Italian

Requisiti di sicurezza delle informazioni

1. Introduzione

Il Fornitore accetta che soggetti terzi che agiscono per suo conto nel fornire servizi e prodotti a CWT rispettino i requisiti di sicurezza delle informazioni contenuti in questo documento ("**Requisiti di sicurezza delle informazioni**"), che definiscono le misure di sicurezza delle informazioni obbligatorie ("**Misure di sicurezza tecniche e organizzative**").

2. Definizioni

2.1 I termini definiti devono intendersi come aventi il significato indicato nel Contratto principale, salvo indicazione o integrazione ivi espressamente citata. Le seguenti definizioni si applicano ai presenti Requisiti di sicurezza delle informazioni:

"Consociate": se non diversamente definito nel Contratto, in particolare riferimento a un soggetto, qualsiasi società o persona giuridica che: (i) controlla, direttamente o indirettamente, un soggetto; oppure (ii) è controllata, direttamente o indirettamente, da un soggetto; oppure (iii) è controllata, direttamente o indirettamente, da una società o persona giuridica che controlla, direttamente o indirettamente, un soggetto. Per "controllo" si intende il diritto di esercitare oltre il cinquanta percento (50%) dei voti o un diritto di proprietà di natura simile, purché tale controllo non cessi di esistere.

"Contratto": se non diversamente definito nelle condizioni principali del Contratto, l'accordo contrattuale o un qualsiasi altro documento legale stipulato tra CWT e il Fornitore.

"Informazioni riservate": qualsiasi informazione sensibile dal punto di vista commerciale, di proprietà dell'azienda o di natura riservata relativa a (a) CWT e alle sue Consociate; (b) clienti di CWT; (c) al personale CWT; (d) partner indipendenti e joint venture o (e) ai contenuti e/o allo scopo del Contratto, che, in forma orale o scritta o mediante qualsiasi altro mezzo possa giungere, direttamente o indirettamente, in possesso del Fornitore o di un suo dipendente, agente, appaltatore o subappaltatore come risultato o in relazione al presente Contratto. A scanso di equivoci, si precisa che qualsiasi prodotto di lavoro costituirà un'Informazione riservata.

"CWT": se non diversamente definito nel Contratto, la persona giuridica CWT definita nel Contratto, nonché le sue Consociate.

"Zona demilitarizzata" o **"DMZ"**: una rete o sottorete che separa una rete interna sicura, come una Local Area Network (LAN) privata aziendale, da una rete esterna non sicura, come la rete Internet pubblica. La DMZ impedisce agli utenti esterni di ottenere l'accesso diretto alle risorse e ai sistemi interni.

"Processo di gestione degli incidenti": il processo e la procedura, sviluppati e documentati da parte del Fornitore, ai quali attenersi nel caso in cui si verifichi o si sospetti l'attacco, l'intrusione, l'accesso non autorizzato, la perdita o qualsiasi altra violazione della riservatezza, della disponibilità o dell'integrità delle Informazioni riservate e dei Dati personali.

"Mascheramento": la procedura di mascheramento delle informazioni visualizzate su uno schermo.

"Dispositivi mobili e portatili": apparecchiature mobili e/o portatili come computer, dispositivi, supporti e sistemi in grado di essere facilmente trasportati, dislocati o trasferiti e utilizzati in combinazione con il Contratto. In questa definizione rientrano computer portatili, tablet, hard disk

USB, schede di memoria USB, palmari (PDA), telefoni cellulari o con porta dati, nonché qualsiasi altro dispositivo senza fili o periferico con la capacità di archiviare Informazioni riservate e Dati personali.

"Dati personali": se non diversamente definito nel Contratto, secondo la definizione fornita dal Regolamento (UE) 2016/679 e gli standard globali applicabili in materia di sicurezza delle informazioni, tutela dei dati e normative sulla privacy,indica qualsiasi informazione relativa a una persona fisica identificata o identificabile che può essere identificata, direttamente o indirettamente, in base a un numero identificativo o uno o più elementi caratteristici della propria identità fisica, fisiologica, mentale, economica, culturale o sociale.

"Gateway di sicurezza": un insieme di meccanismi di controllo implementati tra due o più reti con diverso livello di sicurezza, che filtrano e registrano il traffico che attraversa, o tenta di attraversare, le reti e i server amministrativi e gestionali ad esse collegati. Alcuni esempi di gateway di sicurezza includono firewall, server di gestione del firewall, hopbox, session border controller, server proxy e sistemi di prevenzione delle intrusioni.

"Strong authentication": utilizzo di meccanismi e metodi di autenticazione più forti rispetto alle password richieste ai sensi della presente. Alcuni esempi di meccanismi e metodi di Strong Authentication comprendono certificati digitali, autenticazione a due fattori e one-time password.

"Crittografia avanzata": l'uso di tecnologie crittografiche con chiavi aventi una lunghezza minima di 256 bit nel caso della crittografia simmetrica, e 1024 bit per quella asimmetrica, con una sicurezza tale da garantire una ragionevole protezione delle informazioni crittografate dall'accesso non autorizzato e sufficiente a tutelare la riservatezza e la privacy di tali informazioni crittografate. Tali tecnologie incorporano un regolamento documentato per la gestione delle chiavi crittografiche e delle procedure correlate, atto a tutelare la riservatezza e la privacy delle chiavi e delle password utilizzate come input per l'algoritmo di crittografia. Alcuni esempi di crittografia avanzata includono, a titolo esemplificativo, ma non esaustivo: SSL v3.0+/TLS v1.0+, Point to Point Tunneling Protocol (PPTP), AES 256, FIPS 140-2 (esclusivamente governo degli Stati Uniti), RSA a 1024 bit, SHA1/SHA2/SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4 o WPA2.

