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.

Annexe sur la Sécurité de l'Information de Celonis

La présente Annexe sur la Sécurité de l'Information de Celonis (l'"Annexe") définit la sécurité et les contrôles informatiques applicables à la fourniture d'EMS (définie ci-dessous) par Celonis et est incorporée et fait partie intégrante de Votre contrat (y compris toute Commande) régissant Notre fourniture d'EMS à Vous (collectivement, le "Contrat").

1. Définitions. Tous les termes commençant par une majuscule dans la présente Annexe ont la signification qui leur est donnée dans le Contrat, sauf indication contraire ci-dessous :

1.1 **"EMS"** le « Exécution Management System » 'de Celonis, tel qu'il est mis à votre disposition dans le cadre du Contrat.

1.2 **"Haute disponibilité"** signifie l'élimination des points de défaillance uniques pour permettre aux applications de continuer à fonctionner même si l'un des composants informatiques sous-jacents tombe en panne.

1.3 **"Incident de sécurité de l'information"** signifie toute confirmation (i) d'un accès non autorisé, d'une altération ou d'un dommage au EMS, ou (ii) d'une perte ou d'une altération non autorisée ou d'un dommage aux Données Client, ou (iii) d'un vol ou d'une utilisation, d'une divulgation ou d'une acquisition non autorisée de toute Donnée du Client ou d'un accès à cette donnée.

1.4 **"Logiciels malveillants"** désigne tout programme ou dispositif (y compris tout logiciel, code ou fichier) destiné à empêcher, compromettre ou affecter négativement l'accès ou le fonctionnement, la fiabilité ou l'expérience de l'utilisateur de tout logiciel, matériel ou réseau informatique, service, équipement ou réseau de télécommunications ou de tout autre service ou dispositif, y compris, sans s'y limiter, les vers, les chevaux de Troie, les virus, les logiciels rançonneurs, les trappes et autres dispositifs malveillants similaires.

1.5 **"Principe du moindre privilège"** signifie que l'accès des utilisateurs (ou des processus agissant au nom des utilisateurs) n'est autorisé que dans la mesure nécessaire à l'accomplissement des tâches assignées, conformément aux missions de l'organisation et aux fonctions de l'entreprise.

2. Nos obligations.

2.1 Nous nous respecterons nos obligations et ferons à nos employés respecter nos obligations à la présente Annexe. Entre Vous et Celonis, Nous sommes responsables de tout manquement de nos sous-traitants à se conformer aux contrôles informatiques définis dans la présente Annexe.

2.2 Nous maintiendrons notre programme complet de sécurité de l'information en conformité avec les normes reconnues par l'industrie et la loi applicable. Notre programme de sécurité de l'information comprend des garanties administratives, techniques, physiques, organisationnelles et opérationnelles ainsi que d'autres mesures de sécurité conçues pour (i) assurer la sécurité et la confidentialité des Données Client et (ii) atténuer la menace d'incidents liés à la sécurité de l'information. Notre programme de sécurité de l'information comprend également un programme de sensibilisation à la cybersécurité qui informe et rappelle aux employés les mesures préventives à prendre pour éviter l'exposition par inadvertance des données des clients ou l'exposition par inadvertance de l'EMS à des activités non autorisées.

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/.

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.

5. **Controls.**

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

2.3 Nous testerons, réviserons et mettrons à jour régulièrement notre programme de sécurité de l'information.

3. **Normes / Certifications .**

3.1 Nous conserverons et Vous fournirons, sur demande et sous réserve des exigences de confidentialité, toutes les evidences disponibles à ce moment-là attestant de la conformité avec les certifications et les normes qui peuvent inclure, sans s'y limiter, les éléments suivants :

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

3.2 Vous pouvez consulter notre liste actuelle de certifications et de statuts de conformité ici http://trust.celonis.com/.

4. **Cryptage.**

4.1 Nous assurerons le cryptage de votre connexion à l'EMS avec un niveau de cryptage minimum équivalent à AES-128 (ou l'équivalent en vigueur dans l'industrie).

4.2 Nous crypterons toutes les Données Client résidant sur des sauvegardes avec un niveau de cryptage minimum équivalent à AES-256.

4.3 Nous crypterons les Données Client au repos avec un niveau de cryptage minimum AES-256 bits. Les données seront cryptées, que le dispositif de stockage soit sous tension ou hors tension.

