

Requisiti di sicurezza delle informazioni

1. Introduzione

Il Fornitore e CWT hanno stipulato un accordo in base al quale il Fornitore ha accettato di fornire servizi e/o prodotti secondo i termini di tale accordo (" **Accordo** "). Il Fornitore si impegna a rispettare e far sì che le Terze Parti che agiscono per suo conto rispettino i requisiti di sicurezza delle informazioni contenuti nel presente documento (" **Requisiti di sicurezza delle informazioni** ") e le misure di sicurezza delle informazioni richieste (" **Misure di sicurezza tecniche e organizzative** "). I requisiti di sicurezza delle informazioni e le misure di sicurezza tecniche e organizzative sono incorporati e fanno parte dell'accordo.

2. Definizioni

- 2.1 Salvo quanto diversamente stabilito o ampliato nel presente documento, i termini definiti avranno lo stesso significato stabilito nell'Accordo. I seguenti termini definiti si applicano a questi Requisiti di sicurezza delle informazioni . In caso di conflitto tra la definizione contenuta nell'Accordo e quelle ivi contenute, la definizione contenuta nel presente documento prevarrà per quanto riguarda i Requisiti di sicurezza delle informazioni.

Per "**Affiliate**", salvo diversa definizione nel Contratto, si intende, con riferimento a una parte, qualsiasi società o altra entità giuridica che direttamente o indirettamente: (i) controlla una parte; o (ii) è controllata da una parte; o (iii) è controllata da una società o entità che controlla direttamente o indirettamente una parte. A tal fine, per "controllo" si intende il diritto di esercitare più del cinquanta per cento (50%) dei diritti di voto o diritti analoghi di proprietà; ma solo finché tale controllo continuerà ad esistere.

"**Dipendente autorizzato**" indica i dipendenti del Venditore che hanno la necessità di conoscere o accedere in altro modo alle Informazioni riservate e alle Informazioni personali per consentire al Venditore di adempiere ai propri obblighi ai sensi del Contratto.

"**Parte Autorizzata**" o "**Parti Autorizzate**" indica i (i) Dipendenti Autorizzati del Venditore ; e (ii) Terze parti che hanno la necessità di conoscere o accedere in altro modo alle Informazioni personali e alle Informazioni riservate per consentire al Venditore di adempiere ai propri obblighi ai sensi dell'Accordo e che sono vincolate per iscritto dalla riservatezza e da altri obblighi sufficienti a proteggere le Informazioni personali e le Informazioni riservate in conformità con i termini e le condizioni dell'Accordo e del presente documento.

"**Informazioni riservate**" indica qualsiasi informazione commercialmente sensibile, proprietaria o altrimenti riservata relativa a (a) CWT, i suoi partner e le sue affiliate; (b) un cliente CWT e dipendenti, appaltatori, subappaltatori o fornitori del cliente CWT; (c) personale CWT; (d) i suoi partner indipendenti e joint venture; o (e) il contenuto e/o lo scopo del Contratto, sia orale, scritto o che con qualsiasi altro mezzo possa entrare direttamente o indirettamente in possesso del Venditore o in possesso di Soggetti Autorizzati a seguito di o in connessione con il Accordo. A scanso di equivoci, tutti i prodotti del lavoro costituiscono informazioni riservate.

"**CWT**" se non diversamente definito nell'Accordo, indica l'entità CWT indicata nell'Accordo e le sue Affiliate.

"**Zona demilitarizzata**" o "**DMZ**" è una rete o una sottorete che si trova tra una rete interna attendibile, come una LAN (Local Area Network) aziendale privata, e una rete esterna non attendibile, come Internet pubblica. Una DMZ aiuta a impedire agli utenti esterni di ottenere l'accesso diretto ai sistemi interni e ad altre risorse.

"**Processo di gestione dell'incidente**" è un processo e una procedura documentati sviluppati dal fornitore da seguire in caso di attacco effettivo o sospetto, intrusione, accesso non autorizzato, perdita o altra violazione che coinvolga la riservatezza, la disponibilità o l'integrità delle Informazioni Personali e delle Informazioni Riservate di CWT.

"**mascheramento**" è il processo di copertura delle informazioni visualizzate su uno schermo.

Per "**Dispositivi mobili e portatili**" si intendono computer, dispositivi, supporti e sistemi mobili e/o portatili che possono essere facilmente trasportati, spostati, trasportati o trasportati utilizzati in relazione al Contratto. Esempi di tali dispositivi includono computer portatili, tablet, dischi rigidi USB, memory stick USB, PDA (Personal Digital Assistant), telefoni cellulari o dati e qualsiasi altro dispositivo wireless, periferico o rimovibile con la capacità di archiviare informazioni riservate e informazioni personali .

"**Informazioni personali**" se non diversamente definito nell'Accordo si intende, come definito dal Regolamento (UE) 2016/679 e da altre leggi globali applicabili in materia di sicurezza delle informazioni, protezione dei dati e privacy, qualsiasi informazione relativa a una persona fisica identificata o identificabile, che può essere identificato direttamente o indirettamente, in particolare mediante riferimento a un numero di identificazione oa uno o più elementi propri della sua identità fisica, fisiologica, psichica, economica, culturale o sociale. Le informazioni personali sono di proprietà di CWT, non del venditore.

"**Gateway di sicurezza**" indica un insieme di meccanismi di controllo tra due o più reti aventi diversi livelli di attendibilità che filtrano e registrano il traffico che passa, o tenta di passare, tra le reti e i server amministrativi e di gestione associati. Esempi di gateway di sicurezza includono firewall, server di gestione del firewall, hop box, controller di confine di sessione, server proxy e dispositivi di prevenzione delle intrusioni.

"**Autenticazione forte**" indica l'uso di meccanismi di autenticazione e metodologie di autenticazione che richiedono molteplici fattori di autenticazione, inclusi almeno due dei seguenti: (1) Conoscenza: qualcosa che l'utente conosce, ad esempio password o numero di identificazione personale, (2) Proprietà: qualcosa l'utente ha, ad esempio, token, smart card, telefono cellulare e (3) Inherence - qualcosa che l'utente è, ad esempio l'impronta digitale.

"**Crittografia forte**" indica l'uso di tecnologie di crittografia con lunghezze di chiave minime di 256 bit per la crittografia simmetrica e 1024 bit per la crittografia asimmetrica la cui forza fornisce una ragionevole garanzia di proteggere le informazioni crittografate da accessi non autorizzati ed è adeguata a proteggere la riservatezza e privacy delle informazioni

crittografate e che incorpora una politica documentata per la gestione delle chiavi di crittografia e dei processi associati adeguata a proteggere la riservatezza e la privacy delle chiavi e delle password utilizzate come input per l'algoritmo di crittografia. Strong Encryption include, ma non è limitato a: SSL v3.0+/TLS v1.2, Point to Point Tunneling Protocol (PPTP), AES 256, FIPS 140-2 (solo governo degli Stati Uniti), RSA 1024 bit, SHA1/SHA2 /SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4 o WPA2.

"Misure di sicurezza tecniche e organizzative" indica qualsiasi attività richiesta ai sensi dei presenti Requisiti di sicurezza delle informazioni per accedere, gestire, trasferire, elaborare, archiviare, conservare e distruggere informazioni o dati; per divulgare e notificare le parti interessate richieste dall'Accordo e dalle leggi sulla privacy delle informazioni e sulla protezione dei dati applicabili; e per salvaguardare informazioni o dati per garantire disponibilità, integrità, riservatezza e privacy, o notificare agli individui qualsiasi mancata salvaguardia di tali informazioni o dati. Le misure includono, a titolo esemplificativo ma non esaustivo, quelle richieste o interpretate come obbligatorie ai sensi del Regolamento generale sulla protezione dei dati dell'UE (GDPR), della Direttiva sui servizi di pagamento dell'UE, del California Consumer Privacy Act, del NYS DFS 23 NYCRR 500 , del Gramm-Leach Bliley Act degli Stati Uniti (GLBA), lo United States Health Insurance Portability and Accountability Act (HIPAA), i requisiti sulla privacy dei dati UE/Svizzera e qualsiasi altra legge internazionale e statunitense, interpretazioni legali ufficiali o precedenti di casi relativi a informazioni o dati ai sensi dell'accordo .

