Celonis Information Security Annex

This Celonis Information Security Annex (the "Annex") sets forth the IT security and controls applicable to Celonis' provision of EMS (defined below) and is incorporated into and made part of Your agreement (including any Orders) governing Our provision of EMS to You (collectively, the "Agreement").

1. Definitions. All capitalized terms in this Annex have the meanings specified in the Agreement, except as otherwise provided below:

1.1 **"EMS"** means the Celonis Execution Management System, as made available to You under the Agreement.

1.2 **"High Availability"** means the elimination of single points of failure to enable applications to continue to operate even if one of the underlying IT components fails.

1.3 **"Information Security Incident"** means any confirmed (i) unauthorized access to, alteration of or damage to the EMS, or (ii) loss or unauthorized alteration of or damage to Customer Data or (iii) theft or unauthorized use, disclosure or acquisition of or access to any Customer Data.

1.4 **"Malware"** means any program or device (including any software, code or file) which is intended to prevent, impair or otherwise adversely affect the access to or operation, reliability or user experience of any computer software, hardware or network, telecommunications service, equipment or network or any other service or device, including without limitation worms, trojan horses, viruses, ransomware, trap doors and other similar malicious devices.

1.5 **"Principle of Least Privilege"** means allowing access for users (or processes acting on behalf of users) only as necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

2. Our Obligations.

2.1 We will comply with, and will cause Our employees to comply with, this Annex. As between You and Celonis, We are responsible for any failure of Our subcontractors to comply with any IT controls set forth in this Annex.

2.2 We will maintain Our comprehensive information security program in compliance with industry-recognized standards and applicable law. Our information security program includes administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Customer Data, and (ii) mitigate the threat of Information Security Incidents. Our information security program also includes a cybersecurity awareness program that informs and reminds employees of preventative measures to avoid inadvertent exposure of Customer Data or inadvertent exposure of EMS to unauthorized activity.

2.3 We will regularly test, review and update Our information security program.

Celonis 情報セキュリティ付属書

本 Celonis 情報セキュリティ付属書（以下、「付属書」といいます）は、当社の EMS（以下に定義されます）の提供に適用される IT セキュリティおよび管理事項について規定し、当社がお客様に EMS を提供する際に適用される当社の契約条件（注文書を含み、以下、「本契約」と総称します）の一部を構成します。

1. 定義 本付属書中の用語は、以下に定める場合を除き、本契約に定める意味を有するものとします。

1.1 **"EMS"**とは、本契約に基づきお客様に提供される、Celonis Execution Management System を意味します。

1.2 **"高可用性"**とは、単一の障害を排除し、基盤となる IT コンポーネントのいずれかが故障しても、アプリケーションを継続的に動作させることができるようにすることを意味します。

1.3 **"情報セキュリティインシデント"**とは、確認された(i)EMS への不正アクセス、改変もしくは損傷、(ii)顧客データの損失、不正改変、もしくは損傷、または(iii)顧客データの盗難もしくは不正な使用・開示・取得・アクセスを意味します。

1.4 **"マルウェア"**とは、コンピュータソフトウェア、ハードウェア、ネットワーク、電気通信サービス、機器、ネットワーク、その他のサービスや装置へのアクセスや操作、信頼性、ユーザーエクスペリエンスに悪影響を及ぼすことを意図したプログラムや装置（ソフトウェア、コード、ファイル等を含む）を意味し、ワーム、トロイの木馬、ウイルス、ランサムウェア、トラップドア、その他同様の悪質なものを含むものをいいます。

1.5 **"最小権限の原則"**とは、組織のミッションとビジネス機能に従って、割り当てられたタスクを達成するために必要な場合にのみ、ユーザー（またはユーザーの代理として行動するプロセス）に対してアクセスを許可することを意味します。

2. 当社の義務

2.1 当社は、本付属書を遵守し、当社の従業員に遵守させるものとします。 お客様とセロニスの間において、当社は、当社の委託先業者が本付属書に定める IT 管理事項を遵守しない場合、その責任を負うものとします。