4.4 Nous stockerons les secrets (c'est-à-dire les clés de cryptage, les certificats, les mots de passe, les hachages) dans un service approprié. Nous ne stockerons pas les secrets du système dans des fichiers de configuration ou dans le code source et nous mettrons en œuvre des contrôles d'accès conçus pour garantir que l'accès à ces informations respecte le principe du moindre privilège.

4.5 Nous crypterons tous les mots de passe avec un niveau de cryptage minimum équivalent à AES-256.

4.6 Si Vous avez acheté une instance de cloud privé, Nous prendrons en charge l'utilisation des clés de cryptage fournies par Vous (apportez ou détenez Votre propre clé de cryptage) et Nous fournirons un moyen de Vous permettre de faire tourner la clé comme indiqué dans Notre documentation produit alors en vigueur.

5. **Contrôles.**

5.1 EMS.

i. L'EMS est hébergé sur des plateformes fournies par des fournisseurs tiers de services cloud. Nous mettrons en place, maintiendrons et utiliserons des mesures de sécurité de l'information, y compris des contrôles physiques, techniques et administratifs, raisonnablement conçues pour empêcher tout accès non autorisé à l'EMS.
ii. Nous maintiendrons une séparation logique entre l'environnement cloud de l'EMS et notre réseau d'entreprise interne.
iii. Nos employés et sous-traitants utiliseront des méthodes d'accès sécurisées pour accéder à l'EMS pour les services d'assistance.
iv. Nous surveillerons l'EMS à la recherche d'indicateurs d'activité non autorisée ou de compromission et disposerons d'une organisation dédiée aux opérations de sécurité. Nous conserverons les journaux des événements de détection et de blocage pendant au moins un (1) an, à

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. 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

moins que la législation applicable n'exige une période de conservation différente.

v. Nous mettrons en œuvre des mesures de sécurité conçues pour faciliter un cycle de développement sécurisé destiné à réduire systématiquement la fréquence et la gravité des vulnérabilités dans le code.

vi. Nous utiliserons les mesures de protection standard de l'industrie contre les logiciels malveillants et les activités malveillantes dans l'EMS.

vii. Nous n'introduirons pas sciemment de logiciels malveillants dans l'EMS.

viii. Nous mettrons en œuvre et maintiendrons des contrôles de sécurité conçus pour protéger l'EMS contre les menaces connues du secteur, telles que les menaces du "Top 10" de l'OWASP, par le biais de pratiques de codage sécurisées et de contrôles techniques appropriés.

5.2 Système d'exploitation/applications.

i. Nous mettrons en œuvre et maintiendrons des procédures de gestion des changements pour l'EMS qui comprennent nos processus de test, de certification et d'approbation spécifiquement liés aux corrections de bogues standard, aux mises à jour, aux correctifs de sécurité et aux mises à niveau qui sont mis à votre disposition.

5.3 Sauvegardes.

i. Nous effectuerons et maintiendrons en permanence la réplication des Données Client d'un site de production primaire dans le même pays que le site de production primaire. Le cryptage des données du client et l'accès à ces données pour les sites répliqués doivent être conformes à la présente annexe.

ii. Nous maintiendrons un plan de continuité des activités et/ou de reprise après sinistre en ce qui concerne la fourniture de l'EMS, qui sera testé régulièrement.

iii. L'EMS utilise des sauvegardes de ses applications et de ses données analytiques. Le système de sauvegarde automatisé est configuré pour effectuer des sauvegardes incrémentielles quotidiennes des bases de données de production.

5.4 Authentification/Autorisation/Accès.

i. Nous exigerons une authentification multifactorielle pour tous les membres du personnel lorsqu'ils accèdent à l'EMS, sauf si cela n'est pas techniquement possible.

ii. Les méthodes d'authentification prises en charge pour Vos Utilisateurs sont décrites dans la documentation du produit Celonis.

iii. Nous Vous fournirons l'option d'authentification multifactorielle telle que décrite dans notre documentation produit.

iv. Nous limiterons le nombre de Notre personnel d'assistance (y compris les sous-traitants) ayant un accès permanent aux Données Client conformément au principe du moindre privilège.

v. Nous tiendrons un registre des activités d'accès au système, en remontant jusqu'aux employés spécifiques qui accèdent à l'infrastructure de production de l'EMS, y compris ceux qui peuvent utiliser l'accès administrateur ou d'autres accès privilégiés, sur un serveur central

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 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.