"Misure di sicurezza tecniche e organizzative": qualsiasi attività necessaria, ai sensi dei presenti Requisiti di sicurezza delle informazioni, per l'accesso, la gestione, il trasferimento, l'elaborazione, l'archiviazione, la conservazione e la distruzione di informazioni o dati, per la divulgazione e la notifica alle parti interessate ai sensi del presente Contratto e delle normative pertinenti in materia di privacy delle informazioni e tutela dei dati, nonché per la salvaguardia delle informazioni o dei dati, al fine di preservarne la disponibilità, integrità, riservatezza e privacy, o di notificare le parti in caso di omissione della protezione di tali informazioni o dati. Tali misure includono, a titolo esemplificativo, ma non esaustivo, tutte le azioni necessarie o ritenute necessarie ai sensi delle Direttive 94/46/CE e 2006/24/CE dell'Unione europea così come promulgate negli Stati membri, del Gramm-Leach Bliley Act (GLBA) degli Stati Uniti, dell'Health Insurance Portability and Accountability Act (HIPAA) degli Stati Uniti, degli obblighi di riservatezza dei dati in vigore nell'Unione europea e in Svizzera, nonché di qualsiasi altra normativa internazionale o degli Stati Uniti, interpretazione giuridica ufficiale o precedente giudiziario riguardante le informazioni o i dati facenti parte del presente Contratto.

"Soggetto Terzo": se non diversamente definito nel Contratto, qualsiasi subappaltatore e ciascun membro del personale temporaneo del Fornitore e dei relativi appaltatori o fornitori ulteriori e/o agenti che agiscono per conto del Fornitore. La definizione non comprende altre eventuali definizioni dello stesso termine ai sensi delle normative internazionali, dell'Unione europea o degli Stati Uniti.

"Fornitore": la persona giuridica corrispondente al soggetto contraente indicato nel Contratto, nonché tutte le relative Consociate e i relativi Soggetti Terzi.

2.2 Il Fornitore dichiara e garantisce che agirà in conformità con le seguenti Misure di sicurezza tecniche e organizzative, nella misura in cui esse siano pertinenti alla fornitura dei servizi definiti nel Contratto.

3. Organizzazione della sicurezza delle informazioni

Il Fornitore dovrà:

3.1 Definire, applicare e mantenere un regolamento coerente con le pratiche del settore ma non meno che ragionevole e un programma di misure di sicurezza tecniche, organizzative, operative, amministrative e fisiche, atti a (1) impedire l'accesso alle Informazioni riservate e ai Dati personali non autorizzato ai sensi del Contratto o dei presenti Requisiti di sicurezza delle informazioni, e (2) rispettare e agire in conformità con tutti gli standard di settore pertinenti. Il Fornitore dovrà inoltre garantire che il personale addetto alla sicurezza delle informazioni disponga di un livello di esperienza ragionevole e necessario nell'ambito della sicurezza delle informazioni.

3.2 Garantire un livello adeguato di supervisione, guida e formazione sulle Misure di sicurezza tecniche e organizzative al personale del Fornitore che richiede l'accesso alle Informazioni riservate e ai Dati personali. Il Fornitore dovrà inoltre fornire una formazione adeguata in materia di Misure di sicurezza tecniche e organizzative al momento dell'assunzione e prima di eseguire l'accesso alle Informazioni riservate e ai Dati personali. Corsi di aggiornamento dovranno essere forniti almeno una volta all'anno e quanto prima, in caso di modifica sostanziale alle Misure di sicurezza tecniche e organizzative del Fornitore.

3.3 Il personale del Fornitore incaricato di svolgere importanti compiti di sicurezza, quali, ad esempio, funzioni informatiche o legate alle risorse umane, nonché qualsiasi funzione di amministrazione tecnologica, dovrà seguire corsi di formazione specifici per il ruolo ricoperto. Tali corsi specializzati dovranno includere, in maniera pertinente al ruolo, le procedure di sicurezza delle informazioni, l'uso accettabile delle risorse di sicurezza delle informazioni, le minacce presenti attualmente per i sistemi informatici, le funzionalità di sicurezza di determinati sistemi e le procedure di accesso sicuro.

3.4 Porre in essere tutte le azioni ragionevoli atte ad impedire l'accesso da parte di utenti non autorizzati o la perdita di Informazioni riservate e Dati personali, nonché ai servizi, sistemi, dispositivi o supporti che contengono tali informazioni.

3.5 Avvalersi di processi di valutazione del rischio e procedure per l'analisi periodica dei sistemi utilizzati per fornire servizi o prodotti a CWT. Il Fornitore dovrà inoltre eliminare tali rischi non appena sia ragionevolmente possibile e in maniera commisurata al livello di rischio per le Informazioni riservate e i Dati personali, secondo le minacce note al momento dell'identificazione. Il Fornitore dovrà, inoltre, avvalersi di una procedura per mezzo della quale il suo personale possa segnalare i rischi o gli incidenti sospetti al team di sicurezza del Fornitore stesso.

3.6 Laddove il Fornitore sia impegnato nella fornitura di servizi in virtù del Contratto presso le strutture di CWT, o mediante l'utilizzo di servizi, sistemi, dispositivi o supporti di proprietà di CWT o da esso operati o gestiti, dovrà attenersi a tutti i regolamenti di CWT pertinenti all'accesso a tali risorse. Il Fornitore dovrà inoltre inviare tempestivamente a CWT notifica scritta segnalando il fatto che tale accesso non sia più necessario, nella fattispecie e a titolo esemplificativo, qualora un dipendente,

appaltatore, subappaltatore o soggetto terzo del Fornitore abbia cessato la fornitura di servizi ai sensi del Contratto o non debba più accedere alle Informazioni riservate e ai Dati personali.

