including retaining, using, or disclosing such Personal Data of consumers for a commercial purpose, other than for a business purpose, including providing the Services or as expressly permitted in this DPA or the CRA. In addition, Secureworks will not further collect, sell, or use Personal Data of consumers except as necessary to perform a business purpose, including to provide the Services or as expressly permitted in this DPA or the CRA. Secureworks certifies that it understands the restrictions contained in this clause and otherwise in this DPA with respect to handling of Personal Data of consumers and shall comply with all such obligations. The parties expressly acknowledge and agree that Customer is not providing any Personal Data of consumers to Secureworks for monetary or any other valuable consideration.

10. **一般条項** DPA又はその他の規定にかかわらず、両当事者は、DPAおよびSCCに基づいてSecureworksがお客様のために処理した個人データに関するSecureworksの責任は、CRAに規定された上限及び範囲に限定、DPAのいかなる規定も、CRAに規定される損害、費用その他の支払を行う責任、義務を拡大するものではないことに同意します。

General: Notwithstanding anything in this DPA or otherwise to the contrary, the parties agree that Secureworks' liability with respect to the Personal Data processed by Secureworks on behalf of Customer under this DPA and under the SCCs shall be limited to the amounts and types of liability as set forth in the CRA and nothing in this DPA shall expand any responsibility, liability or obligation to pay damages, costs, expenses or otherwise beyond that set forth in the CRA.

データ保護特約　別紙1:　処理の内容
SCHEDULE 1 TO DATA PROTECTION ADDENDUM
Processing description

1	**処理の目的　Subject matter and purpose**
	Secureworksは、CRAの条件に基づいて情報セキュリティサービスをお客様に提供し、取引文書、サービスレベルアグリーメント、サービス記述書その他に規定された本サービスを提供するために個人データの処理を行います。 Subject to the terms of the CRA, Secureworks provides information security services for Customer and processes the Personal Data for the purpose of providing such services as set out in the applicable Transaction Document, service level agreements, Service descriptions or otherwise.
2	**処理の期間　Duration of processing**
	Secureworksは、CRAの有効期間中、個人データを取得して処理するものとし、DPAに従って個人データを返還又は消去するものとします。 Secureworks will retain and process the Personal Data for the term of the CRA and in accordance with the provisions of this DPA regarding the return or deletion of the Personal Data.
3	**データ主体　Categories of data subjects**
	次の区分に属する個人が、個人データの処理及び移転に係るデータ主体となります。過去、現在、将来の、(i)従業員及びパートナー、(ii)Secureworksが提供する本サービスの対象となるお客様の情報システムを利用し、アクセスするお客様及び個人、(iii)アドバイザー、コンサルタント、契約社員、業務委託先及び代理人、(iv)不服申立者、取引先、照会者、(v)（確定した又は疑いのある）脅威アクター The Personal Data processed and transferred may concern the following categories of data subjects: past, present and prospective (i) employees and partners, (ii) clients and individuals who use and access Customer information technology systems for which Secureworks provides Services, (iii) advisors, consultants, contractors, subcontractors and agents; (iv) complainants, correspondents and enquirers and (v) threat actors (suspected or confirmed).
4	**パーソナルデータの種類　Categories of personal data**
	4.1 **Secureworksがデータ処理者の場合：**処理又は移転される個人データの種類は、以下の内容を含みますが、これらに限定されないものとします。 **When Secureworks is acting as a processor:** the type of Personal Data that may be processed and/or transferred includes (without limitation): (a) **クラウドサービス及びMSSサービス　For both Cloud and MSS Services**: (i) セキュリティログ又はアラートの処理に含まれるネットワークデータ（IPアドレス、プロセス名、プロセス・オーナーID、ユーザID、MACアドレスなどの固有のデバイス識別子、ネットワークトラフィックフロー、通信メタデータ、マシン名など）。 Network data (such as IP address, process name, process owner ID, user ID, MAC address or other unique device identifiers, network traffic flows, communications metadata, machine names) within process security logs or alerts; (ii) エンドポイント・エージェントのアクティビティに関する、ユーザ認証データ（ユーザID、IPアドレス、MACアドレス）及びプロセス・アクティビティ（ユーザID、IPアドレス、MACアドレス）User authentication data (user ID, IP address, MAC address) and process activity (user ID, IP address, MAC address) in connection with endpoint agent activity; (iii) セキュリティログ又はアラートの処理における、悪意のあるファイル、ネットワーク・フラグメントに含まれる個人データ。Any Personal Data within malicious file fragments, network fragments within process security logs or alerts; (iv) サービスの提供に関して、顧客サポートを要請する際にお客様が含めることを選択した個人データ。Any Personal Data which the Customer elects to include in the course of requesting customer support in the course of the provision of Services. (b) **コンサルティングサービス　For SRC (Consulting) Services:** (i) 連絡先情報（氏名、住所、電子メールアドレス、電話番号、FAX番号、現地タイムゾーンに関する情報）contact details (which may include name, address, e-mail address, phone and fax

contact details and associated local time zone information);