"Terze parti" o **"Terze parti"** significa del venditore consulenti di subappaltatori , personale temporaneo, appaltatori o altri fornitori e/o agenti che agiscono per conto del Fornitore e include qualsiasi definizione di Terza parte ai sensi del diritto UE, statunitense o internazionale applicabile.

"Venditore" indica l'ente appaltante stabilito nell'Accordo insieme alle sue Affiliate e alle sue Terze Parti.

3 . Organizzazione per la sicurezza delle informazioni

Il venditore deve, come minimo:

- 3.1 Garantire che solo le parti autorizzate abbiano accesso alle informazioni personali e riservate.
- 3.2 Implementare misure di sicurezza tecniche e organizzative che non siano meno rigorose delle migliori pratiche di sicurezza delle informazioni per proteggere l'integrità, la disponibilità e la riservatezza delle informazioni riservate, delle informazioni personali e di altre informazioni non pubbliche e prevenire l'accesso, l'acquisizione, la divulgazione, la distruzione, l'alterazione non autorizzati , perdita accidentale, uso improprio o danneggiamento delle Informazioni personali o delle Informazioni riservate.
- 3.3 Stabilire, implementare e mantenere la coerenza con le migliori pratiche del settore , le politiche e un programma di misure di sicurezza organizzative, operative, amministrative, fisiche e tecniche e organizzative appropriate per (1) impedire qualsiasi accesso da parte di

parti non autorizzate alle informazioni personali e riservate in un modo non autorizzato dall'Accordo o dai presenti Requisiti di sicurezza delle informazioni e (2) rispettare e soddisfare tutte le leggi e i regolamenti applicabili e gli standard di settore applicabili.

- 3.4 Fornire alle parti autorizzate che avranno accesso alle Informazioni personali e alle Informazioni riservate supervisione, orientamento e formazione sulle misure di sicurezza tecniche e organizzative, inclusa la formazione che fornisce esercitazioni pratiche in linea con gli attuali scenari di minaccia e fornisce feedback a coloro che seguono la formazione . Il Fornitore dovrà fornire formazione tecnica e organizzativa sulle misure di sicurezza al momento dell'assunzione di un dipendente autorizzato e prima dell'accesso di una parte autorizzata alle informazioni riservate e alle informazioni personali. La formazione di aggiornamento deve essere fornita almeno una volta all'anno e il prima possibile a seguito di qualsiasi modifica sostanziale delle misure di sicurezza tecniche e organizzative del fornitore.
- 3.5 Fornire formazione specializzata specifica per le Parti Autorizzate con importanti compiti di sicurezza, incluse, a titolo esemplificativo ma non esaustivo, le risorse umane o le funzioni di tecnologia dell'informazione e qualsiasi funzione di amministratore della tecnologia. Come minimo, la formazione specializzata comprende, ove applicabile al ruolo, le procedure di sicurezza delle informazioni, l'uso accettabile delle risorse di sicurezza delle informazioni, le attuali minacce ai sistemi informativi, le caratteristiche di sicurezza di sistemi specifici e le procedure di accesso sicuro.
- 3.6 Adottare misure ragionevoli per prevenire l'accesso non autorizzato o la perdita di informazioni personali e informazioni riservate e dei servizi, sistemi, dispositivi o supporti contenenti tali informazioni.
- 3.7 Impiegare processi e procedure di valutazione del rischio per valutare regolarmente i sistemi utilizzati per fornire servizi o prodotti a CWT. Il Fornitore dovrà porre rimedio a tali rischi non appena ragionevolmente possibile e commisurato al livello di rischio per le Informazioni personali e le Informazioni riservate date le minacce note al momento dell'identificazione. Attivare un processo per consentire la segnalazione di rischi o incidenti sospetti al team di sicurezza del fornitore.
- 3.8 Nella misura in cui il Fornitore svolga servizi ai sensi dell'Accordo in strutture CWT o utilizzando servizi, sistemi, dispositivi o supporti di proprietà, gestiti o gestiti da CWT, il Fornitore farà in modo che tutte le Parti autorizzate rispettino tutte le politiche CWT messe a disposizione del Fornitore , a sua discrezione richiesta, applicabili a tale accesso. Il Fornitore notificherà tempestivamente a CWT per iscritto quando una Parte autorizzata non ha più bisogno dell'accesso alle Informazioni personali o alle Informazioni riservate affinché il Fornitore possa fornire prodotti o servizi a CWT , incluso, a titolo esemplificativo , quando una

Parte autorizzata viene rescissa o altrimenti non presta più prestazioni servizi previsti dall'Accordo.

- 3.9 Conserva i registri delle parti autorizzate e delle risorse del fornitore che accedono, trasferiscono, conservano, archiviano o elaborano le informazioni personali e le informazioni riservate.
- 3.10 Condurre controlli completi in background su tutte le parti autorizzate prima dell'assunzione, nella misura consentita dalla legge . Il controllo completo dei precedenti delle persone deve includere , come minimo, la precedente storia lavorativa, la fedina penale, la storia creditizia, i controlli di riferimento e qualsiasi altro requisito di controllo dei precedenti standard del settore.
- 3.11 Avere uno o più personale qualificato designato con la responsabilità di mantenere il proprio programma di sicurezza delle informazioni e deve riferire sul proprio programma di sicurezza delle informazioni almeno una volta all'anno al consiglio di amministrazione del venditore o all'organo di governo equivalente. Il venditore deve garantire che il proprio personale di sicurezza abbia un'esperienza e una formazione ragionevoli e necessarie in materia di sicurezza delle informazioni, compreso il mantenimento delle conoscenze sulle mutevoli minacce e contromisure. Su richiesta, il Fornitore fornirà a CWT un punto di contatto per tutti gli elementi relativi alla sicurezza delle informazioni.
- 3.12 Richiedere impegni contrattuali di non divulgazione o riservatezza da parte delle Parti autorizzate prima di fornire loro l'accesso alle Informazioni personali e alle Informazioni riservate.
- 3.13 Garantire che tutte le Parti autorizzate che potrebbero svolgere lavori ai sensi dell'Accordo o che potrebbero avere accesso a Informazioni personali o Informazioni riservate siano conformi a queste Misure di sicurezza tecniche e organizzative che devono essere comprovate da un accordo scritto non meno restrittivo di questi Requisiti di sicurezza delle informazioni .

4. Sicurezza fisica e ambientale

Il venditore deve, come minimo:

- 4.1 Assicurarsi che tutti i sistemi del fornitore e le altre risorse destinate all'uso da parte di più utenti si trovino in strutture fisiche sicure con accesso limitato e limitato alle sole persone autorizzate.
- 4.2 Monitorare e registrare, a fini di audit, l'accesso alle strutture fisiche contenenti sistemi e altre risorse destinate all'uso da parte di più utenti utilizzati in relazione all'adempimento da parte del Fornitore dei propri obblighi ai sensi del Contratto.
- 4.3 Richiedere a tutte le parti autorizzate di rispettare una politica di pulizia della scrivania e di bloccare gli schermi delle workstation prima di lasciare le aree di lavoro.