3.7 Mantenere la documentazione delle proprie risorse che abbiano avuto accesso, trasferito, conservato, archiviato o elaborato Informazioni riservate e Dati personali.

3.8 Soddisfare i requisiti delle referenze di CWT nei termini necessari e consentiti dalla legge e secondo quanto enunciato in una dichiarazione applicabile di impiego/ordine d'impiego/ordine d'acquisto.

4. Sicurezza fisica e ambientale

Il Fornitore dovrà:

4.1 Garantire che tutti i sistemi e le risorse in proprio possesso, destinati all'uso da parte di più utenti, si trovino in luoghi sicuri il cui accesso è limitato e consentito esclusivamente ai soggetti autorizzati.

4.2 Monitorare e documentare, a scopo di verifica, l'accesso alle strutture nelle quali si trovano i sistemi e le altre risorse destinati all'uso da parte di più utenti, utilizzati dal Fornitore stesso per l'adempimento degli obblighi ai sensi del Contratto.

4.3 Garantire che tutto il proprio personale abbia sottoscritto un accordo di non divulgazione o riservatezza prima di accedere alle Informazioni riservate e ai Dati personali.

4.4 Richiedere al proprio personale di rispettare la politica della "scrivania pulita" e di bloccare gli schermi delle proprie stazioni di lavoro prima di allontanarsi da esse.

4.5 Impegnarsi a recuperare tutti i propri beni aziendali al termine dell'impiego o al termine del Contratto.

4.6 Limitare e monitorare l'accesso fisico alle proprie strutture ai sensi dei seguenti requisiti:

a. Ai visitatori è consentito l'accesso previa registrazione. Tale registro deve essere conservato per tre (3) mesi e deve riportare il nome del visitatore, l'azienda che rappresenta e il nome del dipendente che autorizza l'accesso fisico.
b. L'accesso è limitato al personale competente, in base a casi di effettiva necessità per garantire l'espletamento del servizio.
c. Tutti i dipendenti devono indossare la targhetta nominale fornita dall'azienda.
d. L'accesso deve essere revocato immediatamente al termine di esso e tutti i mezzi fisici di accesso, quali chiavi o schede, devono essere restituiti o resi inutilizzabili.
e. Il data center o la sala che contiene i computer devono essere chiusi a chiave e l'accesso deve essere consentito solo agli individui che hanno bisogno dell'accesso per espletare le loro mansioni lavorative.
f. Laddove consentito dalla legge, è richiesto l'utilizzo di telecamere per monitorare l'accesso fisico ad aree sensibili. I dati registrati devono essere analizzati periodicamente. I filmati devono essere conservati per almeno tre (3) mesi.
g. È necessario implementare misure di sicurezza fisiche per le attrezzature utilizzate per archiviare, elaborare o trasmettere Informazioni riservate e Dati personali, quali punti di accesso wireless, gateway, dispositivi portatili, hardware di rete/comunicazione e linee di telecomunicazione.

4.7 Effettuare dei controlli per ridurre al minimo il rischio di minacce fisiche e proteggersi da esse.

4.8 Mantenere tutte le risorse hardware in conformità con i requisiti di manutenzione raccomandati dal service provider terzo.

4.9 Limitare in modo logico l'uso di jack con collegamento alle reti della conference room e di altre reti ad accesso pubblico, restringendone l'uso agli utenti autorizzati oppure disabilitandoli per impostazione predefinita.

4.10 Impedire la manomissione e la sostituzione di qualsiasi dispositivo in grado di acquisire dati su carte di pagamento mediante interazione fisica, impegnandosi a ispezionarlo periodicamente per rivelare la presenza di segni di manomissione o sostituzione. Dovrà altresì formare il personale sensibilizzandolo sulla possibilità di manomissione e sostituzione di tali dispositivi.

4.11 Controllare e separare i punti di accesso, quali le aree di carico e consegna, da tutti i centri presso i quali si esegue l'accesso, la gestione, l'archiviazione o l'elaborazione delle Informazioni riservate e dei Dati personali.

4.12 Provvedere a garantire sistemi di riscaldamento, raffreddamento, rilevamento dell'acqua e di calore/fumo nonché di un impianto antincendio nei data center.

5. Controllo degli accessi

Il Fornitore dovrà:

5.1 Adottare tutte le misure ragionevoli per impedire l'accesso alle Informazioni riservate e ai Dati personali in modalità o per scopi non autorizzati da CWT né previsti dal Contratto. Il Fornitore dovrà inoltre limitare l'accesso alle Informazioni riservate e ai Dati personali esclusivamente al proprio personale che abbia (1) una legittima esigenza di accedere a tali informazioni e dati per fornire servizi ai sensi del Contratto e (2) acconsentito in forma scritta a tutelare l'integrità, la disponibilità e la riservatezza delle Informazioni riservate e dei Dati personali.

5.2 Avvalersi di procedure ragionevoli per terminare l'accesso alle Informazioni riservate e ai Dati personali consentito al personale del Fornitore stesso, qualora tale accesso non sia più necessario o rilevante ai sensi dell'adempimento agli obblighi previsti e prima del termine dell'impiego da parte del Fornitore o dell'impegno contrattuale con CWT.