2.2 当社は、業界で認知された基準および適用法に基づき、当社の包括的な情報セキュリ ティプログラムを維持します。 当社の情報セキュリティプログラムには、(i) 顧客データの安全性と機密性を確保し、(ii) 情報セキュリティインシデントの脅威を軽減するために設計された管理上、技術上、物理上、組織上、および運用上のセーフガード、ならびにその他のセキュリティ対策が含まれます。 また、当社の情報セキュリティプログラムには、顧客データの不用意な流出や EMS の不用意な情報流出を防ぐための予防策を従業員に通知し、周知・徹底させるサイバーセキュリティ啓発プログラムも含まれています。

2.3 当社は、当社の情報セキュリティプログラムを定期的にテストし、見直し、更新します。

3. Standards / Certifications .

3.1 We will maintain and will provide to You upon request and subject to confidentiality requirements, any then-available proof attestations of compliance with certifications and standards which may include, without limitation, the following:

i. SOC 1, Type 2;
ii. SOC2, Type 2;
iii. ISO 27001:2013;
iv. ISO 27701:2019;
v. TISAX; and
vi. ISO 9001:2015

3.2 You may view Our current list of certifications and compliance status at http://trust.celonis.com/.

3. 規格・認証

3.1 当社は、以下を含む規格・認証への準拠を証明するために、お客様の要求の時点で入手可能な証明書等を維持し、お客様の要請に応じて、機密保持の要件に従い、お客様にこれを提供します。

i. SOC 1, Type 2
ii. SOC2, Type 2
iii. ISO 27001:2013
iv. ISO 27701:2019
v. TISAX
vi. ISO 9001:2015

3.2 お客様は、当社の現在の認証および遵守状況に関するリストを、次のリンク先において確認することができます。

http://trust.celonis.com/

4. Encryption.

4.1 We will provide encryption for Your connection to EMS with a minimum encryption level equivalent to AES-128 (or then-current industry equivalent).

4.2 We will encrypt all Customer Data residing on backups with a minimum encryption level equivalent to AES-256.

4.3 We will encrypt Customer Data at rest with a minimum AES-256 bit encryption. Data will be encrypted, whether the storage device is powered on or off.

4.4 We will store secrets (i.e. encryption keys, certificates, passwords, hashes) in an appropriate service. We will not store system secrets in configuration files or in source code and will implement access controls designed to ensure that access to such information follows the Principle of Least Privilege.

4.5 We will encrypt all passwords with a minimum encryption level equivalent to AES-256

4.6 If You have purchased a private cloud instance, We will support use of encryption keys supplied by You (bring or hold Your own encryption key) and will provide a means of allowing You to rotate the key as documented in Our then-current product documentation.

4. 暗号化

4.1 当社は、お客様の EMS への接続に、最低限の暗号化レベルとして AES-128（またはその時点での業界の水準と同等レベル）と同等の暗号化方法を提供します。

4.2 当社は、バックアップに存在するすべての顧客データを、AES-256 を下回らない暗号化レベルで暗号化します。

4.3 当社は、保管中の顧客データを AES-256 ビットを下回らない方法で暗号化します。 データは、ストレージデバイスの電源のオン・オフにかかわらず、暗号化されます。

4.4 当社は、機密事項（すなわち、暗号化キー、証明書、パスワード、ハッシュ等）を適切なサービスに保存します。当社は、システムの機密事項を設定ファイルやソースコードに保存せず、当該機密事項へのアクセスが「最小権限の原則」に従うことを確保するように設計されたアクセス制御を実施します。

4.5 当社は、すべてのパスワードを AES-256 と同等、かつこれを下回らない暗号化レベルで暗号化します。

4.6 お客様がプライベートクラウドインスタンスを購入した場合、当社は、お客様が提供した暗号キーの使用をサポートし（すなわち、お客様自身の暗号キーを持参または保持し）、当該時点で当社の製品の説明書類に記載されるとおり、お客様が暗号キーをローテーションする手段を提供します。

