DATA PRIVACY TERMS FOR ACCENTURE HCM SERVICES

These Data Privacy Terms apply to Client Personal Information processed by Accenture and its subprocessors on Client's behalf in connection with its provision/performance of the SaaS Services, Support and Maintenance or other professional services described in the related Service Order or Order Form for Accenture HCM (the "Services").

Client shall be the controller of Client Personal Information, and Accenture shall be the processor of such data and each Party shall comply with the relevant data privacy laws to the extent applicable to such Party in its respective role. Client warrants to Accenture that it has all necessary rights to provide the Client Personal Data to Accenture for the processing to be performed in relation to the Services. Client shall be responsible for obtaining all necessary consents, and providing all necessary notices, as required under the relevant Data Protection Laws in relation to the processing of the Client Personal Data.

The Parties hereby acknowledge and agree to the following with respect to the processing of any Client Personal Information under these Data Privacy Terms:

1. Unless otherwise required by law, Accenture shall process Client Personal Information on Client's behalf as follows:

   - **The subject matter of the processing** is limited to the Client Personal Information identified in this document.
   - **The nature and purpose of the processing** shall be to provide the Services as defined in the description of the Services in the relevant Service Order or Order Form concluded between Client and Accenture.
   - **The duration of the processing** is the Term of the related Service Order or Order Form.
   - **The types of Personal Information** are: name, phone numbers, e-mail address, time zone, address data, system access /

アクセンチュア HCM サービスにおけるデータプライバシー規約

本データプライバシー規約は、アクセンチュア HCM の関連するサービス注文または注文書に記載された SaaS サービス、サポートおよびメンテナンス、またはその他のプロフェッショナルサービス（以下「サービス」といいます）の提供/履行に関連して、アクセンチュアおよびそのサブプロセッサーがお客様に代わって処理するお客様の個人データに適用されます。

お客様はお客様の個人データの管理者となり、アクセンチュアは当該データの処理者となり、各当事者はそれぞれの役割において当該当事者に適用される範囲で、関連するデータプライバシー法を遵守するものとします。お客様はアクセンチュアに対し、本サービスに関連して実施される処理のためにお客様の個人データをアクセンチュアに提供するために必要なすべての権利を有することを保証するものとします。 お客様は、お客様の個人データの処理に関して、関連するデータ保護法に基づき必要とされるすべての必要な同意を取得し、すべての必要な通知を提供する責任を負うものとします。

両当事者は、本データプライバシー規約に基づくお客様の個人情報の処理に関して、以下の事項を認識し、これに同意するものとします。

1. 法律で義務付けられている場合を除き、アクセンチュアはお客様の個人情報をお客様に代わって以下のように処理するものとします。

   - **処理の目的は**、本文書で特定されたお客様の個人データに限定されます。
   - **処理の性質および目的は**、お客様とアクセンチュアとの間で締結された関連するサービス注文書または注文フォームのサービスの説明に定義されているとおり、サービスを提供することであるものとします。
   - **処理の期間は**、対応するサービス注文書または注文フォームのサービスの期間となります。
   - 個人情報の種類は以下の通りです。 氏名、電話番号、電子メールアドレス、タイムゾーン、住所データ、システムアクセス/使用

usage / authorization data, company name, contract data, invoice data. Client acknowledges that the following types of Personal Information cannot be entered by the Authorized Users into the SaaS Services or processed by Accenture while performing Services:

- Debit card number
- Credit card number
- Credit reports, credit scores and fraud alerts
- Loan or deposit balances
- Payment or purchase history (including information relevant to targeted marketing, e.g., product order history, service subscription history, descriptive listing of consumers)
- Medical care info, such as admissions, discharges, organ donations, medications, data pertaining to the health status of the data subject; this encompasses Protected Health Information as defined in 45 CFR 160.103 of the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Genetic Information
- Biometric identifiers (DNA, finger, iris or retina recognition, facial recognition, hand geometry, ear, signature, and voice prints/speaker recognition technology, speaker verification or authentication)
- Geo-location information (GPS, Movement, GSP, Wifi, Bluetooth data)
- “Black Box” Data; e.g. telemetric, in-vehicle or in-home monitoring
- Conversations (voice recordings, transcripts, or overheard)

/承認データ、会社名、契約データ、請求書データ。お客様は、認定ユーザーが以下の種類の個人データを SaaS サービスに入力すること、またはサービスを提供する過程でアクセンチュアが処理することができないことを認めるものとします。

- デビットカード番号
- クレジットカード番号
- 信用報告書、信用スコア、不正行為警告
- ローン残高または預金残高
- 支払履歴または購入履歴（ターゲットマーケティングに関連する情報、例：製品の注文履歴、サービスの登録履歴、消費者の記述的リストを含む）
- 入退院、臓器提供、投薬、健康状態データなどの医療情報。これには、1996 年医療保険の 相互運用性と説明責任に関する法律（HIPAA）45 CFR 160.103 に定義される保護されるべき医療情報が含まれます。
- 遺伝子情報
- バイオメトリクス識別子（DNA、指、虹彩または網膜認識、顔認識、掌形認識、耳、署名および声紋/話者認識技術、話者の検証/認証）。
- 地理位置情報（GPS、移動、GSP、Wifi、Bluetooth データ）
- 「ブラックボックス」データ、例えばテレメトリー、車内監視、家庭監視など
- 会話（音声録音、記録、立ち聞き）

- Political Views (affiliation or support with a political party or ideology)
- Criminal charges and convictions and court records.

- **The categories of data subjects** are: unless provided otherwise by Client, will include employees, contractors, business partners or other individuals whose Personal Information is stored in the SaaS Services or in the Client's HR system of records.

2. Accenture will process Client Personal Information only in accordance with Client's documented instructions. These Data Privacy Terms constitute such documented initial instructions. Accenture shall use reasonable efforts to follow any other Client's instructions as long as they are required by law, technically feasible and do not require changes to the Services. If Client requires that Accenture follow a processing instruction that may generate additional costs for Accenture, a mutually agreed change request to the Service Order, Order Form or GTC must be concluded in advance.

If Client requires that Accenture follow a processing instruction despite Accenture's notice that such instruction may, in Accenture's opinion, infringe an applicable Data Protection Law, Client shall be responsible for all liability, and shall defend, indemnify and hold Accenture harmless against all claims and damages, arising from any continued processing in accordance with such instruction.

3. All Accenture personnel, including subcontractors, authorized to process the Client Personal Information shall be subject to confidentiality obligations and/or subject to an appropriate statutory obligation of confidentiality.