(ii) 雇用情報（会社名、職制、職位、人口統計データ及びロケーションデータ）employment details (which may include company name, job title, grade, demographic and location data);

(iii) ITシステム情報 （例：ユーザID、パスワード、コンピュータ名、ドメイン名、IPアドレス、cookieなどのソフトウェア使用パターンの追跡情報）IT systems information (which may include user ID and password, computer name, domain name, IP address and software usage pattern tracking information (i.e. cookies));

(iv) 情報技術に関する相談、サポート及びサービスを提供する過程で、偶発的にアクセスする可能性がある、データ主体の電子メールの内容及び送信データ。（偶発的なアクセスには、電子メールの送信、ルーティング、受信に関する電子メールによるコミュニケーション及びデータを含むものとします。）data subjects' e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails);

(v) データ主体に対して、又はデータ主体のために提供される製品及びサービスの内容。details of goods or services provided to or for the benefit of data subjects;

(vi) 財務情報（例：信用情報、支払条件及び銀行口座情報）financial details (e.g. credit, payment and bank details);

(vii) 偶発的に個人データの処理を行うことにより、明らかにされる可能性がある特別カテゴリーのデータ；人種的もしくは民族的素性、政治的思想、宗教的もしくは哲学的信条、又は労働組合の加入状況、健康関連データ（身体的又は精神的な健康又は状態を含む）、性生活又は性的指向、犯罪歴及び犯罪捜査歴もしくは関連する裁判手続、ソーシャルセキュリティーに関するファイルなど(該当する場合） special categories of data (if appropriate) which may involve the incidental processing of Personal Data which may reveal: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health (including physical or mental health or condition); sexual life or sexual orientation; criminal offences or alleged offences and any related court proceedings; social security files.

4.2 **Secureworksがデータ管理者の場合：**処理又は移転されるパーソナルデータの種類は、以下の内容を含みますが、これらに限定されないものとします。

When Secureworks is acting as a controller: the type of personal data that may be processed and transferred may include (without limitation):

(i) 前4.1(a)(i)-(iv)条に記載した情報と同じ情報 the same information as set out in the preceding section 4.1(a)(i)-(iv);

(ii) 本サービスの提供中にセキュリティイベント・データに関連して収集する情報 any other information related to Security Event Data which is collected during Secureworks' provision of Services, and

(iii) 本サービスを支える基盤を使用する際に提供される可能性がある、お客様（又はその社員）のパーソナルデータで、以下の内容を含み、これらに限定されないものとします。(i)分析活動に関連するユーザID（閲覧履歴）、(ii)アカウント管理に関連するユーザ認証情報（氏名、職制、会社名、電子メールアドレス、電話番号、事業所の住所、ユーザ名、ユーザID）any personal data that Customer (or its personnel) may submit through the use of the platform(s) supporting the Services, which may include (without limitation): (i) user ID in connection with analytics activities (browsing history) and/or (ii) user authentication data (first/last name, title/position, company, email, phone, physical business address, username, user ID) in connection with administering accounts.

5 センシティブデータ Sensitive data

5.1 **Secureworksがデータ処理者としてコンサルティングサービスを提供する場合：**本サービスの提供に際して、4.1(b)(vii)に記載された特別な種類のパーソナルデータの偶発的な処理を行う可能性があります。

When Secureworks is providing SRC (Consulting) Services and acting as a processor: the provision of Services may involve the incidental processing of special categories of personal data as described in section 4.1(b)(vii) above.

5.2 **Secureworksがデータ管理者の場合：**特別な種類のパーソナルデータは、能動的又は意図的に収集されません。

When Secureworks is acting as a controller: special categories of personal data are not actively or intentionally collected.

