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 - Allegato sicurezza delle informazioni

Il presente Allegato sulla sicurezza delle informazioni di Celonis (l'"Allegato") definisce la sicurezza informatica e i controlli applicabili alla fornitura di EMS da parte di Celonis (definita in seguito) ed è incorporato e parte integrante del contratto con il Sottoscrittore (compresi eventuali Ordini) che disciplina la nostra fornitura di EMS all'Utente (il "Contratto").

1. **Definizioni.** Tutti i termini in maiuscolo contenuti nel presente Allegato hanno il significato specificato nel Contratto, salvo quanto diversamente previsto di seguito:
   1.1 **"EMS"** indica il sistema Celonis Execution Management System, come messo a disposizione del Sottoscrittore ai sensi del Contratto.
   1.2 **"Alta disponibilità"** si intende l'eliminazione dei singoli punti di guasto per consentire alle applicazioni di continuare a funzionare anche in caso di guasto di uno dei componenti IT sottostanti.
   1.3 **"Incidente di sicurezza delle informazioni"** si intende qualsiasi (i) accesso non autorizzato, alterazione o danneggiamento di EMS, o (ii) perdita, alterazione non autorizzata o danneggiamento dei Dati del Cliente o (iii) furto o uso non autorizzato, divulgazione, acquisizione o accesso a qualsiasi Dato del Cliente.
   1.4 **"Malware"** si intende qualsiasi programma o dispositivo (compreso qualsiasi software, codice o file) volto a impedire, compromettere o altrimenti influenzare negativamente l'accesso o il funzionamento, l'affidabilità o l'esperienza dell'utente di qualsiasi software, hardware o rete informatica, servizio, apparecchiatura o rete di telecomunicazione o qualsiasi altro servizio o dispositivo, compresi, a titolo esemplificativo e non esaustivo, worms, trojan horses , virus, ransomware, trap doors e altri dispositivi maligni simili.
   1.5 **"Principio del minimo privilegio"** significa consentire l'accesso agli utenti (o ai processi che agiscono per conto degli utenti) solo nella misura necessaria per svolgere i compiti assegnati in conformità alle missioni organizzative e alle funzioni aziendali.

2. **I nostri obblighi.**
   2.1 R ispetteremo e faremo in modo che i nostri dipendenti rispettino il presente Allegato. Per quanto riguarda il Cliente e Celonis, siamo responsabili di qualsiasi inadempienza dei nostri subappaltatori nel rispettare i controlli IT stabiliti nel presente Allegato.
   2.2 Manterremo il nostro programma completo di sicurezza delle informazioni in conformità agli standard riconosciuti dal settore e alla legge applicabile. Il nostro programma di sicurezza delle informazioni comprende salvaguardie amministrative, tecniche, fisiche, organizzative e operative e altre misure di sicurezza progettate per (i) garantire la sicurezza e la riservatezza dei Dati del cliente e (ii) mitigare la minaccia di incidenti di sicurezza delle informazioni. Il nostro programma di sicurezza delle informazioni comprende anche un programma di sensibilizzazione sulla sicurezza informatica che informa e ricorda ai dipendenti le misure preventive per evitare l'esposizione involontaria dei Dati del cliente o l'esposizione involontaria di EMS ad attività non autorizzate.

2.3 Verificheremo, rivisiteremo e aggiorneremo regolarmente il nostro programma di sicurezza delle informazioni.

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.

3. Norme / Certificazioni .

3.1 Manterremo e forniremo al Cliente, su richiesta e nel rispetto dei requisiti di riservatezza, qualsiasi attestazione di conformità alle certificazioni e agli standard disponibili in quel momento, che possono includere, a titolo esemplificativo, quanto segue:

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 L'utente può visualizzare il nostro elenco attuale di certificazioni e lo stato di conformità all'indirizzo http://trust.celonis.com/.

4. Crittografia.

4.1 F orniremo la crittografia per la vostra connessione a EMS con un livello minimo di crittografia equivalente a AES-128 (o equivalente all'epoca del settore).

4.2 Crittograferemo tutti i Dati del cliente che risiedono nei backup con un livello di crittografia minimo equivalente a AES-256.