4. Each Party shall implement appropriate **technical and organizational security measures** to safeguard Client Personal Information from unauthorized processing or accidental loss or damage. Client acknowledges and agrees that, taking into

- 政治的見解（政党やイデオロギーへの所属または支持）
- 刑事告訴、有罪判決、裁判記録。

- **データ主体のカテゴリーには**、お客様が別途定める場合を除き、SaaS サービスまたはお客様の人事記録システムに個人データが保存されている従業員、請負業者、ビジネスパートナー、またはその他の人物が含まれます。

2. アクセンチュアは、お客様の個人データを、お客様の文書化された指示に従ってのみ処理するものとします。本データプライバシー規約は、そのような文書化された最初の指示に該当するものです。アクセンチュアは、法律で義務付けられており、技術的に実行可能であり、かつ本サービスに変更を必要としない限り、他のお客様の指示に従うよう合理的な努力を払うものとしますアクセンチュアに追加費用が発生する可能性のある処理指示に従うようお客様から要求される場合は、まずサービス注文書または注文フォーム、または GTC においての変更依頼は、事前に双方合意の上で締結されるものとします。

アクセンチュアからの通知にもかかわらず、お客様からアクセンチュアに処理指示に従うよう要求があった場合、その指示がデータ保護法に違反する可能性があるとアクセンチュアが判断した場合、お客様はすべての責任を負うものとし、当該指示に従って処理を継続することから生じるすべての請求および損害に対してアクセンチュアを防御し、補償し、損害を与えないものとします。

3. お客様の個人データを処理する権限を付与されたアクセンチュアのすべての人員（下請け業者を含む）は、守秘義務および適切な法的守秘義務を負うものとします。

4. 各当事者は、お客様の個人データを不正な処理または偶発的な損失もしくは損害から保護するために、適切な**技術的および組織的なセキュリティ対策**を実施するものとします。　お客様は、技術開発の現状、実施にかかる費用、およびお客様の個人データの処理の性質、範囲、

account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Information, as well as the likelihood and severity of risk to individuals, Accenture's implementation of and compliance with the security measures set forth in **Attachment A** to this document provide a level of security appropriate to the risk in respect of the processing of the Client Personal Information.

文脈および目的、ならびに個人に対するリスクの可能性および重大性を考慮した結果、アクセンチュアが**本付属書 A** に定めるセキュリティ対策を実施し遵守することが、お客様の個人データの処理に関するリスクに適したセキュリティレベルを提供することを認め、同意するものとします。

5. Client generally authorizes the engagement of Accenture's affiliates namely Accenture, Inc, based in Philippines and Accenture, LLP based in the U.S. as **subprocessors** and specifically authorizes, for the SaaS Services, the engagement of Accenture's Cloud Vendor SAP SE, as subprocessor. Accenture shall contractually require (including via standard contractual clauses, sub-processing agreements or, with respect to Accenture's affiliates, intra-company agreements) any such subprocessors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder to the extent applicable to the subprocessors' subcontracted services. Accenture shall remain fully liable for the performance of the subprocessors according to what provided for in the agreement with Client. Accenture shall provide Client with written notice of any intended changes to the authorized subprocessors and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes. If Client's objection is based on anything other than the proposed subprocessor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. Any disagreements between the Parties shall be resolved via the contract dispute resolution procedure. If Client's objection is based on the proposed Sub-processor's inability to comply with agreed data protection obligations, Client may, as a sole and exclusive remedy, object to such change by terminating the applicable Service upon written notice to

5. 一般的に、お客様は、アクセンチュアの子会社、すなわちフィリピンに本社を置くAccenture, Incおよび米国に本社を置くAccenture, LLPが**サブプロセッサー**として関与することに同意し、特にSaaSサービスについては、アクセンチュアのクラウドプロバイダーである SAP 欧州会社がサブプロセッサーとして関与することに同意するものとします。アクセンチュアは、契約上（標準的な契約条項、サブプロセス契約、またはアクセンチュア関連会社に関しては社内契約を通じて）、当該サブプロセッサーに対して、ブプロセッサーの委託サービスに適用される範囲において、アクセンチュアが本契約に基づき遵守することを要求されるものと少なくとも同程度に制限されたデータ保護義務を遵守するよう要求するものとします。　アクセンチュアは、お客様契約に規定されたサブプロセッサーのパフォーマンスに対して引き続き全責任を負うものとします。　アクセンチュアは、許可されたサブプロセッサーに意図された変更がある場合、お客様に書面で通知するものとし、お客様は、かかる変更に対する合理的な異議があれば、直ちに、いかなる場合でも10営業日以内に書面でアクセンチュアに通知するものとします。お客様の異議が、提案されたサブプロセッサーが合意されたデータ保護義務を遵守できないこと以外の理由に基づく場合、追加調整はお客様が負担するものとします。両当事者間の意見の相違は、契約紛争解決手続きを通じて解決されるものとします。お客様の異議が、提案されたサブプロセッサーが合意されたデータ保護義務を遵守できないことに基づいている場合、お客様は、アクセンチュアからの当該変更または追加に関する通知を受領してから90日以内に通知することを条件として、アクセンチュアへの書面による通知により、該当するサービスを終了することにより、唯一かつ排他的な救済として、当該変更に異議を申し立てることができます。

Accenture, provided that Client provides such notice within ninety (90) days of receiving Accenture's notice of such change or addition.

6. Taking into account the nature of the processing and when the processing is within the scope of the EU General Data Protection Regulation ("GDPR"), Accenture shall provide assistance to Client as reasonably requested in responding to requests by data subjects to exercise the rights set out in Chapter III of the GDPR , including rights of access, rectification, erasure, portability, and the right to restrict or object to certain processing. Client shall be responsible for the reasonable costs of such assistance.

6. 処理の性質を考慮し、処理がEU一般データ保護規則（「GDPR」）の範囲に含まれる場合、アクセンチュアは、アクセス権、修正権、消去権、ポータビリティ権、および特定の処理を制限または反対する権利を含む、GDPR第3章に規定された権利の行使に関するデータ主体からの要請に対応するため、合理的な要請に応じてお客様に支援を提供するものとします。 お客様は、かかる支援にかかる合理的な費用を負担するものとします。

7. Taking into account the nature of the processing and the information available to Accenture, when the processing is within the scope of the GDPR Accenture shall provide reasonable assistance to Client with respect to: (i) Client's implementation of appropriate security measures; (ii) Client's obligation to notify regulators and data subjects of a breach with respect to Client Personal Information as required by GDPR; (iii) Client's obligation to conduct data protection impact assessments with respect to the processing as required by GDPR (if applicable); and (iv) Client's obligations to consult with regulators as required by GDPR. Client shall be responsible for the reasonable costs of such assistance.

7. 処理の性質およびアクセンチュアが入手可能な情報を考慮し、処理がGDPRの範囲内である場合、アクセンチュアはお客様に対して以下に関して合理的な支援を提供するものとします。(1) お客様による適切なセキュリティ対策の実施、 (2) GDPRの要求に従い、お客様の個人情報に関する違反について規制当局およびデータ主体に通知するお客様の義務、 (3) GDPRが要求する処理に関するデータ保護影響評価を実施するお客様の義務（該当する場合）、 (4) GDPRが要求する規制当局との協議に関するお客様の義務。お客様は、かかる支援にかかる合理的な費用を負担するものとします。

8. Upon expiration or termination of the Services, Accenture **shall return or destroy** any Client Personal Information in accordance with the Client instruction as soon as reasonably practicable and within a maximum period of 180 days.

8. 本サービスの終了または終了後、アクセンチュアはお客様の指示に従い、合理的に実行可能な限り速やかに、最長 180 日以内にお客様の個人情報を**返却または破棄**するものとします。

9. Accenture shall make available to Client information reasonably requested by Client to demonstrate Accenture's compliance with its obligations in these Data Privacy Terms and Accenture shall submit to **audits** and inspections by Client (or Client directed third parties) in accordance with a mutually agreed process designed to avoid disruption of the Services and protect the

9. アクセンチュアは、アクセンチュアが本「データプライバシー規約」に基づく義務を遵守していることを証明するために、お客様から合理的に要求された情報をお客様に提供し、アクセンチュアは、本サービスの中断を回避し、アクセンチュア、アクセンチュアが承認したサブプロセッサーおよびその他のお客様の機密情報を保護するために、相互に合意したプロセスに従い、以下の原則に従って、お客様（または

confidential information of Accenture, its authorized subprocessors and its other clients and in accordance with the following principles:

- audit limited to once a year;
- not to exceed 3 business days unless otherwise agreed by the parties in writing.
- reasonable prior written notice (at least 60 days unless a data protection authority requires Client ’s earlier control under mandatory Data Protection Law).
- scope and agenda of the audit to be determined in advance.

