La traduzione di seguito è fornita solo a scopo informativo. In caso di discrepanze, incongruenze o conflitti tra la presente traduzione e l'ultima versione in lingua inglese aggiornata (anche a causa di ritardi nella traduzione), prevarrà la versione in lingua inglese.

Soggetta a modifiche come indicato di seguito. Salvare una copia di questa versione come necessario per il proprio archivio.

POLITICA DI SICUREZZA DEI FORNITORI AMAZON

Ultimo aggiornamento: 11 settembre 2024

1. AMBITO DI APPLICAZIONE. Il Fornitore rispetterà questi requisiti di sicurezza (la "Politica di sicurezza"). La presente Politica sulla sicurezza non limita alcuno degli altri obblighi contrattuali o legali del Fornitore. Nella misura in cui vi sia un conflitto tra la presente Politica sulla sicurezza e altri accordi tra il Fornitore e Amazon, il Fornitore rispetterà i requisiti più restrittivi che meglio proteggono le Informazioni di Amazon. Qualsiasi riferimento in altri accordi tra il Fornitore e Amazon ai Requisiti di sicurezza di terze parti sarà interpretato come riferimento alla presente Politica sulla sicurezza.

2. AGGIORNAMENTI.

2.1 Amazon potrà apportare di volta in volta degli aggiornamenti commercialmente ragionevoli alla presente Politica sulla sicurezza, che entreranno in vigore 30 giorni dopo la data dell'"Ultimo aggiornamento" alla presente Politica sulla sicurezza. Il Fornitore accetta di essere vincolato dalla Politica sulla sicurezza aggiornata una volta entrati in vigore gli aggiornamenti.

2.2 Se il Fornitore desidera ricevere un preavviso di tali aggiornamenti prima che diventino effettivi, il Fornitore potrà iscriversi per ricevere avvisi di aggiornamento utilizzando il modulo di iscrizione presente in questa pagina web della Politica sulla sicurezza. Il Fornitore garantirà che tutti propri recapiti forniti per l'iscrizione alla ricezione degli avvisi di aggiornamento siano sempre aggiornati e accurati. Si riterrà che il Fornitore abbia ricevuto qualsiasi avviso di aggiornamento al momento dell'invio tramite e-mail, indipendentemente dal fatto che il Fornitore lo riceva effettivamente o meno.

3. SCOPO CONSENTITO.

3.1 **Espressa autorizzazione.** Il Fornitore potrà trattare solo le Informazioni di Amazon espressamente autorizzate ai sensi del Contratto e al solo scopo di fornire i prodotti o servizi ai sensi del Contratto (lo "Scopo consentito").

3.2 **Conservazione dei dati**. Il Fornitore conserverà le Informazioni di Amazon solo per lo scopo e per il tempo necessario allo Scopo consentito.

3.3 **Limitazioni esplicite**. Il Fornitore dovrà altrimenti astenersi dal: (a) trattare qualsiasi Informazione di Amazon, anche se anonimizzata; (b) trasferire, affittare, scambiare, commerciare, vendere, prestare, noleggiare o altrimenti distribuire o rendere disponibile a terzi qualsiasi Informazione di Amazon, anche se anonimizzata; o (c) sviluppare, addestrare o migliorare qualsiasi modello di Intelligenza artificiale (IA) o di Apprendimento automatico (ML) utilizzando le Informazioni di Amazon, anche se anonimizzate.

4. REQUISITI MINIMI DI SICUREZZA. Il Fornitore manterrà misure di salvaguardia fisiche, amministrative e tecniche coerenti con le migliori pratiche di settore (tra cui gli standard 27001 e 27002 dell'Organizzazione Internazionale per la Standardizzazione ("ISO"), il Quadro di sicurezza

informatica del National Institute of Standards and Technology ("NIST"), o altri standard simili). Le garanzie mantenute dal Fornitore includeranno i requisiti minimi descritti di seguito nelle Sezioni 4.1 – 4.18.