d'enregistrement. Nous mettrons en place et maintiendrons un système de sauvegarde sur le serveur central de journalisation. La période de conservation de ces journaux sera de douze (12) mois. Le journal des activités sera conçu de manière à inclure la date et l'heure, l'identifiant de la personne qui a effectué l'action, la ressource à laquelle on a accédé, l'identifiant de l'événement et les informations relatives à l'événement. Les fichiers journaux seront immuables et inaccessibles aux administrateurs des serveurs et des ressources enregistrés. Nous examinerons régulièrement les journaux relatifs à l'utilisation d'un accès privilégié ou à des événements de sécurité anormaux (tels que des tentatives d'accès anormales, des modifications de données critiques) afin d'identifier toute irrégularité.

5.5 Sécurité des centres de données.

i. Les systèmes de traitement de l'information de l'EMS et l'infrastructure de soutien seront situés dans des centres de données qui répondent à nos exigences en matière de sécurité physique et offrent un niveau approprié de protection contre l'accès physique non autorisé, les dommages et les interférences, ce qui peut inclure:
   a. Contrôles d'accès physiques aux points d'entrée du bâtiment ;
   b. Contrôle de l'identité de tous les visiteurs avant l'enregistrement ;
   c. Dispositifs de contrôle d'accès qui gèrent l'accès physique aux serveurs ;
   d. Révision périodique des privilèges d'accès physique ;
   e. Des procédures complètes de surveillance et de réponse aux alarmes ;
   f. Surveillance par télévision en circuit fermé ;
   g. Systèmes adéquats de détection et de prévention des incendies ;
   h. Systèmes adéquats de redondance et d'alimentation de secours ; et
   i. des systèmes de climatisation adéquats.

5.6 Contrôles administratifs.

i. Dans la mesure où la loi le permet et conformément à nos politiques et procédures internes, nous procéderons à des vérifications d'antécédents conformes aux normes du secteur pour nos employés et sous-traitants ayant accès aux Données Clients.

ii. Nos employés sont tenus d'obtenir et de conserver une certification dans le cadre de notre programme de sensibilisation et de formation à la sécurité.

6. Suppression des données.

6.1 Dans les trente (30) jours suivant l'expiration de Votre période d'abonnement ou la résiliation du Contrat pour quelque raison que ce soit, et à Votre demande, Nous (i) détruirons en toute sécurité ou rendrons illisibles, indéchiffrables ou irrécupérables, ou (ii) Vous remettrons, à Vous ou à Vos représentants, toutes les Données Client ou les informations confidentielles en notre possession, sous notre garde ou sous notre contrôle.

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 You may, at Your own expense, conduct security assessments of Your EMS applications, but only in accordance with Our "Guidelines for Security Assessment by Customers". The following activities are expressly prohibited:

i. Denial of service (DoS). You are expressly prohibited from utilizing any tools or services in a manner that performs DoS attacks or simulations of such against any EMS asset;
ii. Resource request flooding (e.g. HTTP request flooding, Login request flooding, API request flooding);
iii. Protocol flooding (e.g. SYN flooding, ICMP flooding, UDP flooding);
iv. Scanning or testing assets belonging to any other customer;
v. Gaining access to any data that is not wholly-owned by You;
vi. Performing automated testing of services that generate significant amounts of traffic; and
vii. Attempting phishing or other social engineering attacks against Our employees.

7.3 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.

7. Évaluation et test de la sécurité.

7.1 Nous effectuerons ou ferons effectuer par des tiers, à nos frais, des évaluations de la vulnérabilité et des tests de pénétration de l'EMS à intervalles réguliers. Ces évaluations et ces tests comprendront la validation de notre conformité aux exigences de sécurité énoncées dans le présent document et l'identification des failles de sécurité, le cas échéant, de l'EMS. Sur demande, nous communiquerons un résumé confidentiel de la portée et de la méthodologie des tests effectués par l'évaluateur tiers.

7.2 Vous pouvez, à Vos frais, procéder à des évaluations de la sécurité de vos applications EMS, mais uniquement en conformité avec nos "Lignes directrices pour l'évaluation de la sécurité par les clients". Les activités suivantes sont expressément interdites :

i. Déni de service (DoS). Il Vous est expressément interdit d'utiliser des outils ou des services permettant d'effectuer des attaques DoS ou des simulations d'attaques DoS contre tout actif de l'EMS ;
ii. L'inondation des demandes de ressources (par exemple, l'inondation des demandes HTTP, l'inondation des demandes de connexion, l'inondation des demandes API) ;
iii. L'inondation de protocole (par exemple, l'inondation SYN, l'inondation ICMP, l'inondation UDP) ;
iv. Scanner ou tester des actifs appartenant à un autre client ;
v. Accéder à des données qui ne Vous appartiennent pas entièrement ;
vi. Effectuer des tests automatisés de services qui génèrent un trafic important ; et
vii. Tenter des attaques de phising ou d'autres attaques d'ingénierie sociale contre Nos employés.