With regard to this section, Accenture shall inform Client if, in Accenture’s opinion, any Client instruction infringes any applicable Data Privacy Law.

In the context of SaaS Services, Client acknowledges that Accenture’s Cloud Vendor use external, independent auditors to audit and verify the adequacy of their security measures, including the security of their physical data centers, and generate an audit report, available annually ("Report"). The Reports are the Cloud Vendors’ Confidential Information and will be available to Client, at Client’s request, subject to Client executing the Cloud Vendor’s standard non-disclosure agreement. Client agrees to exercise any right to conduct an audit or inspection of the Cloud Vendor, including under the EU Model Clauses (defined here below) if applicable, by instructing Accenture to obtain the relevant Cloud Vendor’s Report, as described in this section. Client may change this instruction at any time upon written notice to Accenture, provided if the Cloud Vendor declines to submit to an audit or inspection requested by Client, Accenture will not be in breach of these Data Privacy Terms, but Client is entitled to terminate the related Service Order to which such request relates upon 30 days’ notice to Accenture. If the EU Model Clauses apply, nothing in this section modifies the EU Model Clauses, and nothing in this Section

お客様が指示した第三者）による監査および検査に応じるものとします。

- 監査は年 1 回に限られ、
- 当事者が書面で別途合意した場合を除き、3 営業日を超えないものとします。
- 合理的な書面による事前通知（データ保護当局が強制的なデータ保護法に基づいてお客様の早期の管理を要求しない限り、少なくとも 60 日間）。
- 監査の範囲と議題は事前に決定されるものとします。

本項に関連して、アクセンチュアは、お客様からの指示が適用されるデータプライバシー法に違反するとアクセンチュアが判断した場合、お客様に通知するものとします。

SaaSサービスにおいて、お客様は、アクセンチュアのクラウドプロバイダーが独立した第三者監査人を用いて、物理的データセンターのセキュリティを含むセキュリティ対策の適切性を監査し、検証し、毎年入手可能な監査報告書（以下「報告書」といいます）を作成することを認めるものとします。 当該レポートはクラウドプロバイダーの機密情報であり、お客様がクラウドプロバイダーの標準的な機密保持契約に署名することを条件に、要求に応じてお客様に提供されるものとします。 お客様は、EU モデル条項（本項で定義）に該当する場合を含め、クラウドプロバイダを監査または検査する権利を行使する場合、アクセンチュアに対し、本条に記載される関連するクラウドプロバイダの報告書を取得するよう指示することに同意するものとします。 ただし、クラウドプロバイダーがお客様から要求された監査または検査に応じることを拒否した場合、アクセンチュアは本データプライバシー規約に違反しませんが、お客様は 30 日前までにアクセンチュアに通知することにより、当該要求に関連するサービス注文を解除する権利を有するものとします。 EU モデル条項が適用される場合、本項のいかなる規定も EU モデル条項を修正するものではなく、本項のいかなる規定も EU モデル条項に基づく監督当局またはデータ主体の権利に影響を与えるものではありません。

affects any supervisory authority's or data subject's rights under the EU Model Clauses.

10. As of the Effective Date of the relevant Service Order or Order Form, Client has identified for Accenture the countries where the data subjects originate.

11. Client acknowledges and agrees that:

11.1. The engagement by Accenture of the authorized sub-processors entail transferring or making Client Personal Information available for processing (including for storing, backup and archiving) to sub-processors located outside of the country(ies) the Client Personal Information originates from ("Data Transfer(s)"), as detailed in Section 5 above.

11.2. Data Transfers might involve destination country(ies) that do not provide an adequate level of protection for personal data as required by the applicable Data Protection Laws ("Third Countries").

11.3. When possible, Data Transfers out of the European Economic Area ("EEA"), the United Kingdom and/or Switzerland will be based on an adequacy decision issued by the competent authorities as applicable.

11.4. Data Transfers occurring out of the EEA, the United Kingdom and/or Switzerland to Third Countries will be governed by the Standard Contractual Clauses approved by the competent authorities as follows:

11.5. When the Accenture contracting entity, acting as a processor, is based within the EEA/UK/Switzerland, Data Transfers out of the EEA, UK and/or Switzerland to Accenture affiliates, acting as sub-processors, located in Third Countries, will be governed by the Module Three Processor-to-Processor of the EU Standard Contractual Clauses for the transfers of personal data to third countries pursuant to Regulation (EU) 679/2016, adopted by the EU Commission by its Implementing Decision (EU)

10. 関連するサービス注文書または注文フォームの発効日時点で、お客様はアクセンチュアのためにデータ主体の所在国を特定するものとします。

11. お客様は、以下を認識し、同意するものとします。

11.1. アクセンチュアが承認されたサブプロセッサーと契約する場合、上記第 5 項で詳述するとおり、お客様の個人データを、お客様の個人データの所在国以外に所在するサブプロセッサー（「データ移転」）に移転または処理（保管、バックアップ、アーカイブを含む）のために利用可能にすることが含まれます。

11.2. データ転送には、適用されるデータ保護法によって要求される個人データの適切な保護レベルを提供しない相手国（以下「第三国」といいます）が関与する可能性があります。

11.3. 可能な場合、欧州経済地域（「EEA」）、英国およびスイス以外へのデータの移転は、必要に応じて管轄当局が発行する妥当性決定に基づいて行われるものとします。

11.4. EEA、英国およびスイス以外の第三国へのデータの転送は、以下の管轄当局によって承認された標準契約条項によって管理されるものとします。

11.5. 処理者として行動するアクセンチュアの契約事業体が EEA/英国/スイス内に拠点を置いている場合、データは EEA、英国およびスイスから第三国にあるサブ処理者として行動するアクセンチュアの関連会社に転送され、EU 委員会が 2021 年 6 月 4 日の実施決定 (EU) 2021/914 により採択した規則 (EU) 679/2016（「2021 EU SCCs」）に従い、第三国への個人データの移転に関する EU 標準契約条項のモジュール 3 プロセッサーからプロセッサー（「2021 EU SCCs」）に準拠し、EEA、英国、スイス内に拠点を置くアクセンチュアの契約

2021/914 of 4 June 2021 (the "2021 EU SCCs"), that has been executed by Accenture contracting entities, based within the EEA, UK and Switzerland, and any such affiliate engaged as a sub-processor;

事業体、およびサブプロセッサーとして従事する当該関連会社により実施されるものとします。

11.6. When the Accenture contracting entity, acting as a processor, is based outside the EEA/UK/Switzerland, Data Transfers out of the EEA, UK and/or Switzerland to Accenture affiliates, acting as sub-processors, located in Third Countries, will be governed by the Module Two Controller-to-Processor (if Client acts as a controller) or the Module Three Processor-to-Processor (if Client acts as a processor) of the 2021 EU SCCs. Client shall execute - or shall procure that its EEA/UK/Swiss entities execute - the applicable Module of the 2021 EU SCCs with the concerned Accenture affiliates acting as sub-processors and importers;

11.6. プロセッサーとして行動するアクセンチュアの契約事業体が EEA/英国/スイス以外の国に拠点を置いている場合、EEA、英国およびスイスから第三国に所在するサブ処理者として行動するアクセンチュアの関連会社へのデータ移転は、2021 EU SCC のモジュール 2「管理者からプロセッサーへ」（お客様が管理者として行動する場合）またはモジュール 3「プロセッサーからプロセッサー」（お客様がプロセッサーとして行動する場合）に準拠するものとします。お客様は、サブプロセッサーおよび輸入業者としてのアクセンチュアの関連会社とともに、EEA/英国/スイスの事業体が該当する 2021 年 EU SCC の該当モジュールを実施する、または実施させるものとします。

11.7. Data Transfers out of the EEA, Switzerland and/or United Kingdom to Accenture engaged third-party sub-processors will be governed by sub-processing agreements, incorporating the applicable SCCs as necessary, executed by Accenture at global level with such third-party sub-processors.