5.3 Separare le informazioni di proprietà di CWT da qualsiasi altra informazione o applicazione di clienti o del Fornitore stesso, mediante server fisicamente distinti o, in alternativa, mediante il controllo degli accessi logici nel caso in cui i server non siano fisicamente separati.

5.4 Identificare i proprietari idonei e richiedere a questi di esaminare e autorizzare l'accesso ai sistemi utilizzati per l'accesso, l'elaborazione, la gestione o l'archiviazione delle Informazioni riservate e dei Dati personali, nonché tracciare e conservare tali autorizzazioni.

5.5 Eliminare l'accesso ai sistemi di gestione delle Informazioni riservate e dei Dati personali di un dipendente, appaltatore, subappaltatore o soggetto terzo entro 24 ore dall'interruzione del rapporto lavorativo tra questo e il Fornitore, oppure entro tre (3) giorni lavorativi nel caso in cui un dipendente, appaltatore, subappaltatore o terzista assuma mansioni lavorative differenti all'interno dell'azienda. Tutti gli ID degli altri utenti devono essere disabilitati o eliminati dopo 90 giorni solari di inattività.

5.6 Esaminare periodicamente e autorizzare l'accesso ai sistemi di gestione delle Informazioni riservate e dei Dati personali almeno una volta ogni trimestre, per eliminare tutti gli accessi non autorizzati.

5.7 Limitare l'accesso come amministratore di sistema (definito anche come utente root, con privilegi o super utente) ai sistemi operativi destinati all'uso da parte di più utenti, assegnandolo esclusivamente ai soggetti che necessitano di un tale livello di accesso per lo svolgimento delle proprie mansioni lavorative. Utilizzare ID di uscita con le credenziali univoche di login dell'utente e mantenere registri di attività per gestire gli accessi con un elevato livello di sicurezza, altrimenti ridurre tale tipo di accesso concedendolo a un numero estremamente limitato di utenti.

5.8 Richiedere agli amministratori di applicazioni, database, rete e sistemi di consentire agli utenti un accesso limitato ai comandi, ai dati, ai sistemi e alle altre risorse necessarie per eseguire le mansioni cui sono preposti.

5.9 Richiedere metodi di Strong Authentication per accedere da remoto.

5.10 Vietare e mettere in atto Misure di sicurezza tecniche e organizzative per impedire la copia, lo spostamento o l'archiviazione delle Informazioni riservate e dei Dati personali su hard disk locali, nonché le operazioni di copia, incolla o stampa delle Informazioni riservate e dei Dati personali da parte del personale del Fornitore avente accesso a tali informazioni e dati.

5.11 Attivare tali funzionalità solo quando necessario, monitorare il loro utilizzo e disattivarle immediatamente dopo l'uso.

5.12 Prevedere almeno l'autenticazione a due fattori per il collegamento alle risorse interne del Fornitore che contengono Informazioni riservate e Dati personali.

6. Identificazione e autenticazione

Il Fornitore dovrà:

6.1 Assegnare ID univoci a ogni utente e meccanismi di autenticazione a ogni singolo account.

6.2 Utilizzare un processo documentato di gestione del ciclo di vita dell'ID utente che includa, a titolo esemplificativo ma non esaustivo, le procedure per la creazione autorizzata di account, l'eliminazione tempestiva di account e la modifica dell'account (ad esempio, modifica dei privilegi, durata dell'accesso, funzioni/ruoli) per tutti gli accessi alle Informazioni riservate e ai Dati personali e tutti gli ambienti (ad esempio, produzione, testing, sviluppo). Tale processo deve prevedere una revisione periodica dei privilegi di accesso e della validità dell'account, che deve avvenire almeno ogni tre mesi.

6.3 Applicare il principio del privilegio minimo (ad esempio, limitare l'accesso solo ai comandi, alle informazioni, ai sistemi e alle altre risorse necessarie per eseguire le funzioni autorizzate in base alla propria mansione lavorativa).

6.4 Limitare l'accesso alle Informazioni riservate e ai Dati personali a coloro che siano in possesso di un ID utente e una password validi e prevedere che l'ID utente univoco sia associato a una delle seguenti misure: password o passphrase, autenticazione a due fattori o valore biometrico.

6.5 Prevedere che la complessità della password sia conforme ai seguenti requisiti: almeno otto (8) caratteri di lunghezza per password di sistema e quattro (4) caratteri per passcode di tablet e smartphone. Le password di sistema devono inoltre presentare tre (3) tra le seguenti caratteristiche: lettera maiuscola, lettera minuscola, valore numerico o caratteri speciali. Le password non possono

corrispondere all'ID utente al quale sono associate, contenere una parola del dizionario o numeri ripetuti o in sequenza, né corrispondere a una delle ultime cinque password. Richiedere la reimpostazione della password a intervalli regolari e comunque almeno ogni novanta (90) giorni. Visualizzare tutte le password in modalità nascosta.

6.6 Consentire un limite massimo di cinque (5) tentativi di accesso errato ogni 24 ore e bloccare l'account dell'utente se questo raggiunge tale limite in modo ricorrente. L'accesso all'account dell'utente potrà essere riattivato tramite una procedura manuale che richieda la verifica dell'identità dell'utente.

6.7 Verificare l'identità dell'utente e assegnare a ciascun utente one-time password e password di ripristino univoche. Richiedere sistematicamente la modifica della password dopo il primo utilizzo.

6.8 Utilizzare un metodo sicuro per inviare le credenziali di autenticazione (ad esempio, password) e i meccanismi di autenticazione (ad esempio, token o smart card).