4.1 **Programma scritto per la sicurezza delle informazioni**. Il Fornitore avrà un programma scritto per la sicurezza delle informazioni che: (a) include politiche, procedure e standard adeguati che soddisfano i requisiti stabiliti nella presente Politica sulla sicurezza; (b) designa un referente per la sicurezza responsabile della comunicazione e della gestione dei problemi di sicurezza (compresi gli Incidenti di sicurezza); (c) viene rivisto almeno una volta all'anno e aggiornato ove necessario; e (d) si applica al Personale. Il Fornitore monitorerà e applicherà il proprio programma per la sicurezza delle informazioni e farà fronte alle violazioni.

4.2 **Gestione delle patch**. Il Fornitore manterrà aggiornati i Sistemi Informatici Interessati con gli ultimi aggiornamenti, correzioni di bug e nuove versioni. Il Fornitore attuerà delle misure di mitigazione per risorse non aggiornabili.

4.3 **Registrazione.** Il Fornitore raccoglierà, gestirà e conserverà i registri di audit, eventi e sicurezza, tra cui: (a) i dati di registro su tutti gli usi (sia autorizzati che non autorizzati) degli account o delle credenziali di Amazon forniti al Fornitore per uno Scopo consentito, e (b) i dati di registro su qualsiasi tentativo, riuscito e non, di impersonare il personale di Amazon o i membri del Personale aventi accesso alle Informazioni di Amazon o ai Sistemi Informatici Interessati. Tali registri conterranno dati sufficienti per identificare ogni evento registrato: (i) il Personale o l'account che avvia l'evento, (ii) l'ora dell'evento e (iii) il sistema, i dati o altre risorse interessate. Il Fornitore analizzerà regolarmente tali registri per aiutare a rilevare, indagare ed effettuare il ripristino da attività non autorizzate.

4.4 **Difese da malware**. Il Fornitore (a) distribuirà software anti-malware o un controllo di sicurezza equivalente a tutti i Sistemi Informatici Interessati; (b) manterrà gli aggiornamenti, le firme e le configurazioni del software anti-malware o controllo di sicurezza equivalente; e (c) configurerà i sistemi per rilevare, prevenire e correggere l'installazione, la diffusione e l'esecuzione di codice dannoso o non autorizzato.

4.5 **Programma di gestione dei rischi**. Il Fornitore disporrà di un programma scritto di gestione dei rischi per la sicurezza delle informazioni, che definisce i processi per l'analisi, il trattamento e l'accettazione dei rischi e le relative eccezioni.

4.6 **Formazione sulla sensibilizzazione alla sicurezza**. Il Fornitore erogherà corsi di formazione per il Personale sulla sicurezza delle informazioni e sulla privacy al momento dell'assunzione e almeno una volta all'anno. Il Fornitore garantirà inoltre che il Personale sia tempestivamente informato degli aggiornamenti alle politiche sulla sicurezza e sulla privacy del Fornitore.

4.7 **Dati di inventario.** Il Fornitore documenterà e conserverà informazioni relative a (a) quali Informazioni di Amazon sta trattando e (b) come e dove tali Informazioni di Amazon vengono trattate (ad es., in un diagramma di architettura aggiornato). Su richiesta di Amazon, il Fornitore comunicherà queste informazioni ad Amazon.

4.8 **Test di sicurezza.**

4.8.1 Il Fornitore eseguirà test annuali per garantire la propria conformità ai requisiti della presente Politica sulla sicurezza.

La traduzione di seguito è fornita solo a scopo informativo. In caso di discrepanze, incongruenze o conflitti tra la presente traduzione e l'ultima versione in lingua inglese aggiornata (anche a causa di ritardi nella traduzione), prevarrà la versione in lingua inglese.

4.8.2 Il Fornitore eseguirà test di penetrazione delle difese di sicurezza del Fornitore almeno una volta all'anno. I test di penetrazione includeranno: (a) test dall'interno e dall'esterno della rete del Fornitore, (b) ingegneria sociale (ad es. simulazioni di phishing) e (c) test di sicurezza per reti wireless. Il Fornitore farà fronte alle vulnerabilità individuate nell'ambito del suo programma di gestione delle vulnerabilità. Su richiesta di Amazon, il Fornitore comunicherà ad Amazon i risultati di tali test di penetrazione e correzione delle vulnerabilità.