11.7. EEA、スイスおよび英国外におけるアクセンチュアが雇用する第三者のサブプロセッサーへのデータの転送は、必要に応じて適用される SCC を組み込んだ、アクセンチュアが当該第三者のサブプロセッサーとグローバルに締結するサブプロセッシング契約によって管理されます。

11.8. For transfers of Client Personal Information out of countries other than the EEA, Switzerland and United Kingdom, the parties will work together expeditiously and in good faith to establish the appropriate transfer mechanism to be implemented, as required by Data Protection Law applicable to the data controller.

11.8. EEA、スイス、英国以外の国からお客様の個人情報を移転する場合、当事者は、データ管理者に適用されるデータ保護法の要求に従い、実施すべき適切な移転メカニズムを確立するために、迅速かつ誠実に協力するものとします。

11.9. If and when Accenture's Binding Corporate Rules for Processors are approved, the parties shall rely on such Binding Corporate Rules for Processors to cover any cross-border transfer of Client Personal Information to Accenture, provided that Accenture: (i) maintains the applicable approval of its Binding Corporate Rules for Processors for the duration of the agreement with the Client; (ii) promptly notifies Client of any subsequent material changes in the Binding

11.9. アクセンチュアのプロセッサーに関する拘束力のある企業規則が承認された場合、両当事者は、アクセンチュアへのお客様個人情報の国境を越えた移転について、以下のような当該プロセッサーに関する拘束力のある企業規則に依拠するものとします。(1) お客様との契約期間中、プロセッサーに関する拘束力のある企業規則の該当する承認を維持すること、(2) プロセッサーに関する拘束力のある企業規則または当該承認にその後重大な変更があった場合は、速やかにお客様に通知すること、(3) 「プロセッサーに関する拘束力のあ

Corporate Rules for Processors or such approval; and (iii) downstreams all of its applicable data protection obligations under its Binding Corporate Rules for Processors to sub-processors by entering into appropriate onward transfer agreements with any such subprocessors.

る企業規則」に基づき、当該プロセッサーとの間で適切な移転契約を締結することにより、当該プロセッサーが負うべきデータ保護義務のすべてを当該プロセッサーに移転すること。

11.10. Any data transfer agreements (including but not limited to any Standard Contractual Clauses approved by the competent supervisory authorities), that the parties or their affiliates may enter into in connection with the Services provided pursuant to a Service Order or Order Form and the GTC will be considered part of the respective Service Order, Order Form and the GTC and, without prejudice to the rights of any data subjects under any data transfer agreement, the liability terms set forth in the GTC will apply to all claims arising thereunder.

11.10. サービス注文書または注文フォームおよび本 GTC に従って提供されるサービスに関連して、当事者またはその関連会社が締結する可能性のあるデータ移転契約（管轄監督当局により承認された標準契約条項を含むが、これに限定されない）は、それぞれのサービス注文書、注文フォームおよび本 GTC の一部とみなされ、データ移転契約に基づくデータ主体の権利を損なうことなく、本 GTC に規定される責任条項が、それに基づいて生じるすべての請求に適用されるものとします。

Attachment A

Data Safeguards for Client Content

These data safeguards ("**Data Safeguards**") set forth the security framework that Client and Accenture will follow with respect to protecting Client Content in connection with the relevant Service Order or Order Form in place between the Parties. In the event of a conflict between these Data Safeguards and any terms and conditions set forth in the relevant Service Order, Order Form or the GTC, the terms and conditions of these Data Safeguards shall prevail.

I. **Controlling Standards.** Each Party will maintain and comply with globally applicable policies, standards and procedures intended to protect data within their own respective environments (e.g., systems, networks, facilities) and such policies will govern and control in their respective environments. Accenture and Client will comply with mutually agreed policies and standards, when relevant to the agreed services, and when accessing or operating within Client's or its Affiliate's environments. Each Party will provide timely notice of any changes to such policies that may materially degrade the security of the Services, after which the Parties will equitably adjust the terms of the applicable agreementas necessary to appropriately address risk. Each Party will not use software or hardware that is past its End of Life (EOL) in connection with the Services without a mutually agreed risk management process for such items.

II. **Penetration Testing of Accenture Systems.**

1. Accenture will perform annual penetration tests on Accenture's IT environments in accordance with Accenture's internal security policies and standard practices.

3. Accenture agrees to share with Client summary level information related to such tests as conducted by Accenture to the extent applicable to the Services.

附属書 A

お客様のコンテンツのデータ保護

これらのデータ保護措置（「データ保護措置」）は、両当事者間で締結された関連するサービス注文または注文書に関連するお客様のコンテンツの保護に関して、お客様とアクセンチュアが従うセキュリティの枠組みを定めるものです。　本「データ保護規定」と、関連する「サービス注文書」、「注文フォーム」、または「GTC」に記載されている諸条件との間に矛盾がある場合は、本「データ保護規定」の諸条件を優先するものとします。

I) **管理基準**　各当事者は、それぞれの環境（システム、ネットワーク、施設など）内のデータを保護するために設計された、グローバルに適用される方針、基準、手続きを維持し、遵守するものとし、かかる方針は、それぞれの環境において支配し、管理するものとします。アクセンチュアおよびお客様は、合意したサービスに関連する場合、およびお客様またはその関連会社の環境にアクセスまたは操作する場合、相互に合意したポリシーおよび基準を遵守するものとします。各当事者は、本サービスのセキュリティを著しく低下させる可能性のあるかかるポリシーの変更を適時に通知するものとし、その後、両当事者は、リスクに適切に対処するために必要に応じて、該当する契約条件を公平に調整するものとします。　各当事者は、本サービスに関連して、耐用年数（EOL）を過ぎたソフトウェアまたはハードウェアを、そのような品目のリスク管理プロセスについて相互に合意することなく使用しないものとします。

II) アクセンチュアのシステムへのペネトレーションテスト。

2. アクセンチュアは、アクセンチュア社内のセキュリティポリシーおよび標準的な慣行に従って、アクセンチュアの IT 環境に対するペネトレーションテストを毎年実施するものとします。

4. アクセンチュアは、本サービスに適用される範囲で、アクセンチュアが実施した当該試験に関する概要レベルの情報をお客様と共有することに同意するものとします。

5. For clarity, as it relates to such penetration testing, Client will not be entitled to (i) data or information of other customers or clients of Accenture; (ii) test third party IT environments except to the extent Accenture has the right to allow such testing; (iii) any access to or testing of shared service infrastructure or environments, or (iv) any other Confidential Information of Accenture that is not directly relevant to such tests and the Services.