6.9 Prevedere che le password dell'account di servizio e del proxy siano composte da almeno 12 caratteri, tra cui lettere maiuscole, lettere minuscole, caratteri numerici e simboli speciali. Cambiare le password dell'account di servizio e del proxy almeno una volta all'anno.

6.10 Dopo un periodo di inattività massimo di quindici (15) minuti, terminare le sessioni interattive o attivare uno screensaver di blocco sicuro che richieda l'autenticazione.

6.11 Ricorrere a un metodo di autenticazione adeguato al grado di sensibilità delle Informazioni riservate e dei Dati personali. In caso di archiviazione delle credenziali di autenticazione, proteggerle con crittografia avanzata.

6.12 Configurare il timeout automatico dei sistemi dopo un periodo massimo di inattività: server (15 minuti), stazioni di lavoro (15 minuti), dispositivi mobili (4 ore), Dynamic Host Configuration Protocol (7 giorni), Virtual Private Network (24 ore).

7. Acquisizione, sviluppo e manutenzione dei sistemi informatici

Il Fornitore dovrà:

7.1 Visualizzare un avvertimento sulle schermate o sulle pagine di accesso, secondo quanto specificato da CWT per iscritto, per i prodotti e i servizi a marchio CWT e per i software sviluppati per CWT.

7.2 Verificare che tutto il personale che potrebbe svolgere mansioni lavorative disciplinate dal Contratto agisca in conformità con le presenti Misure di sicurezza tecniche e organizzative che saranno disposte in un contratto scritto non meno restrittivo dei presenti Requisiti di sicurezza delle informazioni.

7.3 Restituire tutti i dispositivi di accesso ai dati forniti da o di proprietà di CWT il prima possibile, e comunque entro e non oltre quindici (15) giorni da:

(a) il termine previsto o la risoluzione del Contratto;
(b) la richiesta di restituzione da parte di CWT;
(c) la data a partire dalla quale il Fornitore non necessita più di tali dispositivi.

7.4 Applicare una metodologia efficace di gestione delle applicazioni che integri le Misure di sicurezza tecniche e organizzative nel processo di sviluppo del software, garantendo che tali Misure siano

implementate dal Fornitore stesso in modo tempestivo, come definito nel ciclo di vita di sviluppo del software CWT o nei regolamenti, negli standard e nelle procedure di sicurezza delle informazioni.

7.5 Attenersi a procedure standard di sviluppo, che comprendano la separazione di accesso e codice tra ambienti produttivi e non produttivi e la conseguente separazione dei compiti tra tali ambienti.

7.6 Garantire un'analisi regolare dei controlli sulla sicurezza delle informazioni interne per lo sviluppo di software, adeguarsi alle migliori prassi del settore e rivedere e applicare tali controlli in maniera tempestiva.

7.7 Gestire la sicurezza del processo di sviluppo e garantire l'implementazione e il rispetto di prassi di codifica sicure, che comprendano verifiche crittografiche adeguate, protezioni contro i codici malevoli e un processo di peer review.

7.8 Sottoporre le applicazioni funzionalmente complete a test di penetrazione prima di essere messe in produzione e dopo, almeno una volta all'anno e dopo qualsiasi modifica significativa al codice sorgente o alla configurazione che si allinea con OWASP, CERT, SANS Top 25 e PCI-DSS. Porre rimedio a tutte le vulnerabilità sfruttabili prima della distribuzione nell'ambiente produttivo.

7.9 Negli ambienti non produttivi, utilizzare dati resi anonimi o sottoposti a offuscamento. In qualsiasi ambiente non produttivo, non utilizzare mai e per nessun motivo testo in chiaro né Informazioni riservate né Dati personali. Verificare che tutti i dati e gli account creati per i test siano rimossi prima della distribuzione per la produzione.

7.10 Assicurarsi che il Fornitore che ricorre a codice, software, applicazioni o servizi di tipo open source applichino i principi di due diligence nella revisione del codice prodotto, per verificare la presenza di errori, bug o problemi di sicurezza che potrebbero compromettere l'integrità, la disponibilità o la riservatezza dei dati di proprietà di CWT o dei suoi clienti. Il Fornitore dovrà inoltre comunicare a CWT dove il codice open source viene utilizzato e fornire a CWT il nome e la versione del codice open source.

7.11 Assicurarsi che il Fornitore non divulghi, in nessuna circostanza, il codice creato ai sensi del Contratto in qualsiasi fase di sviluppo in ambienti condivisi o non privati, come i repository di codice di tipo Open Access, indipendentemente dalla presenza di una protezione con password.

8. Integrità di software e dati

Il Fornitore dovrà:

8.1 Negli ambienti con software antivirus disponibile in commercio, disporre di un software antivirus aggiornato e installato, in grado di eseguire scansioni dei sistemi e dei dispositivi ed eliminare o mettere rapidamente in quarantena i virus e qualsiasi altro tipo di malware rilevato.

8.2 Separare Le informazioni e le risorse non produttive da quelle produttive.

8.3 Garantire che i team seguano un processo documentato di gestione del cambiamento in caso di qualsiasi modifica al sistema, che comprenda procedure di ripristino delle condizioni per tutti gli ambienti produttivi e processi di cambiamento di emergenza. Prevedere test, documentazione e approvazione per tutti i cambiamenti del sistema e l'approvazione della gestione di cambiamenti significativi in tali processi.

