Secureworks

データ保護特約

Data Protection Addendum

データ保護特約(Data Protection Addendum、「**DPA**」)は、Secureworks とお客様との間で締結された、マスターサービス契約やカスタマー・リレーションシップ契約などの、お客様が本サービスを発注するための契約(いずれの場合も、以下「**CRA**」)の一部を構成し、Secureworks がお客様に提供するサービスにおいて「プライバシー法」の対象となる「個人データ」の処理を行う場合に適用されます(カッコ内の用語は以下に定義されます。)。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**") forms part of the separately signed agreement executed by the parties that expressly authorizes Customer to order the Services, such as the Master Services Agreement or the Customer Relationship Agreement (in either case, the "CRA") between the Customer and Secureworks and except as expressly stated applies solely where Secureworks processes Personal Data (as defined below) as a processor for the Customer in 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 this 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**」、「**データ処理者**」及び「**監督当局**」という用語は、「プライバシー法」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。

   Definitions: References in this DPA to "**controller**", "**data subject**", "**processor**", "**processing**" (and its derivatives) and "**supervisory authority**" shall have the meanings ascribed to them under Privacy Laws. Capitalized terms not defined in this DPA shall have the meaning set out in the CRA. 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、本サービスの提供に関して Secureworks がお客様のためにデータ処理者として処理した、識別された自然人又は識別可能な自然人に関連する、プライバシー法によって保護されるすべての情報を意味します。

   "**Personal Data**" means any information relating to an identified or identifiable natural person which is processed by Secureworks, acting as a processor on behalf of the Customer, in the provision of the Services.

   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及び EU 一般データ保護規則(General Data Protection Regulation 2016/679、「**GDPR**」)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 Act on the Protection of Personal Information in Japan and the General Data Protection Regulation 2016/679 (the "**GDPR**").

   1.4 「**セキュリティイベント・データ**」とは、セキュリティ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.

   1.5 「**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: a description of the processing activities to be undertaken as part of the CRA and this DPA is set out in Annex 1.

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、(i)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、(ii) 本サービスをお客様に提供する過程で、お客様によって個人データを処理される Secureworks の社員に対し、必要な権限及び同意を提供することを表明し、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 (i) it has obtained and will maintain all necessary authorisations and consents required to enable Secureworks to provide the Services and process the Personal Data pursuant to this DPA and CRA in accordance with the Privacy Laws and (ii) it shall provide all necessary authorisations and consents to Secureworks personnel whose personal data is processed by Customer in the course of providing Services to Customer.

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。Secureworks は、お客様の指示が適用される法律を遵守しているかについて判断する責任を負いませんが、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 the Personal Data 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 and is solely responsible for the consequences of Secureworks complying with them 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** 個人データが（適用される法律に従い）機密情報とされる範囲において、Secureworks は、個人データを CRA の機密保持条項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: To the extent the Personal Data is confidential (pursuant to applicable law), Secureworks shall maintain the confidentiality of the Personal Data in accordance with the Confidentiality clause in the CRA and shall require persons authorised 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 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. The parties agree that the security measures described in Annex 2 (Information 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、(i) 復処理者が行う業務の内容において、(ii) 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。

Subprocessors: Customer agrees that Secureworks may appoint and use Subprocessors (which are identified on the subprocessor list posted on the customer portal or the SaaS 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 (i) relevant to the services to be provided by the Subprocessors and (ii) materially similar to the rights and/or obligations granted or imposed on Secureworks under this DPA.

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。Secureworks は、本条に基づく個人データに掛かる合理的な費用をお客様に請求

する権利を留保するものとします。

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. Secureworks reserves the right to charge Customer for any reasonable costs and expenses incurred by Secureworks in deleting the Personal Data pursuant to this clause.

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 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 confidentiality obligations 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 が本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.

お客様は、適用される法令により禁止されていない限り、本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, 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.

5. **国際的な移転** 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、個人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。当該移転を行う場合、Secureworks は、CRA 又は DPA に関連して移転された個人データを保護するために適切な保護措置を講じるものとします。本サービスの提供の際に、(EU データ保護指令 95/46/EC 又は GDPR に基づく十分性認定に基づかずに) 欧州経済領域 (European Economic Area、「EEA」) 域内から EEA 域外へ個人データが移転される場合、当該移転は次の各号に従って行われるものとします。

International transfers: Secureworks may, in connection with the provision of the Services, or in the normal course of business, make international transfers of the Personal Data to its Affiliates and/or Subprocessors. Where the provision of Services involves the transfer of Personal Data from countries within the European Economic Area ("EEA") to countries outside the EEA (which are not subject to an adequacy decision under Directive 95/46/EC or the GDPR) such transfer shall be subject to:

5.1 Secureworks が、当該個人データの移転に対して適切な保護措置を講じること。

Secureworks has implemented appropriate security measures to adequately protect the transfer of such Personal Data

5.2 Secureworks が、個人データに対してアクセス権を有する可能性がある関連会社との間で、欧州委員会が承認した標準契約条項 (「**標**

準契約条項」) を組み込んだグループ間契約を締結していること。
Secureworks having in place intra-group agreements with any Affiliates which may have access to the Personal Data, such agreements incorporating the applicable EU Commission approved Standard Contractual Clauses ("**Standard Contractual Clauses**"); and

5.3 Secureworks が、必要に応じて、復処理者との間で標準契約条項を組み込んだ契約を締結していること。
Secureworks having in place agreements with its relevant Subprocessors that incorporate the applicable Standard Contractual Clauses (as appropriate).