- 4.4 Raccogliere tutti i beni aziendali in caso di cessazione del rapporto di lavoro o risoluzione del contratto.
- 4.5 Limitare e monitorare l'accesso fisico alle proprie strutture secondo i seguenti requisiti:
- a. L'accesso dei visitatori viene registrato, che viene mantenuto per tre (3) mesi, inclusi il nome del visitatore, l'azienda che rappresenta e il nome del dipendente che autorizza l'accesso fisico. I visitatori devono essere sempre scortati da un dipendente del venditore .
 - b. L'accesso è limitato al personale appropriato, in base alla necessità di sapere.
 - c. Tutti i dipendenti devono indossare un badge identificativo fornito dall'azienda e tutti i visitatori o Terze parti devono indossare un badge ospite/visitatore fornito dall'azienda.
 - d. L'accesso viene revocato immediatamente alla cessazione del personale del Venditore o di Terze parti e tutti i meccanismi di accesso fisico, come chiavi, tessere di accesso, ecc., vengono restituiti o disabilitati.
 - e. Il data center o la sala computer sono chiusi e l'accesso è limitato solo a coloro che hanno bisogno dell'accesso per svolgere le proprie mansioni lavorative.
 - f. Ove consentito dalla legge, utilizzare videocamere per monitorare l'accesso fisico individuale alle aree sensibili e rivedere regolarmente tali dati. Le riprese video devono essere archiviate per un minimo di tre (3) mesi.
 - g. Le apparecchiature utilizzate per archiviare, elaborare o trasmettere informazioni personali e informazioni riservate devono essere protette fisicamente, inclusi punti di accesso wireless, gateway, dispositivi palmari, hardware di rete/di comunicazione e linee di telecomunicazione.
- 4.6 Implementare controlli per ridurre al minimo il rischio e proteggersi dalle minacce fisiche.
- 4.7 Mantenere tutte le risorse hardware che elaborano o gestiscono le informazioni personali e riservate in conformità con i requisiti di assistenza consigliati dal produttore .
- 4.8 reti e jack di rete accessibili al pubblico logicamente e fisicamente dalla rete interna del fornitore e limitato solo agli utenti autenticati o disabilitati per impostazione predefinita.
- 4.9 Proteggere qualsiasi dispositivo che acquisisce i dati delle carte di pagamento tramite interazione fisica diretta da manomissioni e sostituzioni ispezionando periodicamente le superfici del dispositivo per rilevare manomissioni o sostituzioni; fornire formazione al personale per essere a conoscenza di tentativi di manomissione o sostituzione dei dispositivi.
- 4.10 Controllare e separare i punti di accesso come le aree di consegna e carico e altri punti da tutti i centri che accedono, gestiscono, archiviano o elaborano le Informazioni personali e le Informazioni riservate.
- 4.11 Assicurati che i data center dei fornitori dispongano di dispositivi di riscaldamento, raffreddamento, soppressione incendi, rilevamento dell'acqua e rilevamento di calore/fumo. I data center dei fornitori e le sale computer devono essere privi di materiale combustibile (es . scatole, carta, ecc.) o conservati in armadi metallici.

5. **Controllo degli accessi**

Il venditore deve, come minimo:

- 5.1 Adottare tutte le misure ragionevoli per impedire a soggetti diversi dalle Parti autorizzate di accedere alle Informazioni personali e alle Informazioni riservate in qualsiasi modo o per qualsiasi scopo non autorizzato da CWT e dal Contratto.
- 5.2 Separare le informazioni di CWT dai dati di altri clienti del fornitore o dalle applicazioni e informazioni del fornitore utilizzando server fisicamente separati o utilizzando controlli di accesso logici in cui la separazione fisica dei server non è implementata.
- 5.3 Identificare e richiedere ai proprietari appropriati di rivedere e approvare l'accesso ai sistemi utilizzati per accedere, elaborare, gestire o archiviare informazioni personali e informazioni riservate almeno trimestralmente per rimuovere l'accesso non autorizzato ; e mantenere e tenere traccia delle approvazioni di accesso.
- 5.4 Rimuovere l'accesso ai sistemi di gestione delle Informazioni Personali e delle Informazioni Riservate entro 24 ore dalla cessazione del rapporto da parte della Parte Autorizzata con il Venditore; e mantenere procedure ragionevoli per rimuovere l'accesso a tali sistemi entro tre giorni lavorativi quando non è più necessario o rilevante per lo svolgimento delle loro funzioni . Tutti gli altri ID utente devono essere disabilitati o rimossi dopo 90 giorni di calendario di inattività.
- 5.5 Limitare l'accesso dell'amministratore di sistema (noto anche come root, privilegiato o superutente) ai sistemi operativi destinati all'uso da parte di più utenti solo a persone che richiedono un accesso di tale livello nell'esecuzione del proprio lavoro. Utilizza gli ID dell'amministratore del sistema di check-out con le credenziali di accesso dei singoli utenti e i registri delle attività per gestire l'accesso ad alta sicurezza e ridurre l'accesso ad alto livello a un numero estremamente limitato di utenti. Richiedere agli amministratori di applicazioni, database, rete e sistema di limitare l'accesso degli utenti ai soli comandi, dati, sistemi e altre risorse necessarie per eseguire le funzioni autorizzate. I ruoli amministrativi del sistema e gli elenchi di accesso devono essere rivisti almeno una volta all'anno.
- 5.6 Applicare la regola del privilegio minimo (vale a dire , limitare l'accesso ai soli comandi, informazioni, sistemi e altre risorse, necessari per svolgere le funzioni autorizzate in base alla propria funzione lavorativa).
- 5.7 Richiede l'autenticazione avanzata per tutti gli accessi amministrativi non da console , qualsiasi accesso remoto e tutti gli accessi amministrativi negli ambienti cloud .
- 5.8 Proibire e utilizzare misure di sicurezza tecniche e organizzative per garantire che le informazioni personali non possano copiare, spostare o archiviare informazioni personali su dischi rigidi locali o tagliare e incollare o stampare informazioni personali.

- 5.9 Attivare l'uso delle funzionalità di accesso remoto solo quando necessario, monitorare durante l'uso e disattivare immediatamente dopo l'uso.
- 5.10 Richiede un'autenticazione forte per connettersi alle risorse interne del fornitore contenenti informazioni personali e informazioni riservate.

6. Identificazione e autenticazione

Il venditore deve, come minimo:

- 6.1 Assegna ID utente univoci a singoli utenti e assegna meccanismi di autenticazione a ciascun singolo account.
- 6.2 Utilizzare un processo documentato di gestione del ciclo di vita dell'ID utente che includa, a titolo esemplificativo, procedure per la creazione di account approvati, la rimozione tempestiva dell'account e la modifica dell'account (ad es. modifiche ai privilegi, intervallo di accesso, funzioni/ruoli) per tutti gli accessi alle informazioni personali e Informazioni riservate e in tutti gli ambienti (ad es. produzione, test, sviluppo, ecc.). Tale processo deve includere la revisione dei privilegi di accesso e della validità dell'account da eseguire con cadenza almeno trimestrale.
- 6.3 Limita l'accesso alle informazioni personali e riservate a coloro che utilizzano un ID utente e una password validi e richiedono che gli ID utente univoci utilizzino uno dei seguenti: password o passphrase, autenticazione a due fattori o un valore biometrico.
- 6.4 Richiede la complessità della password e soddisfa i seguenti requisiti di costruzione della password: una lunghezza minima di dodici (12) caratteri per le password di sistema e quattro (4) caratteri per i codici di accesso di tablet e smartphone. Le password di sistema devono contenere tre (3) dei seguenti caratteri: maiuscolo, minuscolo, numerico o caratteri speciali. Le password inoltre non devono essere uguali all'ID utente a cui sono associate, contenere una parola del dizionario, numeri sequenziali o ripetuti e non essere una delle ultime 24 password. Richiedi la scadenza della password a intervalli regolari per non superare i novanta (90) giorni. Maschera tutte le password quando visualizzate.
- 6.5 Limita i tentativi di accesso non riusciti a non più di cinque (5) tentativi di accesso non riusciti entro 24 ore e blocca l'account utente al raggiungimento di tale limite in uno stato persistente. L'accesso all'account utente può essere riattivato successivamente attraverso un processo manuale che richiede la verifica dell'identità dell'utente.
- 6.6 Verifica l'identità dell'utente e imposta l'utilizzo una tantum e reimposta le password su un valore univoco per ogni utente. Cambio rapido sistematico dopo il primo utilizzo.
- 6.7 Utilizzare un metodo sicuro per la trasmissione di credenziali di autenticazione (ad es. password) e meccanismi di autenticazione (ad es. token o smart card).

- 6.8 Limita le password dell'account di servizio e del proxy a un minimo di 20 caratteri , inclusi caratteri maiuscoli, minuscoli e numerici, nonché simboli speciali. Modificare l'account di servizio e le password proxy almeno una volta all'anno e dopo la cessazione del rapporto di lavoro di chiunque sia a conoscenza della password.
- 6.9 Termina le sessioni interattive o attiva uno screensaver di blocco sicuro che richiede l'autenticazione, dopo un periodo di inattività non superiore a quindici (15) minuti.
- 6.10 Utilizzare un metodo di autenticazione basato sulla sensibilità delle Informazioni personali e delle Informazioni riservate. Ogni volta che le credenziali di autenticazione vengono archiviate, il Fornitore le proteggerà mediante Strong Encryption.
- 6.11 Configurare i sistemi per il timeout automatico dopo un periodo massimo di inattività come segue : server (15 minuti), workstation (15 minuti), dispositivo mobile (4 ore), Dynamic Host Configuration Protocol (7 giorni), Virtual Private Network (24 ore).