5. Controls.

5.1 EMS.

5. 制御

5.1 EMS

i. EMS is hosted on platforms provided by third party cloud providers. We will have in place, maintain, and use information security measures, including physical, technical, and administrative controls, reasonably designed to prevent unauthorized access to EMS.

ii. We will maintain logical separation between the EMS cloud environment and Our internal business network.

iii. Our employees and subcontractors will use securely designed access methods to access EMS for support services.

iv. We will monitor EMS for indicators of unauthorized activity or compromise and have a dedicated security operations organization. We will retain logs of detection and blocking events for a minimum of one (1) year unless applicable law requires retention for a different period.

v. We will implement security measures engineered to facilitate a secure development lifecycle that is designed to systematically reduce the frequency and severity of vulnerabilities in code.

vi. We will utilize industry standard safeguards against Malware and malicious activity in EMS.

vii. We will not knowingly introduce Malware into EMS.

viii. We will implement and maintain security controls designed to protect EMS against known industry threats, such as the "OWASP Top 10" threats, via secure coding practices and appropriate technical controls.

5.2 Operating System/Applications.

i. We will implement and maintain change management procedures for EMS which include Our testing, certification, and approval processes specifically related to standard bug fixes, updates, security patches, and upgrades made available to You.

5.3 Backups.

i. We will perform and continuously maintain replication of a primary production site's Customer Data within the same country as the primary production site. Encryption of and access to Customer Data for the replicated sites must comply with this Annex.

ii. We will maintain a business continuity and/or disaster recovery plan in relation to the provision of EMS, which will be tested regularly.

iii. EMS leverages backups of its application and analytics data. The automated backup system is configured to perform daily incremental data backups of production databases.

5.4 Authentication/Authorization/Access.

i. EMS は、第三者のクラウドプロバイダーが提供するプラットフォーム上にホストされています。 当社は、EMS への不正アクセスを防止するために合理的に設計された、物理上、技術上、管理上のコントロールを含む情報セキュリティ対策を講じ、維持し、使用するものとします。

ii. 当社は、EMS のクラウド環境と当社内部のビジネスネットワークとの間の論理的分離を維持するものとします。

iii. 当社の従業員および委託先事業者は、サポートサービスのために EMS にアクセスする際、安全に設計されたアクセス方法を使用します。

iv. 当社は、不正な活動や侵害の指標がないか EMS を監視し、専門のセキュリティ運用部門を設置します。当社は、適用法が異なる保存期間を要求しない限り、検出事項およびブロックイベントのログを最低 1 年間保持します。

v. 当社は、コードの脆弱性の頻度と深刻度を体系的に低減するように設計された安全な開発ライフサイクルを促進するよう設計されたセキュリティ手段を実施します。

vi. 当社は、EMS におけるマルウェアおよび悪意のある活動に対する業界標準の保護措置を用います。

vii. 当社は、故意に EMS にマルウェアを持ち込みません。

viii. 当社は、「OWASP トップ 10」のような既知の業界の脅威から EMS を保護するために設計されたセキュリティ管理策等を、安全なコーディングの実践と適切な技術管理措置によって実装し、維持します。

5.2 オペレーティングシステム／アプリケーション

i. 当社は、お客様に提供される標準的なバグフィックス、アップデート、セキュリティパッチ、およびアップグレードに特に関連する当社のテスト、認証、および承認プロセスを含む EMS の変更管理手順を実施し維持します。

5.3 バックアップ

i. 当社は、プライマリプロダクションサイトの顧客データの複製を、プライマリプロダクションサイトと同じ国内で実施し、継続的に維持します。 複製されたサイトの顧客データの暗号化および顧客データへのアクセスは、本付属書に準拠する必要があります。

ii. 当社は、EMS の提供に関連する事業継続計画および／または災害復旧計画を維持し、これを定期的にテストします。

iii. EMS は、そのアプリケーションおよび分析データのバックアップを活用します。自動バックアップシステムは、本番用データベースの増加分のデータバックアップを毎日実行するように設定されています。