4.9 **Sicurezza della rete**. Il Fornitore proteggerà i Sistemi Informatici Interessati limitando l'accesso non autorizzato alla rete, specialmente da reti esterne. Il Fornitore manterrà e configurerà firewall o altri controlli di sicurezza equivalenti per proteggere i sistemi da accessi non autorizzati ed esaminerà i set di regole per i firewall almeno una volta all'anno per garantire che esistano casi aziendali validi e documentati per tutte le regole.

4.10 **Ambiente idoneo**. Il Fornitore tratterà le Informazioni di Amazon solo in un ambiente adatto al suo scopo e non in un ambiente di test, a meno che non sia consentito ai sensi del Contratto.

4.11 **Crittografia**. Il Fornitore crittograferà tutte le Informazioni di Amazon a riposo e in transito su reti esterne in conformità alle migliori pratiche di settore. Se le Informazioni di Amazon vengono trasmesse su reti interne del Fornitore, saranno trasmesse attraverso un protocollo crittografato che soddisfa le migliori pratiche di settore. Il Fornitore gestirà e metterà al sicuro le chiavi di crittografia in conformità alle migliori pratiche di settore.

4.12 **Uso controllato dei privilegi amministrativi**. Il Fornitore gestirà le funzioni amministrative in conformità al Quadro di sicurezza informatica del NIST o ISO 27002. Il Fornitore dovrà quantomeno separare gli account amministrativi dagli account standard e limitare gli account amministrativi alle sole competenze necessarie per svolgere le funzioni amministrative. Il Fornitore registrerà tutte le azioni dell'account amministrativo in modo attribuibile a un singolo utente. Le competenze amministrative conferite a un account standard saranno basate sul privilegio minimo e registrate in modo attribuibile a un singolo utente.

4.13 **Controllo degli accessi.**

4.13.1 **ID univoci**. Il Fornitore assegnerà ID individuali e univoci al Personale avente accesso alle Informazioni di Amazon o ai Sistemi Informatici Interessati, compresi gli account con accesso amministrativo.

4.13.2 **Solo "Necessità di sapere".** Il Fornitore limiterà l'accesso alle Informazioni di Amazon e ai Sistemi Informatici Interessati ai soli membri del Personale aventi "necessità di sapere" per uno Scopo consentito.

4.13.3 **Revisione degli accessi degli utenti**. Il Fornitore, almeno una volta ogni 90 giorni, esaminerà l'elenco dei membri del Personale e dei servizi con accesso alle Informazioni di Amazon e ai Sistemi Informatici Interessati e interromperà l'accesso degli account che non ne hanno più bisogno.

4.13.4 **Single Sign-On (SSO).** Qualsiasi servizio del Fornitore che richieda l'autenticazione del personale Amazon deve integrarsi con un provider di identità Amazon (ad es. Amazon Federate) per fornire tale autenticazione. Tali servizi non devono utilizzare credenziali fornite o gestite dal Fornitore per l'autenticazione.

4.14 **Gestione delle password.**

La traduzione di seguito è fornita solo a scopo informativo. In caso di discrepanze, incongruenze o conflitti tra la presente traduzione e l'ultima versione in lingua inglese aggiornata (anche a causa di ritardi nella traduzione), prevarrà la versione in lingua inglese.

4.14.1 **Password complesse**. Il Fornitore non utilizzerà le impostazioni predefinite fornite dal produttore per le password di sistema e altri parametri di sicurezza su alcun Sistema Informatico Interessato. Il Fornitore imporrà e garantirà l'uso di "password complesse" applicate dal sistema in conformità alle migliori pratiche descritte nella pubblicazione speciale NIST SP 800-63B su tutti i Sistemi Informatici Interessati. Il Fornitore esigerà che tutte le password e le credenziali di accesso siano mantenute riservate e non condivise tra i membri del Personale.

4.14.2 **Blocco.** Il Fornitore manterrà e applicherà il "blocco dell'account" disabilitando gli account aventi accesso alle Informazioni di Amazon o ai Sistemi Informatici Interessati quando un account supera non più di dieci (10) tentativi consecutivi di inserimento di password errate.

4.15 **Accesso remoto; Autenticazione a più fattori**. Il Fornitore implementerà l'autenticazione a più fattori (ovvero, esigendo almeno due fattori per autenticare un utente) per l'accesso remoto a qualsiasi rete, sistema, applicazione o altra risorsa del Fornitore.