7. Acquisizione, Sviluppo e Manutenzione di Sistemi Informativi

Il venditore deve, come minimo:

- 7.1 Visualizzare un banner di avviso sulle schermate o sulle pagine di accesso come specificato per iscritto da CWT per prodotti o servizi a marchio CWT o per prodotti e software sviluppati per CWT.
- 7.2 Restituire tutti i dispositivi di accesso di proprietà o forniti da CWT non appena possibile, ma in ogni caso non oltre quindici (15) giorni dopo il primo tra:
 - a. scadenza o risoluzione del Contratto;
 - b. la richiesta di CWT per la restituzione di tale proprietà; o
 - c. la data in cui il Venditore non ha più bisogno di tali dispositivi.
- 7.3 Impiegare un'efficace metodologia di gestione delle applicazioni che incorpori le misure di sicurezza tecniche e organizzative nel processo di sviluppo del software e garantire che le misure di sicurezza tecniche e organizzative, rappresentate dalle migliori pratiche del settore, siano implementate dal fornitore in modo tempestivo.
- 7.4 Seguire le procedure di sviluppo standard del settore , inclusa la separazione dell'accesso e del codice tra gli ambienti non di produzione e quelli di produzione e la relativa separazione dei compiti tra tali ambienti.
- 7.5 Garantire che i controlli interni sulla sicurezza delle informazioni per lo sviluppo del software siano valutati regolarmente e riflettano le migliori pratiche del settore, nonché rivedere e implementare tali controlli in modo tempestivo.

- 7.6 Gestisci la sicurezza del processo di sviluppo e assicurati che vengano implementate e seguite pratiche di codifica sicure, inclusi controlli crittografici appropriati, protezioni contro codici dannosi e un processo di revisione tra pari.
- 7.7 Condurre test di penetrazione su applicazioni funzionalmente complete prima del rilascio in produzione e successivamente, almeno una volta all'anno e dopo qualsiasi modifica significativa al codice sorgente o alla configurazione in linea con OWASP, CERT, SANS Top 25 e PCI-DSS. Correggere eventuali vulnerabilità sfruttabili prima della distribuzione nell'ambiente di produzione.
- 7.8 Utilizzare dati resi anonimi o offuscati in ambienti non di produzione. Non utilizzare mai dati di produzione di testo normale in ambienti non di produzione e non utilizzare mai le Informazioni personali in ambienti non di produzione per nessun motivo. Assicurati che tutti i dati di test e gli account vengano rimossi prima del rilascio in produzione.
- 7.9 Esaminare il codice sorgente aperto o gratuito approvato da CWT, software, applicazioni o servizi per difetti, bug, problemi di sicurezza o non conformità con i termini di licenza open o sorgente gratuita. Il venditore deve notificare a CWT in anticipo l'utilizzo di qualsiasi codice sorgente aperto o gratuito e, se approvato per l'uso da CWT, fornire a CWT il nome, la versione e l'URL del codice sorgente aperto o gratuito. Il Fornitore dichiara e garantisce che (a) qualsiasi codice sorgente aperto o gratuito utilizzato nei suoi prodotti o servizi sarà concesso in licenza in base a licenze di codice sorgente aperte o gratuite "permissive" e non in base a licenze restrittive, reciproche, ereditarie o copyleft; (b) Il venditore ha il diritto di modificare, adattare liberamente codice sorgente aperto o gratuito e combinare codice sorgente aperto o gratuito o contenere codice sorgente aperto o gratuito con codice proprietario senza porre restrizioni a tali modifiche, adattamenti o combinazioni o codice proprietario che contiene codice sorgente aperto o gratuito e come questi possono essere concessi in licenza in seguito (collettivamente, " **opere derivate** ") e (c) tali opere derivate non saranno soggette ad alcuna licenza open source o gratuita che richieda la licenza dell'opera derivata o la renda disponibile gratuitamente a terzi in base ai termini di licenza open source o free source.
- 7.10 Non condividere alcun codice creato ai sensi dell'Accordo, indipendentemente dalla fase di sviluppo, in alcun ambiente condiviso o non privato, come un repository di codice ad accesso aperto, indipendentemente dalla protezione tramite password.

8. Software e integrità dei dati

Il venditore deve, come minimo:

- 8.1 Negli ambienti in cui il software antivirus è disponibile in commercio, installare e in esecuzione il software antivirus aggiornato per cercare e rimuovere o mettere in quarantena tempestivamente virus e altri malware da qualsiasi sistema o dispositivo.
- 8.2 Separare le informazioni e le risorse non di produzione dalle informazioni e dalle risorse di produzione.

- 8.3 Assicurati che i team utilizzino un processo di controllo delle modifiche documentato per tutte le modifiche al sistema, comprese le procedure di back-out per tutti gli ambienti di produzione e i processi di modifica di emergenza. Includere test, documentazione e approvazioni per tutte le modifiche al sistema e richiedere l'approvazione della direzione per modifiche significative in tali processi.
- 8.4 Costruisci e gestisci una zona PCI se il fornitore elabora o archivia i dati del titolare della carta.
- 8.5 Per le applicazioni che utilizzano un database che consente modifiche alle informazioni personali e riservate, abilitare e mantenere le funzionalità di registrazione del controllo delle transazioni del database che conservano i registri di controllo delle transazioni del database per un minimo di un (1) anno con tre mesi immediatamente disponibili per l'analisi.
- 8.6 Esaminare il software per trovare e correggere le vulnerabilità della sicurezza durante l'implementazione iniziale e in caso di modifiche e aggiornamenti significativi.
- 8.7 Eseguire test di garanzia della qualità per i componenti di sicurezza (ad es. test di identificazione, autenticazione e funzioni di autorizzazione), nonché qualsiasi altra attività progettata per convalidare l'architettura di sicurezza, durante l'implementazione iniziale e in seguito a modifiche e aggiornamenti significativi.

9. **Sicurezza del sistema**

Il venditore deve, come minimo:

- 9.1 Creare e aggiornare regolarmente le versioni più recenti del flusso di dati e dei diagrammi di sistema utilizzati per accedere, elaborare, gestire o archiviare informazioni personali e informazioni riservate.
- 9.2 Monitorare attivamente le risorse del settore (ad es. , www.cert.org e mailing list e siti Web dei fornitori di software pertinenti) per la notifica tempestiva di tutti gli avvisi di sicurezza applicabili relativi ai sistemi del fornitore e ad altre risorse informative.
- 9.3 Gestire in modo efficace le chiavi crittografiche riducendo l'accesso alle chiavi del minor numero di custodi necessario, archiviando chiavi crittografiche segrete e private crittografando con una chiave almeno potente quanto la chiave di crittografia dei dati e archiviando separatamente dalla chiave di crittografia dei dati in un luogo sicuro dispositivo crittografico, nel minor numero di posizioni possibili. Modifica le chiavi crittografiche dall'impostazione predefinita al momento dell'installazione e almeno ogni due anni e smaltisci in modo sicuro le vecchie chiavi.
- 9.4 Scansione di sistemi interni ed esterni e altre risorse informative, inclusi, a titolo esemplificativo, reti, server, applicazioni e database, con il software di scansione delle vulnerabilità di sicurezza applicabile standard del settore per scoprire le vulnerabilità della sicurezza, garantire che tali sistemi e altre risorse siano adeguatamente rafforzata e identificare eventuali reti wireless non autorizzate almeno trimestralmente e prima del

rilascio per le applicazioni e per modifiche e aggiornamenti significativi entro i tempi risultanti da analisi dei rischi basate su politiche e standard IT ragionevoli e generalmente accettati.