4.3 Crittograferemo i Dati del Cliente a riposo con una crittografia minima AES-256 bit. I dati saranno crittografati indipendentemente dal fatto che il dispositivo di archiviazione sia acceso o spento.

4.4 Salveremo i segreti (ad esempio chiavi di crittografia, certificati, password, hash) in un servizio appropriato. Non salveremo i segreti del sistema nei file di configurazione o nel codice sorgente e implementeremo controlli di accesso volti a garantire che l'accesso a tali informazioni segua il principio del minimo privilegio.

4.5 Crittograferemo tutte le password con un livello di crittografia minimo equivalente ad AES-256.

4.6 Se il Sottoscrittore ha acquistato un'istanza di cloud privato, supporteremo l'uso di chiavi di crittografia fornite dal Sottoscrittore stesso (porterà o deterrà una propria chiave di crittografia) e fornirà un mezzo per consentire al Sottoscrittore di ruotare la chiave come documentato nella documentazione del prodotto in vigore.

5. Controlli

5.1 EMS.

i. L'EMS è ospitato su piattaforme fornite da fornitori di cloud di terze parti. Avremo, manterremo e utilizzeremo misure di sicurezza delle informazioni, compresi controlli fisici, tecnici e amministrativi, ragionevolmente progettati per impedire l'accesso non autorizzato a EMS.
ii. Manterremo una separazione logica tra l'ambiente cloud di EMS e la nostra rete aziendale interna.
iii. I nostri dipendenti e subappaltatori utilizzeranno metodi di accesso sicuri per accedere ad EMS per i servizi di supporto.
iv. Monitoreremo EMS alla ricerca di indicatori di attività non autorizzate o di compromissioni e disporremo di

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. 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

un'organizzazione dedicata alle operazioni di sicurezza. Conserveremo i registri degli eventi di rilevamento e blocco per un minimo di un (1) anno, a meno che la legge applicabile non richieda la conservazione per un periodo diverso.

v. Implementeremo misure di sicurezza volte a facilitare un ciclo di vita di sviluppo sicuro, progettato per ridurre sistematicamente la frequenza e la gravità delle vulnerabilità nel codice.

vi. Utilizzeremo le protezioni standard del settore contro il malware e le attività dannose nell'EMS.

vii. Non introdurremo consapevolmente malware in EMS .

viii. Implementeremo e manterremo i controlli di sicurezza designati per proteggere EMS dalle minacce note del settore, come le minacce "OWASP Top 10", attraverso pratiche di codifica sicure e controlli tecnici appropriati.

5.2 Sistema operativo/applicazioni.

i. Implementeremo e manterremo procedure di gestione delle modifiche per EMS che includano i nostri processi di test, certificazione e approvazione specificamente legati alle correzioni di bug standard, agli aggiornamenti, ai patch di sicurezza e agli upgrade resi disponibili all'utente.

5.3 Backup.

i. Eseguiremo e manterremo costantemente la replica dei Dati del cliente di un sito di produzione primario all'interno dello stesso paese del sito di produzione primario. La crittografia e l'accesso ai Dati del cliente per i siti replicati devono essere conformi al presente Allegato.

ii. Manterremo un piano di continuità operativa e/o di disaster recovery in relazione alla fornitura di SGA, che sarà testato regolarmente.

iii. EMS sfrutta i backup di applicazioni e dati analitici. Il sistema di backup automatico è configurato per eseguire quotidianamente backup incrementali dei dati dei database di produzione.

5.4 Autenticazione/Autorizzazione/Accesso.

i. Richiederemo l'autenticazione a più fattori per tutto il personale quando accede al sistema EMS, tranne nei casi in cui non sia tecnicamente possibile.

ii. I metodi di autenticazione supportati per i Vostri utenti sono documentati nella documentazione del prodotto Celonis.

iii. Vi forniremo l'opzione di autenticazione a più fattori come documentato nella documentazione del nostro prodotto.

iv. Limiteremo il numero del nostro personale di supporto (compresi i subappaltatori) con accesso persistente ai Dati del Cliente in conformità con il Principio del Minimo Privilegio.

v. Manterremo un registro delle attività di accesso al sistema che riconduca tale accesso a specifici Nostri dipendenti che accedono all'infrastruttura di produzione di EMS, compresi quelli che possono utilizzare l'amministratore o altri accessi privilegiati, su un server di registro centrale. Implementeremo e manterremo un regime di backup sul server di log centrale. Il periodo di conservazione di tali

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.