8.4 Realizzare e mantenere un'area PCI qualora il Fornitore elabori o archivi i dati dei titolari di carte di pagamento.

8.5 Nel caso in cui le applicazioni utilizzino un database che permetta la modifica delle Informazioni riservate e dei Dati personali, abilitare e mantenere le funzionalità di registrazione delle transazioni del database a scopo di verifica e conservare tali registri per almeno sei (6) mesi.

8.6 Controllare qualsiasi tipo di software utilizzato, rilasciato e/o al quale è stato fornito il supporto ai sensi del Contratto, per rilevare e risolvere eventuali vulnerabilità in materia di sicurezza.

8.7 Sottoporre i componenti di sicurezza (ad esempio, test delle funzionalità di identificazione, autenticazione autorizzazione), e qualsiasi altra attività necessaria per la convalida dell'architettura di sicurezza, a test di garanzia di qualità durante la prima implementazione e dopo modifiche significative e aggiornamenti.

9. <u>Sicurezza del sistema</u>

Il Fornitore dovrà:

9.1 Creare e aggiornare periodicamente le versioni più recenti del flusso di dati e degli schemi di sistema usati per l'accesso, l'elaborazione, la gestione o l'archiviazione delle Informazioni riservate e dei Dati personali.

9.2 Monitorare attentamente le risorse del settore (ad esempio,, www.cert.org e mailing list e siti web dei fornitori di software) per un aggiornamento tempestivo circa tutti gli avvertimenti di sicurezza relativi ai sistemi del Fornitore e ad altre risorse di informazioni.

9.3 Gestire in maniera efficace le chiavi crittografiche, limitandone l'accesso al minor numero possibile di persone, archiviando le chiavi crittografiche segrete e private solo dopo averle cifrate, a loro volta, con una chiave almeno tanto forte quanto quella di crittografia dei dati e memorizzandole in maniera separata rispetto a questa in un dispositivo sicuro dal punto di vista crittografico e nel minor numero possibile di posizioni. Cambiare la chiave crittografica predefinita al momento dell'installazione e almeno una volta ogni due anni. Eliminare definitivamente le chiavi obsolete.

9.4 Scansionare i sistemi e altre risorse di informazioni rivolti verso l'esterno, compresi, a titolo esemplificativo ma non esaustivo, reti, server e applicazioni, utilizzando un software di rilevamento delle vulnerabilità della sicurezza che corrisponda allo standard di settore per rilevare vulnerabilità della sicurezza almeno una volta ogni tre mesi, e prima del rilascio di applicazioni e cambiamenti o aggiornamenti significativi, secondo tempistiche determinate da un'analisi dei rischi basata su politiche e standard informatici ragionevoli e generalmente accettati.

9.5 Scansionare i sistemi e altre risorse di informazioni interni, compresi, a titolo esemplificativo ma non esaustivo, reti, server, applicazioni e database, utilizzando un software di rilevamento delle vulnerabilità della sicurezza che corrisponda allo standard di settore. Accertarsi, successivamente, che tali sistemi e risorse siano opportunamente rafforzati e individuare eventuali reti wireless non autorizzate almeno una volta ogni tre mesi, e prima del rilascio di applicazioni e cambiamenti o aggiornamenti significativi, secondo tempistiche determinate da un'analisi dei rischi basata su politiche e standard informatici ragionevoli e generalmente accettati.

9.6 Dotarsi di una procedura di valutazione del rischio per analizzare i risultati della valutazione della vulnerabilità in base alle migliori pratiche del settore e al potenziale impatto. Tutti i risultati con un

punteggio CVSS pari a 4 o superiore devono essere risolti mediante un metodo formalizzato per assicurare che venga gestita la continuità della valutazione del rischio.

9.7 Garantire che tutti i sistemi e le altre risorse del Fornitore siano rafforzati e rimangano tali, ricorrendo a procedure quali la rimozione o la disabilitazione di reti, servizi e prodotti non utilizzati [ad esempio, finger, rlogin, ftp e semplici servizi e prodotti di tipo Transmission Control Protocol/Internet Protocol (TCP/IP)] e l'installazione di un firewall di sistema, involucri Transmission Control Protocol (TCP) o tecnologie simili.

9.8 Distribuire uno o più sistemi di tipo Intrusion Detection System (IDS), Intrusion Prevention System (IPS) o Intrusion Detection and Prevention System (IDP), in una modalità operativa abilitata e in grado di monitorare tutto il traffico in entrata e in uscita dal sistema e dalle altre risorse interessate dal Contratto negli ambienti con tale tecnologia disponibile in commercio e nella misura ragionevolmente possibile.

9.9 Mantenere un processo di valutazione del rischio per la risoluzione delle vulnerabilità della sicurezza in qualsiasi sistema o altra risorsa, che comprenda, a titolo esemplificativo ma non esaustivo, tutte le problematiche evidenziate da pubblicazioni di settore, da scansioni per il rilevamento di vulnerabilità o virus e dall'esame dei registri di sicurezza. Applicare tempestivamente le patch di sicurezza necessarie, in base alla probabilità per la quale la vulnerabilità rilevata possa essere o sia già stata sfruttata. Le patch critiche, con un punteggio CVSS pari a 7,5 o superiore, devono essere installate non appena disponibili ed entro e non oltre un mese dalla data di pubblicazione. Le patch con un punteggio CVSS pari a 4 o superiore devono essere installate entro 90 giorni dalla data di pubblicazione.

9.10 Effettuare test di penetrazione generalizzati a livello interno ed esterno almeno una volta all'anno e dopo qualsiasi modifica o aggiornamento significativi alle infrastrutture o alle applicazioni.