- 9.5 Garantire che tutti i sistemi e le altre risorse del fornitore siano e rimangano protetti, inclusa, a titolo esemplificativo, la rimozione o la disabilitazione della rete inutilizzata e altri servizi e prodotti (ad es. finger, rlogin, ftp e semplice Transmission Control Protocol/Internet Protocol (TCP/ servizi e prodotti IP) e l'installazione di un firewall di sistema, wrapper TCP (Transmission Control Protocol) o tecnologie simili.
- 9.6 Implementare uno o più Sistemi di rilevamento delle intrusioni (IDS), Sistemi di prevenzione delle intrusioni (IPS) o Sistemi di rilevamento e prevenzione delle intrusioni (IDP) in una modalità operativa attiva che monitora tutto il traffico in entrata e in uscita dai sistemi e dalle altre risorse insieme all'accordo in ambienti in cui tale tecnologia è disponibile in commercio e nella misura del possibile.
- 9.7 Mantenere un processo di valutazione del rischio per i risultati della valutazione delle vulnerabilità allineati con le migliori pratiche del settore per rimediare alle vulnerabilità della sicurezza in qualsiasi sistema o altra risorsa, incluse, a titolo esemplificativo, quelle scoperte tramite pubblicazioni di settore, scansione delle vulnerabilità, scansione dei virus e revisione dei registri di sicurezza e applicare tempestivamente adeguate patch di sicurezza in relazione alla probabilità che tale vulnerabilità possa essere o sia in procinto di essere sfruttata. I risultati e le patch della valutazione delle vulnerabilità critiche devono essere corretti immediatamente dopo la disponibilità e in ogni caso non oltre 7 giorni dopo il rilascio. I risultati e le patch della valutazione della vulnerabilità elevata devono essere corretti entro 30 giorni dal rilascio. I risultati e le patch della valutazione della vulnerabilità media devono essere corretti entro 90 giorni di calendario. I risultati e le patch della valutazione della vulnerabilità bassa devono essere corretti entro 120 giorni di calendario.
- 9.8 Condurre test di penetrazione della rete e della segmentazione internamente ed esternamente almeno una volta all'anno e dopo qualsiasi aggiornamento o modifica dell'infrastruttura o dell'applicazione significativa.
- 9.9 Rimuovere o disabilitare il software non autorizzato rilevato sui sistemi del fornitore e utilizzare controlli antimalware standard del settore, inclusi l'installazione, l'aggiornamento regolare e l'uso di routine di prodotti software antimalware su tutti i servizi, sistemi e dispositivi che possono essere utilizzati per accedere alle informazioni personali e CWT Informazioni confidenziali. Utilizzare un software antivirus affidabile e conforme alle migliori pratiche del settore, ove possibile, e assicurarsi che tali definizioni dei virus rimangano aggiornate.
- 9.10 Mantenere aggiornato il software su tutti i servizi, i sistemi e i dispositivi che possono essere utilizzati per accedere alle informazioni personali e alle informazioni riservate CWT, inclusa la manutenzione adeguata del sistema o dei sistemi operativi e l'installazione corretta di patch di sicurezza ragionevolmente aggiornate.

- 9.11 Assegnare responsabilità di amministrazione della sicurezza per la configurazione dei sistemi operativi host a persone specifiche.
- 9.12 Modifica tutti i nomi account predefiniti e/o le password predefinite.

10. Monitoraggio

Il venditore deve, come minimo:

- 10.1 Conservare i dati di registro per le informazioni personali e riservate per almeno 12 mesi dalla data di creazione dei dati di registro e rendere il registro e tali dati disponibili a CWT entro un periodo di tempo ragionevole e su richiesta, se non diversamente specificato nell'Accordo. I registri devono essere progettati per rilevare e rispondere agli incidenti e includere, ma non essere limitati a:
 - a. Tutti i singoli utenti accedono alle Informazioni personali e alle Informazioni riservate
 - b. Tutte le azioni intraprese da chi dispone dei privilegi di amministratore o root
 - c. Tutti gli utenti accedono alle tracce di controllo
 - d. Tentativi di accesso logico non validi
 - e. Utilizzo e modifiche ai meccanismi di identificazione e autenticazione
- 10.2 Registrare le attività del sistema principale di terze parti del fornitore per i sistemi contenenti informazioni personali e informazioni riservate e disporre di un programma di garanzia formale di terze parti per garantire che le terze parti o i subappaltatori del fornitore dispongano di controlli e certificazioni di sicurezza appropriati Effettuare una valutazione della sicurezza del cloud se CWT i dati risiedono in un ambiente cloud.
- 10.3 Limita l'accesso per i registri di sicurezza alle persone autorizzate e proteggi i registri di sicurezza da modifiche non autorizzate.
- 10.4 Implementare un meccanismo di rilevamento delle modifiche (ad es ., monitoraggio dell'integrità dei file) per avvisare il personale di modifiche non autorizzate di file di sistema critici, file di configurazione o file di contenuto; configurare il software per eseguire confronti di file critici settimanalmente.
- 10.5 Esaminare, con cadenza almeno settimanale, tutti i registri di controllo relativi alla sicurezza e alla sicurezza sui sistemi contenenti informazioni personali e informazioni riservate per rilevare eventuali anomalie e documentare e risolvere tempestivamente tutti i problemi di sicurezza registrati.
- 10.6 Esaminare quotidianamente tutti gli eventi di sicurezza, i registri dei componenti del sistema che archiviano, elaborano o trasmettono i dati dei titolari di carte, i registri dei componenti critici del sistema e i registri dei server e dei componenti del sistema che svolgono funzioni di sicurezza.

11. Gateway di sicurezza

Il venditore deve, come minimo:

- 11.1 Richiede l'autenticazione avanzata per l'accesso amministrativo e/o gestionale ai gateway di sicurezza, incluso, a titolo esemplificativo, qualsiasi accesso allo scopo di rivedere i file di registro.
- 11.2 Disporre e utilizzare controlli, politiche, processi e procedure documentati per garantire che gli utenti non autorizzati non abbiano accesso amministrativo e/o gestionale ai gateway di sicurezza e che i livelli di autorizzazione dell'utente per amministrare e gestire i gateway di sicurezza siano appropriati.
- 11.3 Disponi di forti controlli sulla sicurezza della posta elettronica, come la configurazione dei protocolli di autenticazione DKIM e SPF che aiutano a convalidare un messaggio di posta elettronica da un'origine attendibile e convalidata. Implementazione di DMARC sulla ricezione di server di posta elettronica.
- 11.4 Almeno una volta ogni sei (6) mesi, assicurarsi che le configurazioni del gateway di sicurezza siano rafforzate selezionando un campione di gateway di sicurezza e verificando che ogni set di regole predefinito e set di parametri di configurazione garantisca quanto segue:
 - un. Il routing di origine IP (Internet Protocol) è disabilitato,
 - b. L'indirizzo di loopback non può entrare nella rete interna,
 - c. Sono implementati filtri anti-spoofing,
 - d. I pacchetti di trasmissione non possono entrare nella rete,
 - e. I reindirizzamenti ICMP (Internet Control Message Protocol) sono disabilitati,
 - f. Tutti i set di regole terminano con un'istruzione "DENY ALL" e
 - g. Ogni regola è riconducibile a una specifica richiesta aziendale.
- 11.5 Assicurarsi che gli strumenti di monitoraggio vengano utilizzati per convalidare che tutti gli aspetti dei gateway di sicurezza (ad es. hardware, firmware e software) siano costantemente operativi.

Assicurarsi che tutti i gateway di sicurezza siano configurati e implementati in modo tale che tutti i gateway di sicurezza non operativi neghino l'accesso.
- 11.6 I pacchetti in entrata dalla rete esterna non attendibile devono terminare all'interno della zona demilitarizzata (" **DMZ** ") e non devono essere autorizzati a fluire direttamente attraverso la rete interna attendibile. Tutti i pacchetti in entrata che fluiscono verso la rete interna affidabile devono avere origine solo all'interno della DMZ. La DMZ deve essere separata dalla rete esterna non attendibile mediante l'uso di un gateway di sicurezza e deve essere separata dalla rete interna attendibile mediante l'uso di:
 - un. un altro gateway di sicurezza, o

- b. lo stesso Security Gateway utilizzato per separare la DMZ dalla rete esterna non attendibile, nel qual caso il Security Gateway deve garantire che i pacchetti ricevuti dalla rete esterna non attendibile vengano eliminati immediatamente o, se non eliminati, vengano instradati solo alla DMZ senza altre elaborazioni di tali pacchetti in entrata eseguiti in modo diverso dall'eventuale scrittura dei pacchetti in un registro.

Quanto segue deve trovarsi solo all'interno della rete interna affidabile:

- un. Tutte le informazioni personali e le informazioni riservate CWT archiviate senza l'uso di Strong Encryption,
- b. La copia ufficiale delle informazioni
- c. Server di database,
- d. Tutti i registri esportati e
- e. Tutti gli ambienti utilizzati per sviluppo, test, sandbox, produzione e qualsiasi altro ambiente simile; e tutte le versioni del codice sorgente.