5.4 認証/認可/アクセス権

i. We will require multi-factor authentication for all staff when gaining access to EMS, except where it is not technically possible.

ii. Supported authentication methods for Your Users are documented in Celonis product documentation.

iii. We will provide You with the option of multifactor authentication as documented in our product documentation.

iv. We will limit the number of Our support staff (including subcontractors) with persistent access to Customer Data consistent with the Principle of Least Privilege.

v. We will maintain an activity log of system access tracing such access back to specific employees of Ours who access the EMS production infrastructure, including those who may use administrator or other privileged access, on a central log server. We will implement and maintain a backup regime on the central log server. The retention period for such logs will be twelve (12) months. The activity log will be designed to include date and time, ID of who performed the action, resource accessed, event identifier, and event information. Log files will be immutable and inaccessible to administrators of the servers and resources being logged. We will regularly review logs related to the use of privileged access or anomalous security events (such as abnormal access attempts, critical data changes) to identify any irregularities.

5.5 Data Center Security.

i. EMS information-processing systems and supporting infrastructure will be located in data center facilities that meet Our requirements for physical security and provide an appropriate level of protection against unauthorized physical access, damage, and interference, which may include:

a. Physical access controls at building ingress points;
b. Identity controls of all visitors prior to sign-in;
c. Access control devices managing physical access to servers;
d. Regular review of physical access privileges;
e. Comprehensive monitor and alarm response procedures;
f. CCTV surveillance;
g. Appropriate fire detection and prevention systems;
h. Appropriate power redundancy and backup systems; and
i. Appropriate climate control systems.

5.6 Administrative Controls.

i. We will, to the extent legally permitted and in accordance with Our internal policies and processes, perform industry

i. 当社は、技術的に不可能な場合を除き、すべての要員が EMS にアクセスする場合において、多要素認証を要求します。

ii. お客様のユーザーに対してサポートされる認証方法は、Celonis 製品説明書に記載されています。

iii. 当社は、当社の製品説明書に記載されるとおり、お客様に多要素認証のオプションを提供します。

iv. 当社は、最小権限の原則に基づき、顧客データに持続的にアクセスできる当社のサポートスタッフ（委託先事業者を含む）の人数を制限するものとします。

v. 当社は、管理者またはその他の特別のアクセス権を使用する可能性のある従業員を含め、EMS のプロダクションインフラにアクセスする当社の特定の従業員を追跡するシステムアクセスのアクティビティログをセントラルログサーバーで維持します。当社は、セントラルログサーバーにバックアップ体制を導入し、維持します。 当該ログの保存期間は、12 ヶ月とします。 アクティビティログは、日時、アクティビティを行った者の ID、アクセスされたリソース、イベント識別子、イベント情報を含むように設計されます。 ログファイルは、不変であり、アクティビティを記録されるサーバーの管理者およびリソースがアクセスできないものとします。 当社は、特別のアクセス権の使用や異常なセキュリティイベント（すなわち、異常なアクセスの試行、重要なデータの変更等）に関連するログを定期的に確認し、異常の有無を確認します。

5.5 データセンターのセキュリティ

i. EMS の情報処理システムおよびそれを支えるインフラは、以下に掲げる物理的セキュリティに関する当社の要件を満たし、不正な物理的アクセス、損傷および干渉に対して適切なレベルの保護を提供するデータセンター設備に設置されます：

a. 建物の出入り口における物理的なアクセス制御
b. 設備入室前のすべての訪問者の身元管理
c. サーバーへの物理的アクセスを管理するアクセス制御装置
d. 物理的アクセス権の定期的な見直し
e. 包括的なモニターおよびアラーム応答手順
f. CCTV による監視
g. 適切な火災検知・防止システム
h. 適切な電源の冗長性とバックアップシステム
i. 適切な空調管理システム

5.6 管理手続

i. 当社は、法律に定める範囲内で、当社の内部方針および手続に従い、顧客データにアクセスする当社の従業員および委託先事

standard background checks on Our employees and subcontractors with access to Customer Data.

ii. Our employees are required to gain and maintain certification within Our security awareness and training program.