4.16 **Accesso "in blocco".** Ai fini della presente sezione, per accesso "in blocco" si intende l'accesso ai dati tramite query di database, creazione di report o qualsiasi altro trasferimento in massa di dati.

4.16.1 Salvo quanto espressamente stabilito nel Contratto o altrimenti da Amazon per iscritto, il Fornitore non accederà, e non consentirà l'accesso, alle Informazioni di Amazon "in blocco" indipendentemente dal fatto che le Informazioni di Amazon si trovino in un database controllato da Amazon o dal Fornitore o siano archiviate utilizzando qualsiasi altro metodo, inclusa la memorizzazione su archivi basati su file (ad es., file flat).

4.16.2 Laddove Amazon autorizzi l'accesso "in blocco", il Fornitore: (a) limiterà tale accesso solo a specifici membri del Personale aventi "necessità di sapere" e (b) richiederà l'autorizzazione esplicita e la registrazione di tale accesso in conformità ai requisiti della Sezione 4.3. Su richiesta di Amazon in coordinamento con le revisioni della sicurezza di cui alla Sezione 10 o gli Incidenti di sicurezza di cui alla Sezione 11, il Fornitore fornirà ad Amazon tutti i registri sull'accesso "in blocco" a cui si fa riferimento in questa sezione.

4.17 **Separazione dei dati**. Il Fornitore separerà, in maniera fisica o logica, le Informazioni di Amazon dalle informazioni del Fornitore e di qualsiasi terza parte in qualsiasi momento. Se non è possibile una separazione, il Fornitore garantirà che le Informazioni di Amazon siano distinguibili da altre informazioni per scopi di registrazione, eliminazione e risposta agli incidenti.

4.18 **Sicurezza del personale del Fornitore**.

4.18.1 Il Fornitore adotterà tutte le precauzioni ragionevoli per garantire che il Personale a cui è concesso l'accesso alle Informazioni di Amazon mantenga la propria riservatezza e le utilizzi solo per uno Scopo consentito. Queste precauzioni devono includere l'imposizione di requisiti di riservatezza mediante un accordo di non divulgazione o una politica del Fornitore.

4.18.2 Per qualsiasi membro del Personale che (a) non abbia più bisogno di accedere alle Informazioni di Amazon o (b) non sia più classificabile come membro del Personale del Fornitore, il Fornitore interromperà l'accesso alle Informazioni di Amazon e ai Sistemi Informatici Interessati entro 24 ore. Se un membro del Personale continua ad avere accesso alle Informazioni di Amazon o ai Sistemi Informatici Interessati per più di 24 ore dopo il verificarsi dei casi (a) o (b), il Fornitore informerà Amazon del protrarsi di tale accesso entro 24 ore dal momento in cui ne viene a conoscenza inviando un'e-mail a security@amazon.com.

La traduzione di seguito è fornita solo a scopo informativo. In caso di discrepanze, incongruenze o conflitti tra la presente traduzione e l'ultima versione in lingua inglese aggiornata (anche a causa di ritardi nella traduzione), prevarrà la versione in lingua inglese.

5. REQUISITI DI SICUREZZA DEI PAGAMENTI. Se il Fornitore ha accesso ai dati dei titolari di carta di pagamento, o li tratterà, il Fornitore si atterrà all'ultima versione dello Standard di sicurezza dei dati del Settore delle carte di pagamento (Payment Card Industry Data Security Standard, PCI DSS).

6. SUBAPPALTATORI.

6.1 Il Fornitore non subappalterà né delegherà alcuno dei propri obblighi ai sensi della presente Politica sulla sicurezza a terzi (collettivamente, "Subappaltatori") senza il previo consenso scritto di Amazon. A prescindere dall'esistenza o dai termini di qualsiasi subappalto o delega, il Fornitore resterà responsabile del pieno adempimento dei propri obblighi ai sensi della presente Politica sulla sicurezza. I termini e le condizioni della presente Politica sulla sicurezza saranno vincolanti per i Subappaltatori del Fornitore e il Personale dei Subappaltatori.