- 11.7 Le credenziali di autenticazione non protette dall'uso di Strong Encryption non devono trovarsi all'interno della DMZ.

12. Sicurezza della rete

Il venditore deve, come minimo:

- 12.1 Su richiesta di CWT, fornire a CWT un diagramma di rete logico che documenti i sistemi e le connessioni ad altre risorse inclusi router, switch, firewall, sistemi IDS, topologia di rete, punti di connessione esterni, gateway, reti wireless e qualsiasi altro dispositivo che supporti CWT.
- 12.2 Mantenere un processo formale per l'approvazione, il test e la documentazione di tutte le connessioni di rete e le modifiche alle configurazioni del firewall e del router. Configura i firewall per negare e registrare i pacchetti sospetti e limitarli per consentire solo il traffico appropriato e autorizzato, negando tutto il resto del traffico attraverso il firewall. Rivedi le regole del firewall ogni sei mesi.
- 12.3 Installare un firewall su ogni connessione Internet e tra qualsiasi DMZ e l'area di rete interna. Qualsiasi sistema che archivia le informazioni personali deve risiedere nell'area della rete interna, segregata dalla DMZ e da altre reti non attendibili.
- 12.4 Monitorare il firewall a livello perimetrale e interno per controllare e proteggere il flusso del traffico di rete in entrata o in uscita dal confine o confine, se necessario.
- 12.5 Installa tecnologie di rilevamento delle minacce come Network Detection and Response (NDR), Endpoint Detection and Response (EDR) e Extended Detection and Response (XDR) che offrono una soluzione completa per rilevare e rispondere a vari attacchi informatici o attacchi ransomware.

- 12.6 Mantenere un processo documentato e controlli in atto per rilevare e gestire i tentativi non autorizzati di accedere alle informazioni personali e alle informazioni riservate di CWT.
- 12.7 Quando si forniscono servizi e prodotti basati su Internet a CWT, proteggere le informazioni personali e riservate mediante l'implementazione di una rete DMZ. I server Web che forniscono servizi a CWT risiedono nella DMZ. Qualsiasi sistema o risorsa di informazioni che memorizza informazioni personali e informazioni riservate (come applicazioni e server di database) deve risiedere in una rete interna affidabile. Il venditore utilizzerà DMZ per servizi e prodotti Internet .
- 12.8 Limitare il traffico in uscita non autorizzato dalle applicazioni che elaborano, archiviano o trasmettono informazioni personali e informazioni riservate a indirizzi IP all'interno della DMZ e Internet.
- 12.9 Quando si utilizzano tecnologie di rete wireless basate su radiofrequenza (RF) per eseguire o supportare servizi e prodotti per CWT, il Fornitore dovrà garantire che tutte le Informazioni personali e le Informazioni riservate trasmesse siano protette mediante l'uso di tecnologie di crittografia adeguate sufficienti a proteggere la riservatezza delle Informazioni personali e informazioni riservate; fermo restando, tuttavia, che in ogni caso tale cifratura deve utilizzare lunghezze di chiave non inferiori a 256 bit per la cifratura simmetrica e a 2048 bit per la cifratura asimmetrica. Scansiona, identifica e disabilita regolarmente i punti di accesso wireless non autorizzati.
- 12.10 Sicurezza cloud: quando i dati di CWT risiedono sul cloud o il fornitore utilizza un ambiente cloud di terze parti inclusi, a titolo esemplificativo ma non esaustivo, Infrastructure as a Service (IaaS), Software as a Service (SaaS) e Platform as a Service (PaaS), il fornitore deve implementare o valutare per Cloud Security Posture Management per rilevare e correggere automaticamente minacce, configurazioni errate, uso improprio e violazioni della conformità nei cloud pubblici.

13. Requisiti di connettività

- 13.1 Nel caso in cui il Fornitore disponga, o debba essere fornita, connettività alle Informazioni personali e alle risorse di Informazioni riservate CWT in congiunzione con l'Accordo, in aggiunta a quanto sopra, se il Fornitore ha o riceve connettività all'ambiente di CWT, il Fornitore dovrà, a un minimo:
- un. Utilizzare solo le strutture e le metodologie di connessione concordate per interconnettere l'ambiente di CWT con le risorse del fornitore.
 - b. NON stabilire l'interconnessione all'ambiente di CWT senza il previo consenso scritto di CWT.
 - c. Fornire l'accesso CWT a tutte le strutture del Fornitore applicabili durante il normale orario lavorativo per la manutenzione e il supporto di qualsiasi apparecchiatura (ad es. router) fornita da CWT ai sensi dell'Accordo per la connettività alle informazioni personali e alle informazioni riservate.

- d. Utilizzare qualsiasi attrezzatura fornita da CWT ai sensi dell'Accordo per la connettività all'ambiente di CWT solo per la fornitura di quei servizi e prodotti o funzioni esplicitamente autorizzati nell'Accordo.
- e. Se la metodologia di connettività concordata richiede che il fornitore implementi un gateway di sicurezza, conservare i registri di tutte le sessioni che utilizzano tale gateway di sicurezza. Questi registri di sessione devono includere informazioni sufficientemente dettagliate per identificare l'utente finale o l'applicazione, l'indirizzo IP di origine, l'indirizzo IP di destinazione, le porte/protocolli di servizio utilizzati e la durata dell'accesso. Questi registri di sessione devono essere conservati per un minimo di sei (6) mesi dalla creazione della sessione.
- f. Consenti a CWT di raccogliere informazioni relative all'accesso, incluso l'accesso del fornitore, all'ambiente di CWT. Queste informazioni possono essere raccolte, conservate e analizzate da CWT per identificare potenziali rischi per la sicurezza senza ulteriore avviso. Queste informazioni possono includere da file di traccia, statistiche, indirizzi di rete e dati o schermate effettivi a cui si accede o si trasferiscono.
- g. Sospendere o interrompere immediatamente qualsiasi interconnessione all'ambiente di CWT se i Fornitori ritengono che vi sia stata una violazione o un accesso non autorizzato o su istruzioni di CWT se CWT, a sua esclusiva discrezione, ritiene che ci sia stata una violazione della sicurezza o un accesso non autorizzato o un uso improprio delle strutture dati di CWT o qualsiasi informazione, sistema o altra risorsa CWT.

14. Dispositivi mobili e portatili

Il venditore deve, come minimo:

- 14.1 Non archiviare informazioni personali e informazioni riservate su dispositivi mobili e portatili, a meno che non siano completamente crittografate utilizzando Strong Encryption.
- 14.2 Utilizzare la crittografia avanzata per proteggere le informazioni personali e le informazioni riservate trasmesse, utilizzate o accessibili in remoto da dispositivi mobili e portatili compatibili con la rete.
 - un. Quando si utilizzano dispositivi mobili e portatili con riconoscimento della rete che non sono computer portatili per accedere e/o archiviare informazioni personali e informazioni riservate, tali dispositivi devono essere in grado di eliminare tutte le copie archiviate di informazioni personali e informazioni riservate al ricevimento sulla rete di un comando. (Nota: tale funzionalità viene spesso definita funzionalità di "cancellazione remota".)
 - b. Disporre di politiche, procedure e standard documentati per garantire che la parte autorizzata che dovrebbe avere il controllo fisico di un dispositivo mobile e portatile compatibile con la rete che non sia un computer portatile e che sta archiviando informazioni personali e informazioni riservate avvii prontamente la cancellazione di tutti Informazioni personali e informazioni riservate in caso di smarrimento o furto del dispositivo.
 - c. Disporre di politiche, procedure e standard documentati per garantire che i dispositivi mobili e portatili che non sono computer portatili e non riconoscono la rete eliminino

automaticamente tutte le copie archiviate delle informazioni personali e riservate dopo tentativi consecutivi di accesso falliti.