9.11 Rimuovere o disabilitare il software non autorizzato rilevato nei sistemi del Fornitore e ricorrere a controlli della presenza di malware conformi agli standard del settore, che comprendano l'installazione, l'aggiornamento periodico e l'uso regolare di software anti-malware su tutti i servizi, sistemi e dispositivi che potrebbero essere utilizzati per accedere alle Informazioni riservate e ai Dati personali. Ricorrere a software antivirus affidabile e corrispondente alle migliori prassi del settore, se fattibile, e accertarsi che le definizioni di virus siano sempre aggiornate.

9.12 Mantenere aggiornato il software di tutti i servizi, sistemi e dispositivi che potrebbero essere utilizzati per accedere alle Informazioni riservate e ai Dati personali, prevedendo una manutenzione adeguata dei sistemi operativi e l'installazione effettiva di patch di sicurezza ragionevolmente aggiornate.

9.13 Assegnare le responsabilità di amministratore della sicurezza a determinati soggetti, che saranno quindi incaricati della configurazione dei sistemi operativi host.

9.14 Cambiare tutti i nomi predefiniti degli account e/o le password predefinite.

10. Monitoraggio

Il Fornitore dovrà:

10.1 Conservare i dati dei registri relativi alle Informazioni riservate e ai Dati personali per almeno 12 mesi e garantire che siano trasmessi a CWT, previa richiesta, in un tempo ragionevole, a meno che diversamente specificato nel Contratto.

10.2 Registrare le attività del sistema primario per sistemi che contengono Informazioni riservate e Dati personali.

10.3 Limitare l'accesso ai registri di sicurezza solo ai soggetti autorizzati e proteggerli contro modifiche non autorizzate.

10.4 Implementare un meccanismo di rilevamento dei cambiamenti (ad esempio, monitoraggio dell'integrità dei file) che avverta il personale in caso di modifiche non autorizzate ai file critici di sistema, di configurazione o di contenuto; configurare un software che effettui il confronto dei file critici su base settimanale.

10.5 Esaminare, almeno una volta alla settimana, tutti i registri di verifica relativi alla sicurezza dei sistemi che contengono Informazioni riservate e Dati personali, per rilevare eventuali anomalie. Documentare e risolvere in maniera tempestiva tutte le problematiche di sicurezza rilevate.

10.6 Esaminare quotidianamente tutti gli eventi relativi alla sicurezza, i registri dell'archiviazione, dell'elaborazione o della trasmissione dei dati dei titolari di carte di pagamento da parte dei componenti del sistema, i registri dei componenti critici del sistema e dei componenti di server e sistema adibiti alle funzionalità di sicurezza.

11. Gateway di sicurezza

Il Fornitore dovrà:

11.1 Richiedere metodi di Strong Authentication per eseguire l'accesso come amministratore e/o gestore ai gateway di sicurezza, ad esempio allo scopo di esaminare i file di registro.

11.2 Avvalersi di e utilizzare controlli, regolamenti, processi e procedure documentati per negare l'accesso come amministratore e/o gestore ai gateway di sicurezza a tutti gli utenti non autorizzati e assegnare i livelli di autorizzazione come amministratore e gestore dei gateway di sicurezza in maniera adeguata.

11.3 Accertarsi, almeno una volta ogni sei (6) mesi, che le configurazioni dei gateway di sicurezza siano rafforzate, scegliendo un campione di gateway di sicurezza e verificando che ogni set di regole predefinite e di parametri di configurazione assicuri le seguenti condizioni:

a. il source routing dell'Internet Protocol (IP) è disabilitato;
b. l'indirizzo di loopback non può entrare nella rete interna;
c. i filtri anti-spoofing sono stati implementati;
d. i pacchetti di broadcast non possono entrare nella rete;
e. il reindirizzamento dell'Internet Control Message Protocol (ICMP) è disabilitato;
f. tutti i set di regole terminano con la dichiarazione "DENY ALL";
g. tutte le regole sono ricollegabili a una richiesta aziendale.

11.4 Garantire l'utilizzo di strumenti di monitoraggio per verificare che ogni elemento del gateway di sicurezza (ad esempio, hardware, firmware e software) sia costantemente in funzione.

11.5 Configurare e implementare i gateway di sicurezza in modo tale da garantire che tutti i gateway di sicurezza non in funzione neghino qualsiasi tipo di accesso.

11.6 I pacchetti in entrata dalla rete esterna non sicura devono terminare presso la DMZ, senza la possibilità di essere trasmessi direttamente attraverso la rete interna sicura. Tutti i pacchetti in entrata che raggiungono la rete interna sicura devono essere originati esclusivamente all'interno della DMZ. La DMZ deve pertanto essere separata dalla rete esterna non sicura mediante un gateway di sicurezza e da quella interna sicura per mezzo di:

a. un altro gateway di sicurezza; oppure
b. lo stesso gateway di sicurezza che separa la DMZ dalla rete esterna non sicura, il quale deve procedere all'eliminazione immediata dei pacchetti ricevuti dalla rete esterna non sicura, oppure all'instradamento di questi verso la DMZ, senza altra elaborazione possibile senza non la memorizzazione di tali pacchetti in entrata in un registro.

I seguenti elementi devono trovarsi esclusivamente all'interno della rete interna sicura:

a. tutte le Informazioni riservate e i Dati personali archiviati senza ricorrere a crittografia avanzata;
b. la copia autentica di informazioni alle quali è possibile accedere da richieste originate dalla rete esterna non sicura;
c. la copia autentica di informazioni che possono essere modificate in seguito a richieste originate dalla rete esterna non sicura;
d. i server dei database;
e. tutti i registri esportati; e
f. tutti gli ambienti usati a scopo di sviluppo, test, sandbox, produzione e ambienti di natura simile; tutte le versioni del codice sorgente.