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

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、（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, law enforcement agency, Customer shall (unless prohibited by law) allow Secureworks to review the notification and Customer shall have due regard to any reasonable comments or amendments proposed by Secureworks.

7. **セキュリティーイベント・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、Secureworks が顧客に提供す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・データを処理できることに同意します。Secureworks は、セキュリティイベント・データに含まれる個人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て Secureworks が実施する、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、CRA 又は DPA 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義務を負わないものとします。お客様は、本サービスに関連して自己の個人データが Secureworks によって処理される自己の社員又はその他のデータ主体に対し、本条に規定されたセキュリティサービス、製品、サービスの開発、機能向上、改良目的で自己の個人データが Secureworks によって処理されることについて適切な通知を行うことを保証します。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 は当該命令に従い、速やかに、対象となるセキュリティイベント・データの匿名化、仮名化、又は消去を行うことに同意します。
Security Event Data: Secureworks will process Security Event Data as part of its provision of Services. Customer acknowledges that Secureworks may also process Security Event Data in order to develop, enhance and/or improve its security services and the products and services it offers and provides 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 in connection with Secureworks' processing such Security Event Data for the purposes described in this clause, however, 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 CRA and/or the DPA, or the disclosure is required in order to comply with applicable law or legal process. Secureworks shall not be required to return or delete Security Event Data upon termination of the Services (for any reason). Customer shall ensure its personnel and any other data subjects whose personal data is processed by Secureworks in connection with the Services are appropriately notified of the fact their personal data may be processed in connection with the development, enhancement and/or provision of Secureworks' products or services as described in this clause. 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 appropriate, to anonymise, pseudonymise or 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.

別紙 1 - 処理の内容
Annex 1 – Processing description

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、注文書、SOW、SLA、サービス説明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 the Customer and processes the Personal Data for the purpose of providing such services as set out in applicable Service Orders, SOWs, SLAs, Service descriptions or otherwise
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
データ主体 **Data subjects**	次の区分に属する個人が、個人データの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 The Personal Data 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; and (iv) complainants, correspondents and enquirers
個人データの種類 **Type of personal data**	クラウドサービス及び MSS サービス：次の各号の個人データが対象となる可能性があります。 For both the SaaS and MSS Services: Personal Data may be contained:

	1. ユーザ名、ユーザ ID、ロケーション、IP アドレス、MAC アドレスなどのオンライン識別子、アクセスしたリソース、アクセス時刻、デバイス名などの、セキュリティログやアラートに含まれる IT リソースに関する情報。 within the security logs or alerts which may include information related to IT resources access, such as user name, identification number, location, IP address, MAC address or other device identifier, resource accessed, time of access and device name; 2. 悪意のあるファイル、ネットワーク・フラグメント、処理内容、ドメイン名、ネットワーク接続などの、セキュリティログやアラートに関する制御情報。 within context related to the security logs or alert which may include malicious files, network fragment, process details, domain name, network connections; and 3. Secureworks のクラウド又は MSS リソース（例：お客様ポータル）にアクセスするための、ユーザ・アカウント情報 within the user account created to access Secureworks SaaS or MSS resources (e.g. customer portal access). コンサルティングサービス: Secureworks がコンサルティングサービスを提供する上で、必要に応じて処理する可能性がある個人データには、以下に例示する情報が含まれます。 For SRC (Consulting) Services: Personal Data which may be processed by Secureworks if necessary, for the provision of the Consulting Services may include any or all of the following: 1. 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); 2. 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); 3. 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); 4. 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 subject's 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); 5. 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; 6. 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) 7. 偶発的に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.

別紙 2 - 情報セキュリティ対策

Annex 2 – Information 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 Data.

セキュリティに関する運用基準

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 の経営管理部門よって承認され、毎年見直しが行われています。

Security Practices 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

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。

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
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
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
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

Organizational Security 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. 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. Security testing, design and implementation of security solutions to enable security controls adoption across the environment.
3. Security operations of implemented security solutions, the environment and assets, and manage incident response.
4. 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

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。

- 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。
- 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。
- 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。

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。個人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。

Asset Classification and Control Secureworks' practice is to track and manage physical and logical assets. Examples of the assets that Secureworks IT might track include:

- Information Assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information.
- Software Assets, such as identified applications and system software.
- Physical Assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

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

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。

Personnel Security 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

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。

Physical and Environmental Security Secureworks uses a number of technological and operational approaches in its physical security program in regard 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 uniqueness 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

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。

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。

Communications and Operations Management 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.

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

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 Controls 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

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。

System Development and Maintenance 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

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個人情報の保護、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。

Compliance The information security, legal, privacy and compliance departments work to identify regional laws, 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 information, 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.