- 14.3 Disporre di politiche, procedure e standard documentati che garantiscano che tutti i dispositivi mobili e portatili utilizzati per accedere e/o archiviare informazioni personali e informazioni riservate:
- un. Sono in possesso fisico di Soggetti Autorizzati ;
 - b. sono fisicamente assicurati quando non sono fisicamente in possesso di Soggetti Autorizzati ; o
 - c. Eliminare la loro conservazione dei dati in modo tempestivo e sicuro quando non sono fisicamente in possesso di una Parte Autorizzata, o fisicamente protetta, o dopo 10 tentativi di accesso non andati a buon fine.
- 14.4 Prima di consentire l'accesso alle informazioni personali e alle informazioni riservate archiviate su o tramite l'uso di dispositivi mobili e portatili, il venditore deve disporre e utilizzare una procedura per garantire che:
- un. L'utente è un Soggetto Autorizzato autorizzato a tale accesso; e
 - b. L'identità dell'utente è stata autenticata.
- 14.5 Implementare una politica che vieti l'uso di dispositivi mobili e portatili che non sono amministrati e/o gestiti dal fornitore o da CWT per accedere e/o archiviare informazioni personali e informazioni riservate.
- 14.6 Riesaminare, almeno una volta all'anno, l'uso e i controlli per tutti i dispositivi mobili e portatili gestiti o amministrati dal fornitore per garantire che i dispositivi mobili e portatili possano soddisfare le misure di sicurezza tecniche e organizzative applicabili.

15. Sicurezza in transito

Il venditore deve, come minimo:

- 15.1 Utilizzare la crittografia avanzata per il trasferimento di informazioni personali e informazioni riservate al di fuori di reti controllate da CWT o dal fornitore o durante la trasmissione di informazioni personali e informazioni riservate su qualsiasi rete non attendibile.
- 15.2 Per i record contenenti informazioni personali e informazioni riservate in formato cartaceo, microfiche o supporti elettronici da trasferire fisicamente, trasportarli tramite corriere assicurato o altro metodo di consegna che possa essere tracciato, imballato in modo sicuro e secondo le specifiche del produttore. Qualsiasi informazione personale e informazione riservata deve essere trasportata in contenitori chiusi a chiave.

16. Sicurezza a riposo

Il venditore deve , come minimo :

- 16.1 Utilizzare la crittografia avanzata per proteggere le informazioni personali e le informazioni riservate quando archiviate.
- 16.2 Non archiviare le informazioni personali o riservate elettronicamente al di fuori dell'ambiente di rete del fornitore (o della rete di computer sicura di CWT) a meno che il dispositivo di archiviazione (ad esempio, nastro di backup, laptop, memory stick, disco del computer, ecc .) non sia protetto da Strong Encryption.
- 16.3 Non archiviare informazioni personali o informazioni riservate su supporti rimovibili (ad es. unità flash USB, chiavette USB, memory stick, nastri, CD o dischi rigidi esterni) ad eccezione: per scopi di backup, continuità operativa, ripristino di emergenza e scambio di dati, come consentito e richiesto dal contratto tra il venditore e CWT. Se viene utilizzato un supporto rimovibile per archiviare informazioni personali o informazioni riservate in base alle eccezioni indicate in questa sottosezione, le informazioni devono essere protette utilizzando la crittografia avanzata. L'esecuzione automatica deve essere disabilitata per i supporti rimovibili e i dispositivi di archiviazione .
- 16.4 Archiviare e proteggere in modo appropriato i record contenenti Informazioni personali o Informazioni riservate in formato cartaceo o microfiche in aree il cui accesso è limitato al personale autorizzato.
- 16.5 Salvo diversa indicazione scritta da parte di CWT, durante la raccolta, la generazione o la creazione di Informazioni personali o Informazioni riservate in formato cartaceo e supporti di backup per, tramite o per conto di CWT o con il marchio CWT, assicurarsi che tali informazioni siano Informazioni personali o Informazioni riservate e, ove possibile, etichettare tali informazioni di CWT come "Riservate". Il Fornitore riconosce che le Informazioni personali e le Informazioni riservate sono e rimarranno di proprietà di CWT, indipendentemente dall'etichettatura o dalla loro assenza.

17. Restituzione, ritenzione, distruzione e smaltimento

Il venditore deve, come minimo:

- 17.1 Senza costi aggiuntivi per CWT , su richiesta di CWT o alla risoluzione del Contratto , fornire copie di qualsiasi Informazione personale e Informazioni riservate a CWT entro trenta (30) giorni di calendario da tale richiesta o risoluzione del Contratto . Il Fornitore dovrà restituire o, a discrezione di CWT, distruggere tutte le Informazioni Riservate e le Informazioni Personali di CWT, comprese le copie di backup elettroniche , cartacee e protette come previsto nell'Accordo o, se non previsto nell'Accordo, entro novanta calendari (90) giorni dopo il più presto tra: (a) la scadenza o la risoluzione del Contratto, (b) la richiesta di CWT per la restituzione delle Informazioni personali e delle Informazioni riservate, o (c) la data in cui il Fornitore non ha più bisogno delle Informazioni personali e delle Informazioni riservate per eseguire i servizi e prodotti nell'ambito dell'accordo.

- 17.2 Nel caso in cui CWT approvi la distruzione come alternativa alla restituzione di Informazioni Personali e Informazioni Riservate, certificare per iscritto, da un funzionario del Venditore, la distruzione in quanto rende le Informazioni Personali e Informazioni Riservate non recuperabili e irrecuperabili. Il Fornitore distruggerà completamente tutte le copie delle Informazioni personali e delle Informazioni riservate in tutti i luoghi e in tutti i sistemi in cui sono archiviate le Informazioni personali e le Informazioni riservate, incluse, a titolo esemplificativo ma non esaustivo, le Parti autorizzate precedentemente approvate. Tali informazioni devono essere distrutte seguendo una procedura standard del settore per la distruzione completa come DOD 5220.22M o pubblicazione speciale NIST 800-88 o utilizzando un prodotto di smagnetizzazione raccomandato dal produttore per il sistema interessato. Prima di tale distruzione, il Fornitore manterrà tutte le misure di sicurezza tecniche e organizzative applicabili per proteggere la sicurezza, la privacy e la riservatezza delle Informazioni personali e delle Informazioni riservate.
- 17.3 Smaltire le informazioni personali e le informazioni riservate di CWT in modo da garantire che le informazioni non possano essere ricostruite in un formato utilizzabile. Carte, diapositive, microfilm, microfiche e fotografie devono essere smaltiti mediante triturazione incrociata o combustione. I materiali contenenti informazioni personali e informazioni riservate CWT in attesa di distruzione devono essere conservati in contenitori protetti ed essere trasportati utilizzando una terza parte sicura.

18. Risposta all'incidente e notifica

Il venditore deve, come minimo:

- 18.1 Avere e utilizzare un Processo di gestione degli incidenti e relative procedure e personale tale Processo di gestione degli incidenti e procedure con risorse specializzate. Immediatamente, e in nessun caso più di ventiquattro (24) ore, informare CWT all'indirizzo gbt-securitynotification@amexgbt.com ogni volta che si verifica un attacco sospetto o confermato, intrusione, accesso non autorizzato, perdita o altro incidente riguardante le informazioni di CWT, sistemi o altre risorse.
- 18.2 Dopo aver notificato a CWT, fornire a CWT regolari aggiornamenti dello stato, incluse, a titolo esemplificativo, le azioni intraprese per risolvere tale incidente, a intervalli o orari concordati di comune accordo per la durata dell'incidente e non appena ragionevolmente possibile dopo la chiusura dell'incidente, fornire a CWT un rapporto scritto che descriva l'incidente, le azioni intraprese dal venditore durante la sua risposta e i piani del venditore per azioni future per prevenire il verificarsi di un incidente simile.
- 18.3 Non segnalare o divulgare pubblicamente tali violazioni delle informazioni, dei sistemi o di altre risorse di CWT senza prima avvisare CWT e collaborare direttamente con CWT per notificare i funzionari governativi regionali, nazionali, statali o locali applicabili o i servizi di monitoraggio del credito, le persone interessate da tale violazione, e tutti i mezzi di comunicazione applicabili, come richiesto dalla legge.

- 18.4 Disporre di un processo per identificare tempestivamente le violazioni dei controlli di sicurezza, comprese quelle stabilite nei presenti Requisiti di sicurezza delle informazioni da parte del personale del Fornitore o di Terze parti. I trasgressori identificati saranno soggetti ad un'adeguata azione disciplinare soggetta alle leggi applicabili. Nonostante quanto sopra, i trasgressori rimarranno sotto l'autorità del Venditore o dei suoi Terzi. CWT non potrà essere considerata datore di lavoro del Venditore o del personale di Terze Parti .