6. 明確にするため、このようなペネトレーションテストに関連して、お客様は次の権利を有しないものとすします。 (1) アクセンチュアの他のお客様またはお客様のデータまたは情報、(2) アクセンチュアが当該テストを許可する権利を有する範囲を除く、第三者の IT 環境のテスト、(3) 共有サービスのインフラまたは環境へのアクセスまたはテスト、(4) かかるテストおよび本サービスに直接関連しないアクセンチュアのその他の機密情報。

7. For any Accenture IT systems that are physically dedicated to Client, the Parties may agree to separate, written testing plans.

8. 物理的にお客様専用となるアクセンチュアのコンピューターシステムについては、両当事者は別途書面によるテスト計画を合意できるものとします。

II. **Remote Work.** In addition to performing Services from Accenture locations, Accenture personnel may perform the Services or any portion of the Services remotely, provided that performing remotely does not (i) adversely impact Accenture's ability to perform its obligations under the relevant Servoce Order or Order Form; or (ii) require any increase to the Fees.

III) **リモートワーク。** アクセンチュアの社員は、アクセンチュアの拠点からサービスを実施することに加えて、サービスまたはサービスの一部を遠隔地から実施することができます。ただし、遠隔地から実施することが、(1)関連するサービス注文書または注文フォームに基づくアクセンチュアの義務の履行能力に悪影響を及ぼさないこと、または(2)料金の増額を必要としないことを条件とします。

For Services provided on a remote basis, any contractual requirements to provide physical and environmental security controls (e.g., secure bays; security guards; CCTV) at the Accenture service locations will not apply to remote work locations. In addition, where Accenture personnel are required to access Client systems from a remote work location, such access will only occur using Accenture devices.

遠隔地から提供される本サービスの場合、アクセンチュアのサービス拠点において物理的および環境的なセキュリティ管理（安全な保管庫、警備員、CCTV など）を提供する契約上の要件は、遠隔地の作業拠点には適用されません。 さらに、アクセンチュアの社員が遠隔地からお客様のシステムにアクセスする必要がある場合は、アクセンチュアのデバイスのみを使用してアクセスします。

IV. **Technical and Organizational Measures.** Without limiting the generality of the foregoing and subject to any other express agreement between the Parties with respect to the Services as set forth in the applicable Service Order or Order Form, the Parties have implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Client Content in their respective environments against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction, as set out below. To the extent the Client Content includes Personal Data, the implementation of and compliance with these measures and any additional security measures set out in the relevant Service Order or Order Form are designed to provide an appropriate level of security in respect of the processing of the Client Personal Data.

IV) 技術的**および組織的措置。** 上記の一般性を制限することなく、また、該当するサービス注文書または注文フォームに規定される、本サービスに関する両当事者間のその他の明示的な合意を条件として、両当事者は、以下に定めるとおり、偶発的、不正、または違法なアクセス、開示、改変、損失、または破壊からそれぞれの環境におけるお客様のコンテンツを保護するために設計された適切な技術的および組織的措置、内部統制、および情報セキュリティルーチンを実施し、維持するものとします。 お客様のコンテンツに個人データが含まれる限りにおいて、これらの措置の実施および実施、ならびに関連するサービス注文書または注文書に規定されている追加のセキュリティ措置は、お客様の個人データの処理に関して適切なレベルのセキュリティを提供するように設計されています。

1. **Organization of Information Security**

1.- **情報セキュリティの組織**

a) **Security Ownership.** Each Party will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.

a.- **セキュリティの所有権。** 各当事者は、セキュリティー基準及び手続を調整し監督する責任を負うセキュリティー責任者を指名するものとします。

b) **Security Roles and Responsibilities.** Each Party's personnel with access to Client Content will be subject to confidentiality obligations.

b.- **セキュリティーの役割と責任。** お客様のコンテンツにアクセスする各当事者の人員は、守秘義務を負うものとします。

c) **Risk Management Program.** Each Party will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Client Content in connection with the applicable Service Order or Order Form between the Parties.

c.- **リスク管理プログラム。** 各当事者は、両当事者間で適用されるサービス注文書または注文フフォームに関連して、お客様のコンテンツの処理に関連するリスクを特定、評価し、適切な措置を講じるためのリスク管理プログラムを実施するものとします。

2. **Asset Management**

2.- **資産管理**

a) **Asset Inventory.** Each Party will maintain a complete asset inventory of its infrastructure, network, applications and cloud environments. Each Party will also maintain an inventory of all of its media on which

a.- **資産目録。** 各当事者は、そのインフラ、ネットワーク、アプリケーション、クラウド環境の完全な資産目録を維持するものとします。 さらに、各当事者は、お客様のコンテンツが保存されているすべての媒体の目録を維持するものとしま

Client Content is stored. Access to the inventories of such media will be restricted to that Parties' personnel authorized in writing to have such access.

b) **Data Handling.** Each Party will

i. Classify Client Content to help identify such data and to allow for access to it to be appropriately restricted.

ii. Limit printing of Client Content from its systems to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Client Content.

iii. Require its personnel to obtain appropriate authorization prior to storing Client Content outside of contractually approved locations and systems, remotely accessing Client Content, or processing Client Content outside the Parties' facilities.

3. **Human Resources Security**

a) **Security Training.** Each Party will

i. Inform its personnel about relevant security procedures and their respective roles.

ii. Inform its personnel of possible consequences of breaching the security rules and procedures.

iii. Only use anonymous data in training.

4. **Physical and Environmental Security**

a) **Physical Access to Facilities.** Each Party will only allow authorized individuals to access its facilities where information systems that process Client Content are located.

b) **Physical Access to Components.** Each Party will maintain records of the incoming and outgoing media containing

す。 このような媒体の目録へのアクセスは、書面によりアクセスする権限を与えられた両当事者の担当者に制限されるものとします。

b.- **データ処理。** 各当事者は、

i. かかるデータの識別を支援し、かかるデータへのアクセスを適切に制限できるように、お客様のコンテンツを分類するものとします。

ii. システムからのお客様のコンテンツの印刷を、サービスを提供するために必要な最小限のものに制限し、お客様のコンテンツを含む印刷物を廃棄するための手順を整備するものとします。

iii. 契約上承認された場所およびシステム以外でお客様のコンテンツを保存する場合、お客様のコンテンツに遠隔アクセスする場合、または両当事者の施設外でお客様のコンテンツを処理する場合は、事前に適切な権限を得るよう、両当事者の従業員に要請するものとします。

3.- **人事セキュリティ**

a.- **セキュリティ研修。** 各当事者は、

i. 関連する保安手続及びそれぞれの役割について自国の従業員に通知するものとします。

ii. セキュリティ規則や手順に違反した場合、どのような結果が起こりうるかを従業員に通知するものとします。

iii. 研修では匿名データのみを使用するものとします。

4.- **物理的および環境的セキュリティ**

a.- **施設への物理的なアクセス。** 各当事者は、お客様のコンテンツを処理する情報システムが設置されている施設に、権限を付与された個人のみがアクセスできるようにするものとします。

b.- **部品への物理的アクセス。** 各当事者は、お客様のコンテンツを含む媒体の送受信について、媒体の種類、権限 を有する

Client Content, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of Client Content they contain.

c) **Component Disposal.** Each Party will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) processes to delete Client Content when it is no longer needed.