6. Data Deletion.

6.1 Within thirty (30) days of the expiry of Your Subscription Term or termination of the Agreement for any reason, and at Your request, We will either (i) securely destroy or render unreadable, undecipherable, or unrecoverable or (ii) deliver to You or Your designees all Customer Data or Confidential Information in Our possession, custody, or control.

7. Security Assessment and Testing.

7.1 We will conduct, or commission third parties to conduct, at Our expense, vulnerability assessments and penetration testing of EMS regularly. Such assessments and testing will include validation of Our compliance with the security requirements herein and identification of security vulnerabilities, if any, of EMS. On request, We will share a confidential summary of scope and methodology of testing from the third party assessor.

7.2 We will take reasonable steps to mitigate and remediate any confirmed zero-day vulnerabilities detected or identified in EMS through patching, decommissioning or compensating controls.

8. Information Security Incident Detection and Response

8.1 **Notice of Incident.** In the event We become aware of any confirmed Information Security Incident materially and adversely affecting Your data, We will notify You without undue delay. Such notice will summarize in reasonable detail, to the extent known, a description of the nature of the breach, the likely consequences and the measures taken to address the breach. We will also advise details of a contact point where further information can be obtained.

8.2 **Notice of Disclosure.** We will provide You with copies of any public disclosure including filings, communications, general notices, press releases, or reports related to any Information Security Incident affecting Your data ("Communications"). Where the content of any such Communications identifies or may reasonably identify You, We will seek Your approval prior to the disclosure of such information, where permitted by law.

8.3 We will provide reasonable assistance with regards to any legally required reporting in response to any unauthorized access to EMS affecting Your data.

業者について、業界標準相当のバックグラウンドチェックを実施します。

ii. 当社の従業員は、当社のセキュリティ説明会およびトレーニングプログラムにおいて認定を受け、維持することが要求されます。

6. データの削除

6.1 当社は、お客様のサブスクリプション期間の満了または理由の如何にかかわらず本契約の終了から 30 日以内に、お客様の要請に応じて、(i)当社が所有、保管または管理するすべてのお客様データまたは秘密情報を安全に破壊し、読み取り不能にし、解読不能または復元不能にし、または(ii)お客様またはお客様が指定した者に引き渡すものとします。

7. セキュリティアセスメントとテスト

7.1 当社は、当社の費用負担で、EMS の脆弱性評価および侵入テストを定期的に実施し、または第三者に委託します。かかる評価およびテストには、当社が本付属書のセキュリティ要件に準拠していることの検証、および EMS のセキュリティ脆弱性がある場合にはその特定が含まれます。お客様の要請がある場合、当社は、第三者評価者によるテストの範囲と方法に関する機密文書の要約版を共有します。

7.2 当社は、EMS において検出または特定されたゼロデイ脆弱性が確認された場合、パッチ適用、廃止、または補償的な手段を通じて、これに関する緩和および修復のための合理的な措置を講じます。

8. 情報セキュリティインシデントの検知と対応

8.1 **インシデントの通知** お客様のデータに重大かつ不利な影響を与える情報セキュリティインシデントが確認された場合、当社は、遅滞なくこれをお客様に通知します。当該通知は、当社の知る限りにおいて、違反の性質、予想される結果、および違反に対処するために取られる措置の説明を合理的な内容で要約されるものとします。また、当社は、お客様が追加の詳細を取得するための連絡先を通知するものとします。

8.2 **開示の通知** 当社は、お客様のデータに影響を与える情報セキュリティインシデントに関連する提出書類、コミュニケーション、一般通知、プレスリリース、または報告書を含む公開情報（以下、「コミュニケーション」といいます）の写しをお客様に提供します。当該コミュニケーションの内容がお客様を特定し、またはお客様を合理的に特定しうる場合、当社は、法律で認められる限りにおいて、当該コミュニケーションの開示に先立ってお客様に承諾を求めるものとします。