6.2 Se il Fornitore utilizza dei Sistemi Informatici Interessati del Subappaltatore, eseguirà una revisione della sicurezza di tali sistemi e i relativi controlli di sicurezza e, su richiesta di Amazon e nel formato da essa richiesto, le fornirà dei rapporti periodici su tali controlli di sicurezza dei Sistemi Informatici Interessati del Subappaltatore (ad es., Dichiarazione sugli standard per gli Incarichi di attestazione n. 16 (SSAE 16)).

7. ACCESSO AI SISTEMI INFORMATICI GESTITI DA AMAZON. Amazon potrà concedere al Fornitore il diritto di trattare le Informazioni di Amazon tramite portali web o altri siti web o extranet non pubblici (ciascuno, un "Sistema Informatico gestito da Amazon") solo per lo Scopo consentito. Se Amazon consente al Fornitore di trattare le Informazioni di Amazon utilizzando un Sistema Informatico gestito da Amazon, il Fornitore e il suo Personale devono rispettare i seguenti requisiti:

7.1 **Account**. Il Fornitore garantirà che il proprio Personale utilizzi solo lo/gli account del Sistema Informatico gestito da Amazon che Amazon ha designato per ogni individuo e richiederà al Personale del Fornitore di mantenerne riservate le credenziali di accesso e di non condividerle.

7.2 **Sistemi**. Il Fornitore e il suo Personale utilizzeranno i Sistemi informatici gestiti da Amazon solo attraverso sistemi o applicazioni di computazione o trattamento (a) eseguiti su sistemi operativi gestiti dal Fornitore e che utilizzano la crittografia completa del disco e (b) che soddisfano i requisiti di cui alle Sezioni 4.2 (Gestione delle patch), 4.4 (Difese malware) e 4.9 (Sicurezza della rete).

7.3 **Restrizioni**. Salvo previa approvazione scritta da parte di Amazon, il Fornitore e il suo Personale si asterranno dall'effettuare il download, il mirroring o dal conservare in modo permanente Informazioni di Amazon da qualsiasi Sistema Informatico gestito da Amazon su qualsiasi supporto.

7.4 **Interruzione dell'account**. Per qualsiasi membro del Personale che (a) non abbia più necessità di accedere al Sistema Informatico gestito da Amazon o (b) non sia più classificabile come Personale del Fornitore (ad es., la persona lascia il posto di lavoro presso il Fornitore), il Fornitore dovrà immediatamente (entro un massimo di 24 ore) interrompere l'accesso di tale membro del Personale al Sistema Informatico gestito da Amazon o avvisare Amazon di interrompere tale accesso.

8. DOMINI O URL AMAZON. Qualsiasi dominio o URL che il Fornitore rende disponibile ad uso esclusivo di Amazon non deve essere rilasciato dal Fornitore a terze parti, o riutilizzato da queste, per almeno 5 anni dopo la risoluzione del Contratto.

9. RESTITUZIONE ED ELIMINAZIONE DEI DATI; DISTRUZIONE FORENSE DEI SUPPORTI.

La traduzione di seguito è fornita solo a scopo informativo. In caso di discrepanze, incongruenze o conflitti tra la presente traduzione e l'ultima versione in lingua inglese aggiornata (anche a causa di ritardi nella traduzione), prevarrà la versione in lingua inglese.

9.1 **Restituzione ed eliminazione dei dati**. Su richiesta di Amazon, il Fornitore restituirà tempestivamente (e comunque entro e non oltre le 72 ore successive) ad Amazon, ed eliminerà in modo permanente e sicuro, tutte le Informazioni di Amazon in conformità all'avviso di Amazon indicante l'obbligo di restituzione e/o eliminazione. Il Fornitore eliminerà inoltre in modo permanente e sicuro tutte le istanze in tempo reale (online o accessibili in rete) delle Informazioni di Amazon entro 30 giorni dal perseguimento dello Scopo consentito o dalla risoluzione o scadenza del Contratto, a seconda di quale evento si verifichi per primo. Se richiesto da Amazon, il Fornitore certificherà per iscritto l'avvenuta eliminazione di tutte le Informazioni di Amazon. Per chiarezza, questa sezione non si applica alle Copie di archivio ai sensi della Sezione 9.3.