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:

registri sarà di dodici (12) mesi. Il registro delle attività sarà progettato in modo da includere la data e l'ora, l'ID di chi ha eseguito l'azione, la risorsa a cui si accede, l'identificatore dell'evento e le informazioni sull'evento. I file di registro saranno immutabili e inaccessibili agli amministratori dei server e delle risorse registrate. Esamineremo regolarmente i registri relativi all'uso di accessi privilegiati o a eventi di sicurezza anomali (come tentativi di accesso anomali, modifiche di dati critici) per identificare eventuali irregolarità.

5.5 Sicurezza del centro dati.

i. I sistemi di elaborazione delle informazioni di EMS e le infrastrutture di supporto saranno collocati in strutture di data center che soddisfano i nostri requisiti di sicurezza fisica e forniscono un livello adeguato di protezione contro l'accesso fisico non autorizzato, i danni e le interferenze, che possono includere:

a. Controlli fisici dell'accesso ai punti di ingresso dell'edificio;
b. Controllo dell'identità di tutti i visitatori prima dell'accesso;
c. Dispositivi di controllo degli accessi che gestiscono l'accesso fisico ai server;
d. Revisione periodica dei privilegi di accesso fisico;
e. Procedure complete di monitoraggio e risposta agli allarmi;
f. Sorveglianza a circuito chiuso;
g. Sistemi adeguati di rilevazione e prevenzione degli incendi;
h. S istemi di ridondanza e backup dell'alimentazione adeguati; e
i. Sistemi di controllo del clima adeguati.

5.6 Controlli Amministrativi

i. Nella misura consentita dalla legge e in conformità con le nostre politiche e processi interni, effettueremo controlli di base standard del settore sui nostri dipendenti e subappaltatori con accesso ai Dati del cliente.

ii. I nostri dipendenti sono tenuti ad acquisire e mantenere la certificazione nell'ambito del nostro programma di formazione e sensibilizzazione alla sicurezza.

6. Cancellazione dei dati.

6.1 Entro trenta (30) giorni dalla scadenza del Periodo di Sottoscrizione del Sottoscrittore o dalla risoluzione del Contratto per qualsiasi motivo, e su richiesta del Sottoscrittore, la Società (i) distruggerà in modo sicuro o renderà illeggibili, indecifrabili o irrecuperabili o (ii) consegnerà al Sottoscrittore o ai suoi incaricati tutti i Dati del Cliente o le Informazioni Riservate in nostro possesso, custodia o controllo.

7. Valutazione e test di sicurezza.

7.1 Condurremo, o incaricheremo terze parti di condurre a nostre spese, valutazioni di vulnerabilità e test di penetrazione di EMS regolarmente. Tali valutazioni e test comprenderanno la convalida della nostra conformità ai requisiti di sicurezza del presente documento e l'identificazione delle eventuali vulnerabilità di sicurezza

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.

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;

dell'EMS. Su richiesta, condivideremo una sintesi confidenziale dell'ambito e della metodologia dei test effettuati dal valutatore terzo.

7.2 Il Cliente può, a proprie spese, condurre valutazioni di sicurezza delle proprie applicazioni EMS, ma solo in conformità alle nostre "Linee guida per la valutazione della sicurezza da parte dei clienti". Le seguenti attività sono espressamente vietate:

i. Negazione del servizio (DoS). È espressamente vietato utilizzare strumenti o servizi in modo da eseguire attacchi DoS o simulazioni di tali attacchi contro qualsiasi asset di EMS;
ii. Inondazione di richieste di risorse (ad esempio, inondazione di richieste HTTP, inondazione di richieste di accesso, inondazione di richieste API);
iii. Protocollo di flooding (ad es. SYN flooding, ICMP flooding, UDP flooding);
iv. Scansione o test di risorse appartenenti a qualsiasi altro cliente;
v. Ottenere l'accesso a qualsiasi dato che non sia interamente di proprietà del Cliente;
vi. Esecuzione di test automatizzati di servizi che generano quantità significative di traffico; e
vii. Tentativi di phishing o altri attacchi di social engineering contro i nostri dipendenti.