8.3 当社は、お客様のデータに影響を与える EMS への不正アクセスへの対応として、お客様が法的に要求される報告に関して、合理的な支援を提供します。

9. Customer Responsibilities

9.1 You are solely responsible for and shall take all reasonable steps to ensure appropriate administrative, technical, physical, organizational and operational safeguards are implemented and enforced for all areas under Your control, including but not limited to:

i. Ensuring that Customer Data for which HIPAA, FedRAMP or similar elevated security requirements apply is uploaded only to EMS instances specifically designated as appropriate for such data;

ii. Ensuring that payment card information is not uploaded or otherwise published to any EMS environment;

iii. Implementing all appropriate customer-configurable security controls to protect Your Customer Data;

iv. Implementing source system and Customer Data backups and appropriate data hygiene controls;

v. Ensuring any anonymization or pseudonymization tools (including those made available by Celonis) are configured properly;

vi. Safeguarding against Malware and other malicious activity, including without limitation scanning Your systems and Customer Data with current versions of industry-standard antivirus software and leveraging adequate firewall technologies;

vii. Monitoring and updating the Celonis status page to indicate incidents affecting availability (status.celonis.com). We will provide updates during the duration of any incident;

viii. Managing and protecting Your User roles and credentials; and

ix. Managing and protecting any encryption keys held by You to ensure the integrity, availability and confidentiality of the key and the Customer Data secured with such key.

9.2 You shall ensure that all Customer Data is subject to a regular backup cycle consistent with the nature of data being processed to ensure that data can be recovered in the event of any data loss, for which Celonis is not responsible. Recovery from backups shall be tested by You at least annually.

This Japanese version is a translation of the original in English, and is provided for informational purposes only. In case of any ambiguity or discrepancy, the English original will prevail

9. お客様の責任

9.1 お客様は、お客様の管理下にあるすべての領域（以下を含みますがこれらに限定されません）について、適切な管理上、技術上、物理上、組織上および運用上のセーフガードが実施および施行されるよう、単独で責任を負い、あらゆる妥当な措置をとるものとします。

i. HIPAA、FedRAMP または同様の高度なセキュリティ要件が適用される顧客データが、当該データに対して適切であると特に指定された EMS インスタンスにのみアップロードされることを確保すること。

ii. ペイメントカード情報がいかなる EMS 環境にもアップロードまたはその他の方法で公開されないことを保証すること。

iii. お客様の顧客データを保護するために、すべての適切な顧客設定のセキュリティ制御を実施すること。

iv. ソースシステムおよび顧客データのバックアップと適切なデータに関する衛生管理策を実施すること。

v. 匿名化または仮名化ツール（Celonis が提供するものを含む）が適切に設定されていることを確認すること。

vi. マルウェアおよびその他の悪意のある行為に対する保護（業界標準のウイルス対策ソフトウェアの最新バージョンによるお客様のシステムおよび顧客データのスキャン、適切なファイアウォール技術の活用を含みますが、これに限定されません）。

vii. 可用性に影響を及ぼすインシデントを示すために、Celonis ステータスページ（status.celonis.com）を監視し更新すること。当社は、あらゆるインシデントの期間中、更新情報を提供します。

viii. お客様のユーザーの役割および資格情報を管理し、保護すること。

ix. 暗号キーおよびこれによって保護される顧客データの完全性、可用性および機密性を確保するために、お客様が保有する暗号キーを管理および保護すること。

9.2 お客様は、セロニスが責任を負わないいかなるデータ損失の場合にもデータを回復できるよう、処理されるデータの性質に応じて定期的なバックアップサイクルの対象となるすべての顧客データを確保するものとします。バックアップからの復旧は、少なくとも年 1 回、お客様によりテストされるものとします。

本付属書の日本語版は、英語の原文を翻訳したものであり、情報提供のみを目的として提供されるものです。日本語版において曖昧さや矛盾がある場合、英語の原文が優先されます。