	いずれの場合も、収集された特別な種類のパーソナルデータの保護は、別紙２（セキュリティ対策）に規定された、安全管理措置及び制限に基づくものとします。In each case, safeguards and restrictions to protect any special categories of personal data that may be collected are as set out in Schedule 2 (Security Measures).	
6	**処理の態様　Nature of the processing**	
	パーソナルデータは、以下の処理の対象になります：自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又はそれら以外に利用可能なものにすること、整列又は統合、制限、消去若しくは破壊のような、パーソナルデータ又は一群のパーソナルデータに対して行われるあらゆる操作または一連の操作。 Personal data will be subject to the following processing activities: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	
7	**保持期間　Retention period**	
	保持期間は、Secureworksの保管ポリシーに記載されるものとします。特定の本サービスに適用される保管ポリシーは、お客様の書面による請求に基づいて提供されます。Retention periods are as set out in Secureworks' retention policy. The retention policy for specific Services is available upon written request from Customer.	
8	**連絡先　Contact details**	
	8.1　**お客様**の連絡先及びデータ保護責任者 **Customer** contact details and Data Protection Officer:	CRAの記載、又はCRAに基づく通知に従う。 As set out in (or otherwise notified under) the CRA
	8.2　**Secureworks**の連絡先及びデータ保護責任者 **Secureworks** contact details and Data Protection Officer:	電子メール　Contact email: legal@secureworks.com データ保護責任者　DPO: privacy@secureworks.com

Published date: March 25, 2024

データ保護特約　別紙2:　セキュリティ対策
SCHEDULE 2 TO DATA PROTECTION ADDENDUM
Security Measures

この情報セキュリティに関する概要は、お客様データを保護するためのSecureworksの企業管理に適用されます。This information security overview applies to Secureworks' corporate controls for safeguarding Customer's Personal Data.

セキュリティに関する運用基準　Security Practices

Secureworksは、企業環境を保護するために情報セキュリティ運用基準を施行し、(1)情報セキュリティ、(2)システム及び資産管理、(3)開発、(4)ガバナンスについて定めています。当該運用基準はSecureWorks の経営管理部門によって承認され、毎年見直しが行われています。
Secureworks has implemented corporate information security practices and standards that are designed to safeguard Secureworks' corporate environment and to address: (1) information security; (2) system and asset management; (3) development; and (4) governance. These practices and standards are approved by Secureworks' executive management and undergo a formal review on an annual basis.

組織的安全管理措置　Organizational Security

セキュリティに関する運用基準に従うことは、各社員の義務です。運用基準を遵守するために、情報セキュリティ部門は次の役割を担います。
It is the responsibility of the individuals across the organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, the function of information security provides:

1. 戦略、ポリシー/基準ならびに規制の遵守、意識向上ならびに教育、リスク・アセスメント、セキュリティ要求管理、アプリケーションならびにインフラストラクチャー・コンサルティング、確認テストの実施及び自社のセキュリティ指針の運用
   Strategy and compliance with policies/standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and drives the security direction of the company;
2. 当該環境におけるセキュリティ管理を施行するためのセキュリティテスト、設計及びセキュリティソリューションの実施
   Security testing, design and implementation of security solutions to enable security controls adoption across the environment;
3. 施行されたセキュリティソリューション、環境、資産に関するセキュリティの運用と、インシデント対応の管理
   Security operations of implemented security solutions, the environment and assets, and manage incident response;
4. （eDiscovery及びeForensicsを含む）調査のためのセキュリティ運用、法律、データ保護及び人事に関するフォレンジック調査
   Forensic investigations with security operations, legal, data protection and human resources for investigations including eDiscovery and eForensics.

資産の分類及び管理　Asset Classification and Control

Secureworksでは物理的及び論理的な資産を記録し管理しています。SecureworksのIT部門は、次のような資産を記録しています。
Secureworks' practice is to track and manage physical and logical assets. Examples of the assets that Secureworks IT might track include:

- 情報資産：特定のデータベース、災害復旧計画、事業継続計画、データ分類基準、アーカイブされた情報など。
  Information Assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information;
- ソフトウェア資産：特定のアプリケーション、システムソフトウェアなど。
  Software Assets, such as identified applications and system software;
- 物理的資産：特定のサーバ、デスクトップ型/ノート型パソコン、バックアップ用/保管用テープ、プリンタ、通信機器など。
  Physical Assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

これらの資産は、事業への重要性に基づいて機密性の高さが分類されています。パーソナルデータの取り扱いに関する業界ガイドラインに基づいて、技術的、組織的、物理的な管理措置の枠組みが定められています。その中で、アクセス管理、暗号化、ロギング及び監視、データ消去の制御が含まれる場合があります。
The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These may include controls such as access management, encryption, logging and monitoring, and data destruction.