7.3 Adotteremo misure ragionevoli per mitigare e rimediare a qualsiasi vulnerabilità "zero-day" confermata, rilevata o identificata nell'EMS, mediante patch, disattivazione o controlli di compensazione.

8. Rilevamento e risposta agli incidenti di sicurezza delle informazioni

8.1 Avviso di incidente. Nel caso in cui venissimo a conoscenza di un Incidente di Sicurezza delle Informazioni confermato, che abbia ripercussioni materiali e negative sui dati dell'Utente, lo comunicheremo all'Utente senza indebito ritardo. Tale avviso riassumerà in modo ragionevolmente dettagliato, per quanto noto, una descrizione della natura della violazione, delle probabili conseguenze e delle misure adottate per affrontare la violazione. Comunicheremo inoltre i dettagli di un punto di contatto per ottenere ulteriori informazioni.

8.2 Avviso di divulgazione. Vi forniremo copie di qualsiasi divulgazione pubblica, compresi i documenti, le comunicazioni, gli avvisi generali, i comunicati stampa o i rapporti relativi a qualsiasi incidente di sicurezza delle informazioni che riguardi i vostri dati ("comunicazioni"). Qualora il contenuto di tali comunicazioni identifichi o possa ragionevolmente identificare l'Utente, chiederemo l'approvazione dell'Utente prima della divulgazione di tali informazioni, ove consentito dalla legge.

8.3 Forniremo un'assistenza ragionevole per quanto riguarda qualsiasi segnalazione richiesta dalla legge in risposta a qualsiasi accesso non autorizzato ai dati dell'EMS.

9. Responsabilità del cliente

9.1 L'utente è l'unico responsabile e dovrà adottare tutte le misure ragionevoli per garantire l'implementazione e l'applicazione di adeguate misure di salvaguardia amministrative, tecniche, fisiche, organizzative e operative per tutte le aree sotto il suo controllo, tra cui, a titolo esemplificativo, le seguenti:

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.

i. Garantire che i Dati del Cliente per i quali si applicano i requisiti di sicurezza elevati HIPAA, FedRAMP o simili siano caricati solo nelle istanze EMS specificamente designate come appropriate per tali dati;

ii. Garantire che i dati delle carte di pagamento non vengano caricati o pubblicati in altro modo in nessun ambiente EMS;

iii. Implementare tutti gli appropriati controlli di sicurezza configurabili dal cliente per proteggere i Dati del Cliente;

iv. Implementare backup del sistema sorgente e dei Dati del Cliente e adeguati controlli di igiene dei dati;

v. Assicurare che qualsiasi strumento di anonimizzazione o pseudonimizzazione (compresi quelli resi disponibili da Celonis) sia configurato correttamente;

vi. Salvaguardare da malware e altre attività dannose, inclusa, senza limitazioni, la scansione dei sistemi dell'Utente e dei Dati del Cliente con versioni aggiornate di software antivirus standard del settore e l'utilizzo di tecnologie firewall adeguate;

vii. Monitorare e aggiornare la pagina di stato di Celonis per indicare gli incidenti che influiscono sulla disponibilità (status.celonis.com). Verranno forniti aggiornamenti durante la durata di qualsiasi incidente;

viii. Gestione e protezione dei ruoli e delle credenziali dell'Utente; e

ix. Gestione e protezione di qualsiasi chiave di crittografia in possesso dell'Utente per garantire l'integrità, la disponibilità e la riservatezza della chiave e dei Dati del Cliente protetti con tale chiave.

9.2 L'Utente dovrà garantire che tutti i Dati del Cliente siano soggetti a un ciclo di backup regolare e coerente con la natura dei dati elaborati, per assicurare che i dati possano essere recuperati in caso di perdita di dati, per la quale Celonis non è responsabile. Il ripristino dai backup dovrà essere testato dall'Utente almeno una volta all'anno.

This Italian 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

La presente versione italiana è una traduzione dell'originale in inglese e viene fornita solo a scopo informativo. In caso di ambiguità o discrepanze, prevarrà l'originale inglese.