9.2 Sanificazione dei dati. Tutte le Informazioni di Amazon eliminate dal Fornitore saranno eliminate in conformità alle Raccomandazioni minime di sanificazione contenute nella NIST SP 800-88 Revisione 1, Linee guida per la sanificazione dei supporti (18 dicembre 2014, Appendice A) per la pulizia del tipo di dispositivo pertinente. In assenza di indicazioni nella NIST SP 800-88 per il tipo di dispositivo pertinente, il Fornitore distruggerà il dispositivo contenente le Informazioni di Amazon in uno dei seguenti modi: (a) eliminazione secondo le direttive della NIST SP 800-88, (b) distruzione secondo le direttive della NIST SP 800-88, o (c) mediante tali altri standard che Amazon potrà richiedere in base alla classificazione e alla sensibilità delle Informazioni di Amazon.

9.3 Copie di archivio. Se il Fornitore è tenuto per legge a conservare Copie di archivio delle Informazioni di Amazon, il Fornitore non utilizzerà le Informazioni di Amazon archiviate per alcun altro scopo e rimarrà vincolato da tutti i suoi obblighi ai sensi della presente Politica sulla sicurezza. Qualsiasi Informazione di Amazon archiviata deve essere crittografata e archiviata laddove il Sistema Informatico Interessato che ospita o memorizza le Informazioni di Amazon crittografate non abbia accesso a una copia della/e chiave/i utilizzata/e per la crittografia. Qualsiasi backup offline o "a freddo" (ovvero, non disponibile per l'uso immediato o interattivo) deve essere conservato in una struttura fisicamente sicura.

9.4 **Distruzione forense dei supporti**. Prima di smaltire qualsiasi hardware, software o altro supporto che contenga, o abbia contenuto in qualsiasi momento, le Informazioni di Amazon, il Fornitore eseguirà una distruzione forense completa dell'hardware, del software o di altri supporti in conformità alla NIST SP 800-88, Appendice A. Questo obbligo di distruzione non si applicherà ai supporti di archiviazione a cui il Fornitore non abbia accesso fisico o di cui non abbia il controllo. In tali casi, il Fornitore garantirà che le Informazioni di Amazon, ove non più necessarie, siano eliminate in modo sicuro seguendo le migliori pratiche di settore.

> 9.4.1 A meno che il Fornitore non riceva il previo consenso scritto esplicito di Amazon, non venderà, rivenderà, donerà, ricondizionerà né altrimenti trasferirà alcun hardware, software o altro supporto che abbia in qualsiasi momento contenuto le Informazioni di Amazon, a meno che non sia stato distrutto dal punto di vista forense in conformità alla presente Sezione.

10. **REVISIONI DI SICUREZZA**. Su richiesta di Amazon, il Fornitore dovrà: (a) completare una valutazione del rischio di Amazon, (b) fornire prove richieste da Amazon per convalidare la conformità del Fornitore alla presente Politica sulla sicurezza, (c) consentire ad Amazon o a una terza parte nominata per suo conto di eseguire una revisione della conformità del Fornitore alla presente Politica sulla sicurezza, e/o (d) fornire ad Amazon tutti i registri a cui si fa riferimento nella Sezione 4.3 nel formato Open Cybersecurity Schema Framework (OCSF). Se il Fornitore richiede che qualsiasi prova sia esaminata di persona o mediante un'ispezione in loco piuttosto che fornire tali prove perché Amazon le esamini da remoto, il Fornitore si farà carico delle spese di viaggio e

altre spese relative a tale ispezione in loco. Se una valutazione o revisione indica dei risultati, il Fornitore, interamente a proprie spese, prenderà tempestivamente tutte le ragionevoli misure necessarie a correggere tali risultati, con ragionevole soddisfazione di Amazon ed entro un periodo di tempo concordato.

11. **INCIDENTI DI SICUREZZA.**

11.1 **Avviso di incidente di sicurezza**. Il Fornitore informerà Amazon il prima possibile, ma non oltre 24 ore dopo aver scoperto o ragionevolmente sospettato il verificarsi di un evento non autorizzato di accesso, raccolta, acquisizione, uso, trasmissione, divulgazione, corruzione o perdita delle Informazioni di Amazon o di un Sistema Informatico Interessato (un "Incidente di sicurezza"). Il Fornitore invierà gli avvisi di Incidenti di sicurezza a security@amazon.com.