5. **Communications and Operations Management**

a) **Operational Policy.** Each Party will maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Client Content.

b) **Mobile Device Management (MDM)/Mobile Application Management (MAM).** Each Party will maintain a policy for its mobile devices that:

i. Enforces device encryption.

ii. Prohibit use of blacklisted apps.

iii. Prohibits enrollment of mobile devices that have been "jail broken."

c) **Data Recovery Procedures.** Each Party will

i. Have specific data recovery procedures with respect to its systems, in place designed to enable the recovery of Client Content being maintained in its systems.

ii. Review its data recovery procedures at least annually.

iii. Log data restoration efforts with respect to its systems, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if

送信者/受信者、日時、媒体の数、媒体に含まれるお客様のコンテンツの種類を含む 記録を保持するものとします。

c.- **部品の廃棄。** 各当事者は、お客様のコンテンツが不要になった場合、業界標準（例：ISO 27001、CIS Sans 20、および NIST Cyber-Security Framework、該当する場合）のプロセスを使用して削除するもとします。

5.- **コミュニケーションと運営管理**

a.- **運営ポリシー。** 各当事者は、そのセキュリティ対策、関連手順、およびお客様のコンテンツにアクセスできる担当者の責任を記載したセキュリティ文書を保持するものとします。

b.- **モバイルデバイス管理（MDM）/モバイルアプリケーション管理（MAM）。** 各当事者は、そのモバイル機器について、以下のポリシーを維持するものとします。

i. デバイスの暗号化を行うこと。

ii. ブラックリストに載ったアプリの使用を禁止すること。

iii. 「脱獄された」携帯端末の登録を禁止すること。

c.- **データ復旧の手順** 各当事者は、

i. 各当事者は、自己のシステムに関して、自己のシステム上に保持されている顧客コンテンツを検索できるように設計された特定のデータ検索手順を導入するものとします。

ii. 少なくとも年 1 回、データ復旧手順を見直すものとします。

iii. 責任者、復元されたデータの説明、該当する場合は責任者、データ復元プロセスにおいて手動入力が必要であったデータ（もしあれば）を含め、そのシステムに関するデータ復元作業を記録するものとします。

any) had to be input manually in the data recovery process.

d) **Malicious Software.** Each Party will have anti-malware controls to help avoid malicious software gaining unauthorized access to Client Content, including malicious software originating from public networks.

e) **Data Beyond Boundaries.** Each Party will

i. Encrypt Client Content that it transmits over public networks.

ii. Protect Client Content in media leaving its facilities (e.g., through encryption).

iii. Implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes from its systems.

f) **Event Logging.**

i. For its systems containing Client Content, each Party will log events consistent with its stated policies or standards.

6. **Access Control**

a) **Access Policy.** Each Party will maintain a record of security privileges of individuals having access to Client Content via its systems.

b) **Access Authorization.** Each Party will

i. Maintain and update a record of personnel authorized to access Client Content via its systems.

ii. When responsible for access provisioning, promptly provision authentication credentials.

d.- **マルウェア。** 各当事者は、公共ネットワークからの悪意のあるソフトウェアを含め、悪意のあるソフトウェアが顧客コンテンツに不正にアクセスすることを防止するために、マルウェア対策を講じるものとします。

e.- **境界を越えたデータ。** 各当事者は、

i. 公共ネットワーク上で送信するお客様のコンテンツを暗号化するものとします。

ii. お客様の施設を出る媒体上の顧客コンテンツを保護するものとします（暗号化など）。

iii. 可能な限り自動化ツールを導入し、システムから誤った E メール、手紙、ファックスを送信するリスクを減らすものとします。

f.- **イベントログ。**

i. 各当事者は、お客様のコンテンツを含むシステムに関して、その明記されたポリシーまたは基準に従ってイベントログを記録するものとします。

6.- **アクセス制御**

a.- **アクセスポリシー。** 各当事者は、そのシステムを通じてお客様のコンテンツにアクセスできる個人のセキュリティ権限の記録を保持するものとします。

b.- **アクセス許可。** 各当事者は、

i. そのシステムを通じてお客様のコンテンツにアクセスすることを許可された人員の記録を保持し、更新するものとします。

ii. アクセスの提供に責任を負う場合は、認証情報を速やかに提供するものとします。

iii. Deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed 90 days).

iv. Deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days.

v. Identify those personnel who may grant, alter or cancel authorized access to data and resources.

vi. Ensure that where more than one individual has access to its systems containing Client Content, the individuals have unique identifiers/log-ins (i.e., no shared ids).

c) **Least Privilege.** Each Party will

i. Only permit its technical support personnel to have access to Client Content when needed

ii. Maintain controls that enable emergency access to productions systems via firefighter ids, temporary ids or ids managed by a Privileged Access Management (PAM) solution.

iii. Restrict access to Client Content in its systems to only those individuals who require such access to perform their job function.

iv. Limit access to Client Content in its systems to only that data minimally necessary to perform the services.

v. Support segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of

iii. 認証情報が一定期間使用されなかった場合、その認証情報を無効にするものとします（かかる不使用期間は 90 日を超えないものとします）。

iv. アクセスが不要になったと通知された場合（従業員の解雇、プロジェクトの配置転換など）、2 営業日以内に認証情報を停止するものとします。

v. データおよびリソースへの認可されたアクセスを許可、変更、または取り消すことができる要員を特定するものとします。

vi. 複数の人がお客様のコンテンツを含むシステムにアクセスする場合、各人が固有の 識別子/ログインを持つようにします（すなわち、識別子を共有しない）。

c.- **最低限の特権。** 各当事者は、

i. その技術サポート要員に対して、知る必要がある場合にのみ、お客様のコンテンツへのアクセスを許可するものとします。

ii. 消防士の識別子、一時的な識別子、または特権アクセス管理（PAM）ソリューションによって管理される識別子を通じて、本番システムへの緊急アクセスを許可する管理を維持するものとします。

iii. システム上のお客様のコンテンツへのアクセスを、その職務を遂行するためにアクセスを必要とする者のみに制限するものとします。

iv. システム内のお客様のコンテンツへのアクセスを、サービス遂行に最低限必要なデータのみに制限するものとします。

v. セキュリティ上の利害の対立を生じさせるタスク（開発者/レビュアー、開発者/テスターなど）を実行するアクセス

interest (e.g., developer/ reviewer, developer/tester).

d) **Integrity and Confidentiality.** Each Party will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.

e) **Authentication.** Each Party will

i. Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access its information systems.

ii. Where authentication mechanisms are based on passwords, require that the passwords are renewed regularly.

iii. Where authentication mechanisms are based on passwords, require the password to contain at least eight characters and three of the following four types of characters: numeric (0-9), lowercase (a-z), uppercase (A-Z), special (e.g., !, *, &, etc.).

iv. Ensure that de-activated or expired identifiers are not granted to other individuals.

v. Monitor repeated attempts to gain access to its information systems using an invalid password.

vi. Maintain industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

vii. Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) password protection practices, including practices designed to maintain the confidentiality and