人的セキュリティ　Personnel Security

採用プロセスにおいて、各地域の法令に基づいてスクリーニング審査が行われます。Secureworksでは、毎年従業員向けの必修コンプライアンス・トレーニングが実施され、従業員は情報セキュリティとデータ・プライバシーに関するオンライン・コースを受

講し、合格することが義務付けられています。職種に応じて、セキュリティ啓発プログラムに基づいてその他の資料が提供されます。
As part of the employment process and subject to local law, employees undergo a screening process at hire and periodically thereafter. Secureworks' annual compliance training includes a requirement for employees to complete an online course and pass an assessment covering information security and data privacy. The security awareness program may also provide materials specific to certain job functions.

物理的・環境的セキュリティ　Physical and Environmental Security

Secureworksは、物理的なセキュリティのリスクを低減するため、様々な技術的・運用上の手段を講じています。Secureworksのセキュリティチームは、各拠点の担当者と適切な対策を導入し、物理的な施設、事業内容、既知の脅威に関する変更点について継続的に確認します。また、セキュリティチームは、業界のベストプラクティスの情報を得て、全体として、独自の事業慣行とSecureWorksの期待値の両方を満たす手法を選択します。Secureworksは、アーキテクチャ、運用、システムを含む、管理の要素を考慮したうえで、セキュリティに対する取り組みを検討するものとします。
Secureworks uses a number of technological and operational approaches in its physical security program in regards to risk mitigation. Secureworks' security team works closely with each site to determine appropriate measures are in place and continually monitor any changes to the physical infrastructure, business, and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniquenesses in business practice and expectations of Secureworks as a whole. Secureworks balances its approach towards security by considering elements of control that include architecture, operations, and systems.

コミュニケーション及び運用管理　Communications and Operations Management

IT部門は、集中的な変更管理プログラムによって、企業インフラ、システム、アプリケーションに対する変更を管理します。テスト、ビジネス影響評価、必要に応じて経営層の承認などが含まれます。セキュリティ及びデータ保護に係るインシデントに対する、インシデント対応計画が策定されており、インシデント分析、封じ込め、対応、殲滅、報告、通常業務への復旧について定められています。
The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program which may include testing, business impact analysis and management approval where appropriate. Incident response procedures exist for security and data protection incidents which may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

悪意のある資産の使用及び悪意のあるソフトウェアから防御するために、リスクに応じた追加の対策が講じられており、情報セキュリティ運用基準の制定、アクセス権の制御、開発及びテスト環境の整備、サーバ、デスクトップ型/ノート型パソコンにおけるウィルス検知、電子メール及び添付ファイルのスキャン、システムコンプライアンスのスキャン、侵入防止の監視及び対応、主要なイベントのロギング及び通知、データの種類に応じた情報取扱手順、eコマースのセキュリティ及びネットワークセキュリティ、システム/アプリケーションの脆弱性スキャンなどが含まれます。
To protect against malicious use of assets and malicious software, additional controls may be implemented based on risk. Such controls may include, but are not limited to, information security policies and standards, restricted access, designated development and test environments, virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans, intrusion prevention monitoring and response, logging and alerting on key events, information handling procedures based on data type, e-commerce application and network security, and system and application vulnerability scanning.

アクセス管理　Access Controls

承認を取得する適切な手続きによって、企業システムへのアクセス権は制限されています。故意その他の理由を問わず、不正使用のリスクを低減するため、アクセス権は職務の分離と最小権限の原則に基づいて付与されます。リモートアクセス及び無線接続は制限されており、ユーザ及びシステム上のセキュリティの設定が必要となっています。主要なデバイスとシステムの特定のイベントログは集中的に収集され、インシデント対応及びフォレンジック調査を可能にするために例外事項が報告されています。
Access to corporate systems is restricted, based on procedures to ensure appropriate approvals. To reduce the risk of misuse, intentional or otherwise, access is provided based on least privileges. Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place. Specific event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

システム開発及びメンテナンス　System Development and Maintenance

Secureworksは、公表された第三者の脆弱性について、自社の環境での適用性を検討します。Secureworksの事業及びお客様へのリスクを踏まえ、対処に向けた時間軸をあらかじめ設定しています。また、リスクに応じて、新規の主要なアプリケーションに対し、脆弱性スキャン及び診断を実施しています。リスクに応じて、コードの脆弱性を事前に把握するために、実装前に開発環境でコードレビュー及びスキャンを行っています。これらの手続によって積極的に脆弱性を特定し、コンプライアンスを推進しています。
Publicly released third party vulnerabilities are reviewed for applicability in the Secureworks environment. Based on risk to Secureworks' business and customers, there are pre-determined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable

proactive identification of vulnerabilities as well as compliance.