7.3 Nous prendrons des mesures raisonnables pour atténuer et remédier à toute vulnérabilité confirmée de type "zero-day" détectée ou identifiée dans l'EMS au moyen de correctifs, d'une mise hors service ou de contrôles compensatoires.

8. Détection et réponse aux incidents de sécurité de l'information

8.1 **Notification d'incident.** Si Nous prenons connaissance d'un incident de sécurité de l'information confirmé affectant matériellement et négativement vos données, Nous Vous en informerons sans délai excessif. Cette notification résumera de manière raisonnablement détaillée, dans la mesure où elle est connue, une description de la nature de la violation, les conséquences probables et les mesures prises pour remédier à la violation. Nous indiquerons également les coordonnées d'un point de contact où de plus amples informations peuvent être obtenues.

8.2 **Avis de divulgation.** Nous Vous fournirons des copies de toute divulgation publique, y compris les dépôts, les communications, les avis généraux, les communiqués de presse ou les rapports liés à tout incident de sécurité de l'information affectant Vos données ("communications"). Lorsque le contenu de ces communications Vous identifie ou peut raisonnablement vous identifier, Nous Vous demanderons Votre accord avant de divulguer ces informations, dans la mesure où la loi le permet.

8.3 Nous fournirons une assistance raisonnable en ce qui concerne tout rapport légalement requis en réponse à tout accès non autorisé à l'EMS affectant Vos données.

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.

9. Responsabilités des clients

9.1 Vous êtes seul responsable et devez prendre toutes les mesures raisonnables pour Vous assurer que des mesures de protection administratives, techniques, physiques, organisationnelles et opérationnelles appropriées sont mises en œuvre et appliquées pour tous les domaines sous Votre contrôle, y compris, mais sans s'y limiter, les suivants

i. Veiller à ce que les Données Client auxquelles s'appliquent les exigences HIPAA, FedRAMP ou des exigences de sécurité élevées similaires ne soient téléchargées que vers des instances de l'EMS spécifiquement désignées comme appropriées pour ces données ;

ii. Veiller à ce que les informations relatives aux cartes bleus ou de paiement ne soient pas téléchargées ou publiées d'une autre manière dans un environnement EMS ;

iii. En mettant en œuvre tous les contrôles de sécurité appropriés configurables par le client pour protéger Vos Données Client ;

iv. Mettre en œuvre des sauvegardes du système source et des Données Client ainsi que des contrôles d'hygiène des données appropriés ;

v. S'assurer que tous les outils d'anonymisation ou de pseudonymisation (y compris ceux mis à disposition par Celonis) sont configurés correctement ;

vi. Protéger contre les logiciels malveillants et autres activités malveillantes, y compris, sans s'y limiter, analyser Vos systèmes et les Données Clients avec les versions actuelles des logiciels antivirus standard de l'industrie et utiliser des technologies de pare-feu adéquates ;

vii. Contrôler et mettre à jour la page de statut de Celonis pour indiquer les incidents affectant la disponibilité (status.celonis.com). Nous fournirons des mises à jour pendant la durée de tout incident ;

viii. La gestion et la protection de Vos rôles d'utilisateur et de vos informations d'identification ; et

ix. Gérer et protéger toutes les clés de cryptage que Vous détenez afin d'assurer l'intégrité, la disponibilité et la confidentialité de la clé et des Données Client sécurisées par cette clé.

9.2 Vous devez Vous assurer que toutes les Données Client font l'objet d'un cycle de sauvegarde régulier compatible avec la nature des données traitées afin de garantir que les données peuvent être récupérées en cas de perte de données, pour laquelle Celonis n'est pas responsable. La récupération des sauvegardes doit être testée par Vous au moins une fois par an.

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

Cette version française est une traduction de l'original en anglais et n'est fournie qu'à titre d'information. En cas d'ambiguïté, contradiction ou de divergence, la version original en anglais prévaudra.