権を一人の人間が持たないように、環境間の職務分離をサポートするものとします。

d.- **完全性および機密性。** 各当事者は、施設を離れるとき、またはコンピュータが放置されているときは、管理セッションを無効にするようその要員を指導するものとします。

e.- **認証。** 各当事者は、

i. 情報システムにアクセスしようとするユーザーを特定し、認証するために、業界標準（ISO 27001、CIS Sans 20、およびNIST Cyber-Security Frameworkなど）を使用するものとします。

ii. 認証メカニズムがパスワードに基づく場合は、パスワードの定期的な更新を義務付けるものとします。

iii. 認証メカニズムがパスワードに基づいている場合、パスワードには少なくとも8文字と、次の4種類の文字のうち3種類を含めることを要求するものとします。数字（0～9）、小文字（a～z）、大文字（A～Z）、特殊文字（!、*、&など）

iv. 使用停止または期限切れの識別子が他人に付与されないようにします。

v. 無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するものとします。

vi. 業界標準の手順（ISO 27001、CIS Sans 20、NIST Cyber-Security Frameworkなど）を維持し、破損したパスワードや不注意で開示されたパスワードを無効にするものとします。

vii. パスワードが割り当てられ、配布されるとき、および保管中に、パスワードの機密性と完全性を維持するように設計された慣行を含む、業界標準（例えば、ISO 27001、CIS

integrity of passwords when they are assigned and distributed, as well as during storage.

f) **Multi Factor Authentication.** Each Party will implement Multi-Factor Authentication for internal access and remote access over virtual private network (VPN) to its systems. Client will enable Multi-Factor Authentication in its Successfactors systems.

7. **Network and Application Design and Management.** Each Party will

a) Have controls to avoid individuals gaining unauthorized access to Client Content in its systems.

b) Use email-based data loss prevention to monitor or restrict movement of sensitive data.

c) Use network-based web filtering to prevent access to unauthorized sites.

d) Use firefighter IDs or temporary user IDs for production access.

e) Use network intrusion detection and / or prevention in its systems.

f) Use secure coding standards.

g) Scan for and remediate OWASP vulnerabilities in its systems.

h) To the extent technically possible, work together to limit the ability of Accenture personnel to access non-Client and non-Accenture environments from the Client systems.

i) Maintain up to date server, network, infrastructure, application and cloud security configuration standards.

Sans 20、およびNIST Cyber-Security Framework、該当する場合）のパスワード保護慣行を使用するものとします。

f.- **多要素認証。** 各当事者は、そのシステムへの内部アクセスおよび仮想プライベートネットワーク（VPN）を介したリモートアクセスのために、多要素認証を導入するものとします。お客様は、サクセスファクターズのシステムで多要素認証を有効にするものとします。

7.- **ネットワークとアプリケーションの設計と管理**各当事者は、

a.- そのシステム内のお客様のコンテンツに個人が不正にアクセスできないように管理するものとします。

b.- 電子メールベースのデータ損失防止を使用して、機密データの移動を監視または制限するものとします。

c.- 許可されていないサイトへのアクセスを防ぐために、ネットワークベースのウェブフィルタリングを使用するものとします。

d.- プロダクション・アクセスには、ファイアーファイターID または一時的なユーザーID を使用するものとします。

e.- ネットワーク侵入検知および防止をシステムに使用するものとします。

f.- 安全なコーディング標準を使用するものとします。

g.- 自社システムの OWASP 脆弱性をスキャンし、修復するものとします。

h.- 技術的に可能な範囲で、アクセンチュアの社員がお客様のシステムからお客様以外の環境やアクセンチュア以外の環境にアクセスすることを制限するよう協力するものとします。

i.- 最新のサーバー、ネットワーク、インフラ、アプリケーション、クラウドのセキュリティ構成基準を維持するものとします。

j) Scan their respective environments to ensure identified configuration vulnerabilities have been remediated.

8. **Patch Management**

a) Each Party will have a patch management procedure that deploys security patches for its systems used to process Client Content that includes:

i. Defined time allowed to implement patches (not to exceed 90 days for high or medium patches as defined by the Party's respective standard); and

ii. Established process to handle emergency or critical patches as soon as practicable.

9. **Workstations**

a) Each Party will implement controls for all workstations it provides that are used in connection with service delivery/receipt incorporating the following:

a. Software agent that manages overall compliance of workstation and reports at a minimum on a weekly basis to a central server

c. Encrypted hard drive

e. Patching process so that workstations are patched within the documented patching schedule

g. Ability to prevent blacklisted software from being installed

i. Antivirus with a minimum weekly scan

k. Firewalls installed

10. **Information Security Breach Management**

a) **Security Breach Response Process.** Each Party will maintain a record of its own security breaches in its

j.- 各自の環境をスキャンし、特定された構成の脆弱性が修正されていることを確認するものとします。

8.- **パッチ管理**

a.- 各当事者は、お客様のコンテンツの処理に使用するシステムにセキュリティパッチを適用するパッチ管理手順を有し、これには以下が含まれます。

i. パッチの適用期間を定めること（各当事国の基準に定める高または中程度のパッチについては90日を超えないこと）。

ii. 緊急または重要なパッチを可能な限り速やかに処理するプロセスを確立すること。

9.- **ワークステーション**

a.- 各当事者は、自己が提供し、サービスの提供/受領に関連して使用されるすべてのワークステーションについて、以下を組み込んだ管理を実施するものとします。

b. ワークステーション全体のコンプライアンスを管理し、少なくとも毎週中央サーバーに報告するソフトウェアエージェント。

d. 暗号化されたハードドライブ

f. ワークステーションが文書化されたパッチ適用スケジュール内にパッチを受け取れるようにするためのパッチ適用プロセス。

h. ブラックリストに登録されたソフトウェアのインストールを防止する機能

j. 最低週1回のスキャンが可能なアンチウイルス

l. ファイアウォールの設置

10.- **情報セキュリティ侵害管理**

a.- **セキュリティ侵害への対応プロセス。** 各当事者は、違反の説明、期間、違反の結果、違反の報告者名および報告先、デ

systems with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.

b) **Service Monitoring.** Each Party's security personnel will review their own logs as part of their security breach response process to propose remediation efforts if necessary.

11. **Business Continuity Management**

Each Party will have processes and programs that are aligned to ISO 22301 to enable recovery from events that impact its ability to perform in accordance with the relevant Service Order or Order Form.

SUPPLEMENTARY MEASURES. In addition, in accordance with regulatory guidance following the European Court of Justice "Schrems II" decision, Accenture further commits to maintaining the following additional technical, organizational and legal/contractual measures with respect to Client Content, including personal data.

Technical Supplementary Measures:

1. The Client Content in transit between Accenture entities will be strongly encrypted with encryption that:

a. is state of the art,

b. secures the confidentiality for the required time period,

c. is implemented by properly maintained software,

d. is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and

ータの回復プロセスを記載した、各自のシステムのセキュリティ違反のログを保持するものとします。

b.- **サービス監視。** 各当事者のセキュリティー担当者は、セキュリティー侵害対応プロセスの一環として自らのログを確認し、必要であれば是正措置を提案するものとします。

11.- **事業継続管理**

各当事者は、関連するサービス注文書または注文フォームに従って履行する能力に影響を及ぼす事象からの回復を可能にするために、ISO22301 に準拠したプロセスおよびプログラムを実施するものとします。

補足措置。 加えて、欧州司法裁判所の「シュレムス II」判決後の規制ガイドラインに従い、アクセンチュアは、個人データを含むお客様のコンテンツに関して、以下の追加的な技術的、組織的、法的/契約上の措置を維持することを約束するものとします。

技術的補足措置：

1.- アクセンチュアの事業体間で転送されるお客様のコンテンツは、以下の暗号化方式で強力に暗号化されるものとします。

a.- 最新技術

b.- 必要な期間、機密保持を保証

c.- 適切にメンテナンスされたソフトウェアによって実装

d.- 堅牢であり、暗号解読を含む公的機関による能動的および受動的な攻撃からの保護を提供

e. does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client.