コンプライアンス　Compliance

情報セキュリティ部門、法務部門、プライバシー及びコンプライアンス部門は、Secureworksに適用され得る適用法令の把握に協力しています。自社及びお客様の知的財産権、ソフトウェアの使用権、従業員及びお客様のパーソナルデータの保護、データ保護及びデータ取扱手続、越境データ移転、財務及び運用手続、技術に関する輸出規制、フォレンジック対応などの項目が含まれますが、これらに限定されません。情報セキュリティプログラム、プライバシー委員会、内部/外部監査及びアセスメント、 社内/社外弁護士による相談、内部管理アセスメント、社内ペネトレーションテスト及び脆弱性診断、契約管理、セキュリティ啓発、セキュリティ・コンサルティング、ポリシーの例外審査、リスク管理などを兼ね備えることによってコンプライアンスを推進しています。
The information security, legal, privacy and compliance departments work to identify regional laws and regulations applicable to Secureworks. These requirements cover areas such as, intellectual property of the company and our customers, software licenses, protection of employee and customer personal data, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements. Mechanisms such as the information security program, the executive risk committee, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

データ保護特約　別紙3:　標準契約条項

契約（モジュール１：データ管理者からデータ管理者、モジュール２：データ管理者からデータ処理者）

SCHEDULE 3 TO DATA PROTECTION ADDENDUM

Standard Contractual Clauses
(Module One: controller to controller and Module Two: controller to processor)

In the event of a transfer from the European Economic Area ("**EEA**"), the UK and/or Switzerland to a Third Country (as defined in clause 5.2) in accordance with the DPA, such transfer shall be subject to the terms of this Schedule 3 and the Standard Contractual Clauses set out below shall apply and shall be incorporated by reference into, and form part of, this DPA.

1. **Transfers from the EEA**

1.1 In relation to transfers of personal data that are subject to the Privacy Laws of a country within the EEA: Module One and Module Two of the SCCs shall apply as set out below.

For SCCs Module One (controller to controller) AND Module Two (controller to processor):	
Clause 7 (Docking clause)	The optional docking clause shall apply.
Clause 11(a) (Redress)	The optional wording in Clause 11(a) shall **not** apply.
Clause 13 (Supervision) and Annex I.C	All the options in Clause 13(a) are retained and shall apply depending on the establishment of the data exporter (as identified by the data exporter's address set out in, or otherwise notified under, the CRA).
Clause 17 (Governing law)	The SCCs shall be governed by the law of the country in which the data exporter is established provided such law allows for third-party beneficiary rights. Where such law does not allow for third-party beneficiary rights, the SCCs shall be governed by Irish law.
Clause 18(b) (Choice of forum and jurisdiction)	The court of the country in which the data exporter is established.
For SCCs Module Two (controller to processor) ONLY:	
Clause 9(a) (Use of sub-processors)	**Option 2: General written authorisation** is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least fourteen (14) days in advance.

1.2 The Appendix to the SCCs is completed as set out below for both Module One (controller to controller) and Module Two (controller to processor):

Annex I.A (List of parties)	
Data exporter name and address:	The data exporter is: (i) the Customer and/or Customer Affiliate that has entered into the Transaction Document and/or (ii) the relevant Customer Affiliate (if any) that is receiving Services (under the CRA) and is based in the EEA, the UK, and/or Switzerland ("**Relevant Affiliates**"). The data exporter's address is the Customer's address or the Customer Affiliate's address as set out in the Transaction Document.
Data importer name and address:	The data importer is Secureworks Inc. and its address is One Concourse Parkway, Atlanta, GA 30328, US.
Activities relevant to the data transferred:	Activities relate to the provision by data importer to data exporter of information security services (as set out in the applicable Transaction Document, service level agreement, Services description or otherwise).
Role of data exporter:	The data exporter is a **controller**.
Role of data importer:	The data importer is: (i) a **processor** in respect of personal data (as defined in the DPA) and (ii) a **controller** in respect of any personal data contained in Security Event Data.