19. Gestione della continuità operativa e ripristino di emergenza

Il venditore deve, come minimo:

- 19.1 Sviluppare , utilizzare, gestire e rivedere i piani di continuità aziendale per ciascuna sede e piani di ripristino di emergenza per ciascuna tecnologia di base al fine di ridurre al minimo l'impatto per CWT sul servizio o sui prodotti del fornitore. Tali piani devono includere: risorse nominative specifiche per le funzioni di continuità operativa e ripristino di emergenza, obiettivi stabiliti per i tempi di ripristino e obiettivi per i punti di ripristino, backup almeno giornaliero di dati e sistemi, archiviazione fuori sede dei dati e backup e record dei sistemi, registrazione piani di protezione e di emergenza commisurati ai requisiti dell'Accordo, archiviare tali registri e piani in modo sicuro fuori sede e garantire che tali piani siano disponibili per il Fornitore secondo necessità.
- 19.2 Su richiesta di CWT, fornire a CWT un piano di continuità aziendale documentato che assicuri che il Fornitore possa adempiere ai propri obblighi contrattuali ai sensi dell'Accordo e del presente documento , compresi i requisiti di qualsiasi dichiarazione di lavoro applicabile o accordo sul livello di servizio. Tali piani eserciteranno il recupero proteggendo al contempo l'integrità e la riservatezza delle Informazioni personali e delle Informazioni riservate.
- 19.3 Disporre di procedure documentate per il backup e il recupero sicuri delle Informazioni personali e delle Informazioni riservate che devono includere, come minimo, procedure per il trasporto, l'archiviazione e l'eliminazione delle copie di backup delle Informazioni personali e delle Informazioni riservate e, su richiesta di CWT, fornire tali procedure documentate a CWT.
- 19.4 Assicurarsi che i backup di tutte le informazioni personali e riservate archiviate o del software e delle configurazioni per i sistemi utilizzati da CWT vengano creati almeno una volta alla settimana.
- 19.5 I piani di continuità operativa e di ripristino di emergenza devono essere aggiornati almeno una volta all'anno o ogniqualvolta ciò sia reso necessario da modifiche significative dell'ambiente aziendale e/o tecnologico.
- 19.6 Tali piani devono inoltre essere esercitati in modo comprensibile almeno una volta all'anno, oa seguito di qualsiasi cambiamento sostanziale nei piani di continuità operativa o di ripristino

di emergenza a esclusivo costo e spesa del Fornitore. Tali esercizi devono garantire il corretto funzionamento delle tecnologie interessate e la consapevolezza interna di tali piani.

- 19.7 Esaminare tempestivamente il suo piano di continuità aziendale per affrontare fonti o scenari di minaccia aggiuntivi o emergenti e fornire a CWT un riepilogo di alto livello dei piani e dei test entro un lasso di tempo ragionevole su richiesta.
- 19.8 Garantire che tutte le sedi convenzionate o convenzionate che ospitano o elaborano informazioni personali e informazioni riservate CWT siano monitorate 24 ore al giorno, sette (7) giorni alla settimana contro intrusioni, incendi, acqua e altri rischi ambientali.

20. Conformità e accreditamenti

Il venditore deve, come minimo:

- 20.1 Conservare registrazioni complete e accurate relative all'adempimento dei propri obblighi derivanti da questi Requisiti di sicurezza delle informazioni e dal rispetto del presente documento da parte del Fornitore in un formato che consenta la valutazione o l'audit per un periodo non inferiore a tre (3) anni o più, se necessario a seguito di un'ingiunzione del tribunale o di un procedimento civile o regolamentare. Fermo restando quanto sopra, il Fornitore sarà tenuto a mantenere i registri di sicurezza solo per un minimo di un (1) anno dopo l'eventuale esecuzione continua del Contratto.
- 20.2 Consentire a CWT, senza costi aggiuntivi per CWT, di condurre, previo ragionevole preavviso, valutazioni di sicurezza periodiche o audit della Misura di sicurezza tecnica e organizzativa utilizzata dal Venditore durante i quali CWT fornirà al Venditore questionari scritti e richieste di documentazione. Per tutte le richieste, il Venditore risponderà con una risposta scritta e prove, se del caso, immediatamente o previo accordo reciproco. Su richiesta di CWT per un audit da parte di CWT, il Fornitore pianificherà un audit di sicurezza che inizi entro dieci (10) giorni lavorativi da tale richiesta. CWT potrebbe richiedere l'accesso a strutture, sistemi, processi o procedure per valutare l'ambiente di controllo della sicurezza del fornitore.
- 20.3 Su richiesta di CWT, dichiarare di essere conforme al presente documento insieme alle certificazioni di supporto per le versioni più recenti di PCI-DSS, ISO 27001/27002, SOC 2, Cyber Essentials o valutazioni simili per il Fornitore e per qualsiasi subappaltatore o terza parte elaborazione, accesso, archiviazione o gestione per conto del Venditore. Se il Fornitore non è in grado di certificare la conformità, deve fornire un rapporto scritto che specifichi in dettaglio dove è non conforme e il suo piano di riparazione per diventare conforme.
- 20.4 Nel caso in cui CWT, a sua esclusiva discrezione, ritenga che si sia verificata una violazione della sicurezza che non è stata segnalata a CWT in conformità al presente Accordo e al Processo di gestione degli incidenti del fornitore, programmare l'inizio dell'audit o della valutazione entro ventiquattro (24) ore della comunicazione di CWT che richiede una valutazione o un audit.
- 20.5 Entro trenta (30) giorni di calendario dal ricevimento dei risultati della valutazione o del rapporto di audit, fornire a CWT un rapporto scritto che illustri le azioni correttive che il

Fornitore ha implementato o si propone di attuare con il programma e lo stato attuale di ciascuna azione correttiva. Il Fornitore aggiornerà questo rapporto a CWT ogni trenta (30) giorni di calendario riportando lo stato di tutte le azioni correttive fino alla data di attuazione. Il Fornitore dovrà attuare tutte le azioni correttive entro novanta (90) giorni dal ricevimento da parte del Fornitore della relazione di valutazione o audit o entro un periodo di tempo alternativo a condizione che tale periodo di tempo alternativo sia stato concordato di comune accordo per iscritto dalle parti entro non più di trenta (30) giorni dal ricevimento da parte del Venditore della relazione di valutazione o di audit.

- 20.6 Conformità PCI DSS - Nella misura in cui il fornitore gestisce i numeri di conto di pagamento o qualsiasi altra informazione di pagamento correlata, il fornitore deve essere attualmente conforme alla versione più recente di Payment Card Industry (PCI-DSS) per l'intero ambito dei sistemi che gestiscono queste informazioni e continuare tale conformità. Se un subappaltatore o una terza parte sta elaborando, accedendo, archiviando o gestendo i dati della carta di credito per conto del venditore, il venditore deve ottenere un PCI AOC da tale subappaltatore o terza parte e renderlo disponibile a CWT su richiesta. Nel caso in cui il Fornitore non sia o non sia più conforme a PCI-DSS per qualsiasi parte dell'intero ambito dei sistemi che gestiscono dati applicabili PCI, il Fornitore informerà tempestivamente CWT, procederà immediatamente senza indebito ritardo a porre rimedio a tale non conformità e fornirà stato regolare di tale riparazione a CWT su richiesta.

21. Standard, migliori pratiche, regolamenti e leggi

Nel caso in cui il Fornitore elabori, acceda, visualizzi, memorizzi o gestisca Informazioni personali o Informazioni riservate relative a personale CWT, partner, Affiliati, clienti CWT; o dipendenti, appaltatori, subappaltatori o fornitori di clienti CWT; Il Fornitore adotterà misure di sicurezza tecniche e organizzative non meno rigorose di quelle richieste dalle linee guida, dai regolamenti, dalle direttive e dalle leggi globali, regionali, nazionali, statali e locali applicabili.

22. Modifica

CWT si riserva il diritto di aggiornare o modificare questi Requisiti di sicurezza delle informazioni di volta in volta pubblicando l'ultima versione sul sito Web di CWT. A meno che il Venditore non fornisca una notifica scritta di opposizione a tali aggiornamenti o modifiche entro trenta (30) giorni dalla pubblicazione, si riterrà che il Venditore li abbia accettati.

Versione 8

Data: settembre 2026