11.2 **Piano di risposta agli incidenti**. Il Fornitore manterrà un piano scritto di risposta agli incidenti e, su richiesta, ne fornirà una copia ad Amazon. Il Fornitore porrà rimedio a ciascun Incidente di sicurezza in modo tempestivo seguendo l'apposito piano scritto di risposta del Fornitore e le migliori pratiche di settore. Il Fornitore esaminerà, testerà e (se necessario) aggiornerà il piano almeno una volta all'anno.

11.3 **Collaborazione con Amazon**. Il Fornitore (a) coadiuverà l'indagine di Amazon sull'Incidente di sicurezza; (b) agevolerà dei colloqui con il Personale e altre persone coinvolte nell'Incidente di sicurezza o nella risposta allo stesso; (c) conserverà i dettagli scritti dell'indagine e della risposta all'Incidente di sicurezza del Fornitore; e (d) metterà a disposizione di Amazon tutti i documenti, registri, file, rapporti sui dati, relazioni forensi, relazioni d'indagine e altri materiali pertinenti richiesti da Amazon.

11.4 **Avvisi di terzi**. Salvo diversamente richiesto dalla legge, il Fornitore otterrà il previo consenso scritto di Amazon prima di: (a) informare qualsiasi terza parte (inclusa qualsiasi autorità regolatoria o cliente) di un Incidente di sicurezza; o (b) indicare Amazon in qualsiasi notifica o dichiarazione pubblica relativa a qualsiasi Incidente di sicurezza. Salvo diversamente previsto per legge, Amazon avrà il diritto di determinare se occorre fornire a terze parti un avviso di un Incidente di sicurezza e la forma, le tempistiche e il contenuto di tale avviso.

12. **AVVISO DI PROCEDIMENTO LEGALE**. Avviso di procedimento legale. Salvo laddove vietato per legge, se le Informazioni di Amazon vengono richieste in risposta a un procedimento legale o altra legge applicabile, il Fornitore fornirà ad Amazon un preavviso sufficiente a consentirle di richiedere un ordine restrittivo o altro provvedimento adeguato.

13. **DEFINIZIONI**.

13.1 "**Accordo**" indica qualsiasi accordo che faccia riferimento alla presente Politica sulla sicurezza.

13.2 "**Amazon**" indica Amazon.com, Inc. e le sue affiliate.

13.3 "**Informazioni di Amazon**" indica: (a) tutte le Informazioni riservate di Amazon (come definite in qualsiasi altro accordo tra le parti); (b) tutti i dati, i registri, i file, i contenuti o le informazioni, in qualsiasi forma, acquisite, consultate, raccolte, ricevute, archiviate o mantenute dal Fornitore o dalle sue affiliate, da o per conto di Amazon, o altrimenti in relazione al Contratto; e (c) le informazioni derivate da (a) o (b), anche se anonimizzate.

13.4 "**Anonimizzare**" significa trattare qualsiasi dato o informazione (comprese le Informazioni di Amazon) in un modo o forma che non identifichi, consenta di identificare e non sia altrimenti

La traduzione di seguito è fornita solo a scopo informativo. In caso di discrepanze, incongruenze o conflitti tra la presente traduzione e l'ultima versione in lingua inglese aggiornata (anche a causa di ritardi nella traduzione), prevarrà la versione in lingua inglese.

attribuibile ad Amazon, o a qualsiasi utente, identificatore del dispositivo, fonte, prodotto, servizio, contesto o marchio dello stesso.

13.5 "**Sistemi Informatici Interessati**" indica qualsiasi sistema utilizzato dal Fornitore per trattare le Informazioni di Amazon.

13.6 "**Personale**" indica i dipendenti, gli agenti, i subappaltatori e altri utenti autorizzati del Fornitore o del Subappaltatore dei suoi sistemi e risorse di rete.

13.7 "**Trattamento**" indica l'esecuzione di qualsiasi operazione sui dati, come l'accesso, l'uso, la raccolta, la ricezione, la conservazione, l'alterazione, la trasmissione, la diffusione o altra messa a disposizione, cancellazione o distruzione.

13.8 "**Fornitore**" indica ciascun fornitore, venditore o appaltatore definito in un Contratto e qualsiasi altro fornitore che sia vincolato a un Contratto.