Signature by data exporter:	The SCCs shall be deemed to have been signed: (i) if the Customer and/or Customer Affiliate has signed an offline CRA, on the same date as such CRA is executed; or (ii) if the Customer and/or Customer Affiliate is trading under the online CRA, on the date of execution of the relevant Transaction Document. Where applicable, Customer enters into these Clauses for and on behalf of itself and each Relevant Affiliate and hereby confirms that it has the necessary authority to do so.
Signature by data importer:	*Patricia Ford*
The remainder of this Annex I.A shall be deemed completed with the information set out in Schedule 1 of the DPA (and, where applicable, any other information set out in the DPA and/or CRA).	
Annex I.B	
B1 Categories of data subjects whose personal data is transferred: shall be completed with the information set out in Schedule 1, section 3. **B2** Categories of personal data transferred: shall be completed with the information set out in Schedule 1, section 4. **B3** Sensitive data transferred: shall be completed with the information set out in Schedule 1, section 5. **B4** Frequency of the transfer: The transfer is made on a continuous basis for MSS and Cloud Services. For SRC (Consulting) Services the frequency of the transfer is determined by the relevant Transaction Document. **B5** Nature of the processing: shall be completed with the information set out in Schedule 1, section 6. **B6** Purpose of the data transfer and further processing: (i) for **Module Two** (controller to processor) SCCs: the purpose of the data transfers and processing is to enable data importer to provide the data exporter with information security services (as set out in the applicable Transaction Document, service level agreement, Service descriptions or otherwise); (ii) for **Module One** (controller to controller) SCCs: data importer will transfer and further process the personal data (including Security Event Data) described in B2 for the purpose of: (a) developing, enhancing and/or improving its security services and the products and services it offers and provides to customers, (b) administration and management of data importer's products, services and customer accounts, (c) research and analytics, and (d) provision of customer support. **B7** Period of time for which personal data will be retained: shall be completed with the information set out in Schedule 1, section 7. **B8** For transfers to subprocessors: The subject matter, nature and duration of processing by subprocessors acting on behalf of data importer will be the same as for data importer.	
Annex I.C	
The competent supervisory authority/ies will be those located in the country in which the data exporter is located (as identified by the data exporter's address set out in, or otherwise notified under, the CRA).	
Annex II (Security measures)	
The description of the technical and organisational measures implemented by the data importer(s) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons are as set out in Schedule 2 (Security Measures) of the DPA.	

2. **Transfers from the UK**

2.1 For transfers of personal data that are subject to UK Privacy Laws: the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses for UK transfers of Personal Data dated 21 March 2022 ("**Addendum**") issued by the UK Information Commissioner shall apply and shall be incorporated by reference into, and form part of, this DPA, and will come into effect, where applicable, upon signature by the parties of the DPA. Capitalised terms used in this section 2 that are not defined in the DPA shall have the meaning set out in the Addendum.

2.2 The Tables in the Addendum shall be completed as follows:

Table 1: Parties		
Start date	This Addendum will start: (i) if the Customer has signed an offline CRA, on the same date as such CRA is executed; or (ii) if the Customer is trading under the online CRA, on the date of execution of the relevant Transaction Document	
The Parties	**Exporter (who sends the Restricted Transfer):**	**Importer (who receives the Restricted Transfer):**
	The data exporter (as defined in Schedule 3, section 1.2)	Secureworks Inc. (as specified in Schedule 3, section 1.2)
Parties' details and key contacts	As set out in Schedule 3, section 1.2 or otherwise notified between the parties	
Signature	The Addendum shall be deemed to have been signed by the parties as set out in Schedule 3, section 1.2.	
Table 2: Selected SCCs, Modules and Selected Clauses		
Addendum EU SCCs:	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:	
Module One:	– Clause 7 (Docking clause): the docking clause shall apply – Clause 11 (Redress): the optional wording in Clause 11(a) shall **not** apply	
Module Two:	– Clause 7 (Docking clause): the docking clause shall apply – Clause 11 (Redress): the optional wording in Clause 11(a) shall **not** apply – Clause 9(a) (Sub-processors): **Option 2: General written authorisation** is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least fourteen (14) days in advance	
Table 3: Appendix Information		
"**Appendix Information**" means the information which must be provided for the selected Modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out as follows:		
Annex I.A: List of Parties:	See Schedule 3, section 1.2	
Annex I.B: Description of Transfer:	See Schedule 3, section 1.2	
Annex II: Technical and organisational measures	See Schedule 2	
Annex III: List of Sub processors:	See Clause 4.6 of the DPA	
Table 4: Ending this Addendum when the Approved Addendum changes		
Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum (as set out in Section 19 of the Addendum): ☑ Importer ☑ Exporter ☐ neither Party	

3. **Transfers from Switzerland**

3.1 **Definitions** – in this section 3, the following definitions are used:
(a) "**FDPIC**" means the Federal Data Protection and Information Commissioner; and
(b) "**Swiss Data Protection Laws**" means any law, enactment, regulation or order in Switzerland concerning the processing of data relating to living persons, including, as applicable, the Federal Act on Data Protection of 19 June 1992 (SR 235.1) ("**FADP**") and the revised version of the FADP dated 25 September 2020 ("**Revised FADP**").