2. The Client Content at rest and stored by any Accenture entities will be strongly encrypted with encryption that:

a. is state of the art,

b. secures the confidentiality for the required time period,

c. is implemented by properly maintained software,

d. is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and

e. does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client.

Organizational Supplementary Measures:

1. The Client Content transfer between Accenture entities and the processing by any Accenture entities will be in accordance with:

a. Accenture's internal policies and procedures to manage requests from public authorities to access personal data,

b. Accenture's internal data access and confidentiality policies and procedures,

c. Accenture's internal data minimization policies and procedures, and

d. Accenture's internal data security and data privacy policies and procedures.

2. Accenture will maintain a documented log of requests for access to personal data received from public authorities and the response provided, along with the legal reasoning and the involved parties.

e.- 該当するお客様との別段の合意がない限り、ハードウェアまたはソフトウェアにバックドアを含まない

2.- アクセンチュアの各事業体によって保存される静止状態のお客様のコンテンツは、以下の暗号化方式で厳重に暗号化されます。

a.- 最新技術

b.- 必要な期間、機密保持を保証

c.- 適切にメンテナンスされたソフトウェアによって実装

d.- 堅牢であり、暗号解読を含む公的機関による能動的および受動的な攻撃からの保護を提供

e.- 該当するお客様との別段の合意がない限り、ハードウェアまたはソフトウェアにバックドアを含まない

組織の補足措置：

1.- アクセンチュアの事業体間でのお客様のコンテンツの移転、およびアクセンチュアの事業体による処理は、以下に従うものとします。

a.- 公的機関からの個人データへのアクセス要求に対応するためのアクセンチュアの社内方針および手順

b.- アクセンチュア社内のデータアクセスおよび機密保持に関するポリシーと手順

c.- アクセンチュア社内のデータ最小化方針および手順

d.- アクセンチュア社内のデータセキュリティおよびデータプライバシーの方針と手順

2.- アクセンチュアは、公的機関から受領した個人データへのアクセス要求とそれに対する回答を、法的根拠および関係者と共に文書化した記録を保持するものとします。

3. Accenture will regularly provide reports of public authority requests for personal data, if any, to Accenture's Chief Compliance Officer.

3.- アクセンチュアは、公的機関からの個人データの要求があった場合、アクセンチュアのチーフコンプライアンスオフィサーに定期的に報告するものとします。

Legal/Contractual Supplementary Measures:

法的/契約上の補足措置：

1. Accenture will maintain regularly updated assessment reports with respect to the surveillance laws and privacy practices for the countries in which Accenture processes Client Content where such country is not formally recognized as providing a lever of protection essentially similar to EU countries and will provide copies of applicable reports to clients upon request.

1.- アクセンチュアは、アクセンチュアがお客様のコンテンツを処理する国のプライバシー慣行および監督法に関して、その国が EU 諸国と実質的に同様の保護レベルを提供していると正式に認められていない場合、定期的に更新される評価報告書を維持し、要求に応じて該当する報告書の写しをお客様に提供するものとします。

2. The Accenture entity/s processing Client Content certify that, unless otherwise agreed with the applicable Client, (a) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data (b) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (c) to the best of Accenture's knowledge, applicable national law or government policy does not require the Accenture entity to create or maintain back doors or to facilitate access to personal data or systems or for the Accenture entity to be in possession or to hand over the encryption key without a legally valid order and following an appropriate legal review.

2.- お客様のコンテンツを処理するアクセンチュアの組織/団体は、該当するお客様と別段の合意がない限り、以下のことを証明するものとします。(a) システムおよび個人データへのアクセスに使用される可能性のあるバックドアまたは類似のプログラムを意図的に作成していないこと、(b) 個人データやシステムへのアクセスを容易にするような方法で、業務プロセスを意図的に作成または変更していないこと、 (c) アクセンチュアが知る限りにおいて、適用される国内法または政府の方針は、アクセンチュアの事業体に対して、法的に有効な令状がなく、かつ適切な法的審査の後でなければ、バックドアを作成もしくは維持すること、または個人データもしくはシステムへのアクセスを容易にすること、またはアクセンチュアの事業体が暗号化キーを所有もしくは提供することを要求していないこと。

3. To the extent permitted under applicable law the Accenture entity/s processing Client Content will inform the client of Government Requests relating to Personal Data that Accenture is processing on behalf of the client. If, under applicable law, Accenture is not permitted to inform the client of a Government Request, Accenture will take reasonable steps to either (i) obtain administrative or judicial leave to inform the client at the earliest possible time or (ii) request that the respective Government Authority directly informs the client. In any event, Accenture will take reasonable steps before the courts or in

3.- 適用される法律で許可される範囲内で、お客様のコンテンツを処理するアクセンチュアの事業体は、アクセンチュアがお客様のために処理している個人データに関連する政府からの要請をお客様に通知するものとします。適用される法律上、アクセンチュアが政府からの要請をお客様に通知することが許可されない場合、アクセンチュアは、(1)お客様に通知するための行政上または司法上の権限をできるだけ早く取得する、または(2)適切な政府当局がお客様に直接通知するよう要請するための合理的な手段を講じるものとします。いかなる場合においても、アクセンチュアは、違法と思われる政府勧誘に異議を唱えるため、裁判所または行政手続において妥当な措置を講じるものとします。

administrative proceedings to challenge Government Requests it deems unlawful.

4. Accenture will advise the applicable client of any change in applicable law that would affect Accenture's ability to comply with the data transfer mechanism relied on.

4.- アクセンチュアは、アクセンチュアが依存するデータ転送メカニズムに従う能力に影響を及ぼす可能性のある適用法の変更について、関連するお客様に通知するものとします。

5. The Accenture entity/s processing Client Content will allow the applicable client to verify if its personal data was disclosed to public authorities via agreed audit procedures as set out in the applicable client agreement.

5.- お客様のコンテンツを処理するアクセンチュアの事業体は、該当するお客様との契約に定める合意された監査手続を通じて、お客様の個人データが公的機関に開示されたかどうかを確認できるようにするものとします。

6. The Accenture entity/s processing Client Content will not engage in any onward transfer of Client Content, or suspend ongoing transfers, without the client's approval as required in the applicable client agreement or as otherwise required by law.

6.- お客様のコンテンツを処理するアクセンチュアの事業体は、該当するお客様との契約または法律で義務付けられているお客様の承認なしに、お客様コンテンツの転送または継続的な転送を停止しないものとします。

7. Nothing herein shall prejudice the rights of the data subject to recover damages from Accenture to the extent permitted by applicable law in the event Accenture discloses Client Content transferred in violation of its commitments contained under the chosen transfer tool.

7.- 本規約のいかなる規定も、アクセンチュアが選択した移転ツールに含まれるコミットメントに違反して移転されたお客様のコンテンツを開示した場合、データ対象者が適用法で認められる範囲でアクセンチュアに対して損害賠償を求める権利を損なうものではありません。