3.2 **SCCs** – For transfers from Switzerland to a Third Country of personal data that are subject to Swiss Data Protection Laws, the parties agree to:
(a) adopt the GDPR standard for all such data transfers;

(b) use Module One (controller to controller) and Module Two (controller to processor) of the SCCs; and
(c) amend the SCCs in order to comply with Swiss Data Protection Laws as set out below.

3.3 **Amendments to the SCCs** – Where the SCCs apply (in accordance with section 3.2 above) and the transfer from Switzerland to a Third Country is:
(a) exclusively subject to Swiss Data Protection Laws, OR
(b) subject to both Swiss Data Protection Laws and the GDPR
the following amendments shall apply:
(i) references in the SCCs to "Regulation (EU) 2016/679" or "that Regulation" are (in respect of section 3.3(a) above) replaced or (in respect of section 3.3(b) above) supplemented by references to the "FADP and Revised FADP, as appropriate" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced or supplement (as applicable) with the equivalent Article or Section of the FADP or Revised FADP;
(ii) reference to the "EU", "EU Member State", "European Union" and "Union" are (in respect of section 3.3(a) above) replaced or (in respect of section 3.3(b) above) supplemented with references to "Switzerland"; and
(iii) references to competent supervisory authority are (in respect of section 3.3(a) above) replaced or (in respect of section 3.3(b) above) supplemented with references to FDPIC.

3.4 In addition to the above, the following amendments shall also apply to the SCCs:

Swiss amendments that apply to Module One (controller to controller) AND Module Two (controller to processor) SCCs:	
Clause 7 (Docking clause)	The optional docking clause shall apply.
Clause 11(a) (Redress)	The optional wording in Clause 11(a) shall **not** apply.
Clause 13 (Supervision) and Annex I.C	– Where the transfer is exclusively subject to Swiss Data Protection Laws: FDPIC. – Where the transfer is subject to both Swiss Data Protection Laws and GDPR: (i) FDPIC is the supervisory authority insofar as the transfer is governed by Swiss Data Protection Laws; and (ii) the EU authority is the supervisory authority insofar as the data transfer is governed by the GDPR (the criteria of Clause 13(a) for the selection of the competent authority must be observed).
Clause 17 (Governing law)	– Where the transfer is exclusively subject to Swiss Data Protection Laws: Swiss law is the governing law. – Where the transfer is subject to both Swiss Data Protection Laws and GDPR: the law of the country in which the data exporter is established will apply provided such law allows for third-party beneficiary rights. Where such law does not allow for third-party beneficiary rights, the SCCs shall be governed by Irish law.
Clause 18(b) (Choice of forum and jurisdiction)	– Clause 18(b): The courts of the country in which the data exporter is established – Clause 18(c): The term "Member State" in the SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs.
Annex I.A	For a list of the parties see Schedule 3, section 1.2.
Annex I.B	For a description of the transfer see Schedule 3, section 1.2.
Annex II	For the technical and organisational measures see Schedule 2.
Swiss amendments to ONLY Module Two (controller to processor) SCCs:	
Clause 9(a) (Use of sub-processors)	**Option 2: General written authorisation** is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least fourteen (14) days in advance.
Annex III (List of sub-processors)	See Clause 4.6 of the DPA.

3.5 **Supplemental –** The SCCs shall protect the data of legal entities in Switzerland until the entry into force of the Revised FADP (effective 1 January 2023).

3.6 **Incorporation –** The SCCs (Module One and Module Two) adapted for Switzerland in accordance with this section 3 shall

apply and shall be incorporated by reference into, and form part of, this DPA and will come into effect, where applicable, upon signature by the parties in accordance with Schedule 3, section 1.2.

データ保護特約　別紙4:　ドイツ及びスイス刑法の遵守

SCHEDULE 4 TO DATA PROTECTION ADDENDUM
Compliance with GERMAN and SWISS criminal law

1. **Scope**

(i) This Appendix applies to all Services provided in or accessed from Germany and are intended to avoid any possible criminal liability in Germany (German cyber security law, esp. sec. 202a et seq, 203, 206, 303a, 303b German Criminal Act [StGB]).

(ii) This Appendix also applies to all Services provided in or accessed from Switzerland and are intended to avoid any possible criminal liability in Switzerland (Swiss cyber security law, esp. articles 143, 143bis, 144bis, 147, 150, 179 et seq Swiss Criminal Code [StGB]).

Customer acknowledges its acceptance with the German or the Swiss criminal law provisions set out herein if the Services are provided in or accessed from Germany or Switzerland, as the case may be.

2. **Security Services, further security measures and other Services as performed by Secureworks**

2.1 Should a Transaction Document include security scanning, testing, assessment, forensics, or remediation Services ("**Security Services**"), Secureworks may use various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. The Security Services, such as penetration testing or vulnerability assessments, may entail buffer overflows, fat pings, operating system specific exploits and attacks specific to custom coded applications but will exclude intentional and deliberate Denial of Service ("DoS")-Attacks. Secureworks shall perform Security Services during a timeframe mutually agreed upon with Customer.

2.2 The aforementioned Security Services as well as all further security measures to be performed under the CRA, the Transaction Documents as well as other Services to be taken by Secureworks hereunder may result in:

(a) Secureworks obtaining personal and other private data of individuals and/or third parties (e.g. customers of Customer, Customer employees) located on Customer's IT-systems concerned by the performance of Services hereunder, in particular by:
  (i) the circumvention of Customer's security systems which are especially protected against unauthorized access; and/or
  (ii) the interception of data by technical means from a non-public data processing facility (e.g. e-mail communication).
(b) Secureworks directly or, if applicable, as a result of performing the Services, deleting, suppressing, rendering, making unusable or altering data and/or interfering with data processing operations by destroying, damaging, rendering making unusable, removing or altering a data processing system or a data carrier and/or
(c) service interruptions or degradation regarding the Customer's systems.

2.3 Secureworks will treat any data which may be subject to the postal or telecommunications secret and/or further contractual and/or statutory business secret (e.g. data subject to Section 203 German Criminal Code [StGB]) as confidential. Secureworks will only obtain knowledge of the content or the specific circumstances of the data obtained to the extent necessary for the protection of the Customer's IT-systems.

3. **Customer consent with respect to intrusion attempts and Customer's system security checks**

3.1 Customer authorizes Secureworks to perform the Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services) on network resources with the internet protocol addresses ("**IP Addresses**") identified by Customer. Customer represents that, if Customer does not own such network resources, it will have obtained consent and authorization from the applicable third party, in the necessary form and substance satisfactory to Secureworks, to permit Secureworks to provide the Security Services on such third party's network resources.

3.2 In light of the foregoing, upon execution of a Transaction Document for the aforementioned Security Services, Customer consents and authorizes Secureworks to provide any or all the Security Services in the applicable Transaction Document with respect to the Customer's systems. Customer further acknowledges it is the Customer's responsibility to restore network computer systems to a secure configuration after completion of Secureworks's testing. Customer acknowledges and accepts the risks and consequences as laid out above under 2.2.

3.3 The Customer acknowledges and explicitly declares its consent that Secureworks may in this context involve Secureworks' subcontractors and/or other Secureworks Affiliates located around the world (e.g. Secureworks Inc. in the United States, Secureworks Europe SRL in Romania, Secureworks entities located in Asian countries) in order to provide the Services to be performed under the CRA and the Transaction Documents, including the security measures described above. Secureworks undertakes to require any Secureworks subcontractor and/or any other Secureworks Affiliate that Secureworks may involve in order to provide the aforesaid services to treat any data which may be subject to the postal or telecommunications secret and/or further contractual and/or statutory business secret (e.g. data subject to Section 203 German Criminal Code [StGB] or data subject to Article 321 Swiss Criminal Code [StGB]) as confidential.

4. Customer guarantee to provide necessary consents

4.1 Customer hereby guarantees with respect to the provision of Services by Secureworks:

(a) that it has obtained all necessary consents, authorization and required permissions in a valid manner to enable Secureworks to conduct all system security checks and provide to Secureworks respective proof upon Secureworks's request;

(b) that by implementing all necessary technical and organizational measures it will safeguard that Secureworks will only be enabled to conduct or be requested to conduct system security checks on the network resources to the extent as agreed upon by the Parties.

4.2 Customer shall document the obtaining of all necessary consents, authorization and required permissions audit-proof, and shall, upon Secureworks' request and at Secureworks' discretion, provide Secureworks with the documentation in order to enable Secureworks to prove compliance.