11.7 Le credenziali di autenticazione non protette da crittografia avanzata non devono essere collocate nella DMZ.

12. Sicurezza di rete

Il Fornitore dovrà:

12.1 Previa richiesta da parte di CWT, fornire a CWT uno schema logico di rete che documenti i sistemi e le connessioni ad altre risorse, quali router, switch, firewall, sistemi IDS, topologia di rete, punti di connessione esterni, gateway, reti wireless e qualsiasi altro dispositivo che supporti CWT.

12.2 Adottare una procedura formale per l'approvazione, il test e la documentazione di tutte le connessioni di rete e le modifiche alle configurazioni di firewall e router. Configurare i firewall in modo che rifiutino e registrino tutti i pacchetti sospetti e consentano l'accesso esclusivamente al traffico adeguato e autorizzato, bloccando l'intero traffico restante. Rivedere le regole dei firewall ogni sei mesi.

12.3 Installare un firewall per ciascuna connessione Internet e tra la DMZ e la rete interna. Tutti i sistemi di archiviazione delle Informazioni riservate e dei Dati personali devono trovarsi nella rete interna, separati dalla DMZ e da qualsiasi altra rete non sicura.

12.4 Monitorare i firewall internamente e ai confini della rete interna per controllare e proteggere il flusso del traffico di rete in entrata o in uscita dal bordo o limite, se necessario.

12.5 Mantenere una procedura documentata e porre in essere i controlli necessari per rilevare e gestire i tentativi di accesso non autorizzato alle Informazioni riservate e ai Dati personali.

12.6 Nell'ambito della fornitura di servizi e prodotti basati su Internet a CWT, proteggere le Informazioni riservate e i Dati personali implementando una DMZ di rete. I server web che forniscono servizi a CWT devono trovarsi nella DMZ. Ogni sistema o risorsa di informazioni sui quali siano archiviati le Informazioni riservate e i Dati personali (ad esempio, server di applicazioni e database) devono trovarsi in una rete interna sicura (i servizi e prodotti basati su Internet devono utilizzare la DMZ).

12.7 Limitare il traffico non autorizzato in uscita dalle applicazioni che risulti nell'elaborazione, l'archiviazione o la trasmissione di Informazioni riservate e Dati personali a indirizzi IP all'interno della DMZ e della rete Internet.

12.8 Quando utilizza tecnologie di rete wireless a radiofrequenza (RF) per la fornitura o il supporto di servizi e prodotti per CWT, garantire che tutte le Informazioni riservate e i Dati personali trasmessi siano protetti mediante tecnologie crittografiche sufficienti a tutelare la riservatezza di tali Informazioni riservate e Dati personali. Scansionare, individuare e disabilitare periodicamente tutti i punti di accesso wireless non autorizzati.

13. Requisiti di connettività

Il Fornitore dovrà:

13.1 Nel caso in cui il Fornitore fornirà, o riceverà in fornitura, connettività alle risorse contenenti Informazioni riservate o Dati personali, in relazione a quanto disposto nel Contratto, impegnarsi a:

a. Ricorrere esclusivamente alle strutture e ai metodi di connessione concordati per collegare le risorse contenenti Informazioni riservate e Dati personali alle risorse del Fornitore.
b. Non stabilire alcuna connessione alle risorse contenenti Informazioni riservate e Dati personali, senza aver ricevuto il consenso preventivo da parte di CWT.
c. Garantire a CWT l'accesso alle strutture del Fornitore durante l'orario lavorativo a scopo di manutenzione e supporto delle apparecchiature (ad esempio, router) fornite da CWT ai sensi dell'accordo sulla connessione alle risorse contenenti Informazioni riservate e Dati personali.
d. Utilizzare le apparecchiature fornite da CWT ai sensi dell'accordo sulla connessione alle risorse contenenti Informazioni riservate e Dati personali solo ed esclusivamente per la fornitura di servizi, prodotti e funzioni espressamente autorizzati nel Contratto.
e. Qualora il metodo di connessione concordato preveda l'implementazione di un gateway di sicurezza da parte del Fornitore, questo deve registrare tutte le sessioni che utilizzano tale gateway di sicurezza. I registri delle sessioni devono comprendere informazioni sufficientemente dettagliate, tali da identificare l'utente finale o l'applicazione, l'indirizzo IP di origine, l'indirizzo IP di destinazione, le porte o i protocolli di servizio utilizzati e la durata dell'accesso. Tali registri devono essere conservati per almeno sei (6) mesi dalla creazione della sessione.

13.2 Oltre ai diritti definiti nel presente documento, nel caso in cui il Fornitore fornirà, o riceverà in fornitura, connettività alle risorse contenenti Informazioni riservate e Dati personali, in relazione a quanto disposto nel Contratto, esso dovrà consentire a CWT di:

a. Raccogliere informazioni sugli accessi, effettuati anche dal Fornitore, alle risorse contenenti Informazioni riservate e Dati personali. CWT potrà raccogliere, conservare e analizzare tali informazioni, senza ulteriore preavviso, allo scopo di individuare potenziali rischi per la sicurezza. Tali informazioni potranno comprendere file di traccia, statistiche e indirizzi di rete, nonché i dati o le schermate trasferiti o ai quali si ha effettivamente avuto accesso.
b. Interrompere o terminare immediatamente qualsiasi connessione alle risorse contenenti Informazioni riservate e Dati personali, a propria discrezione, in caso di sospetto di violazione alla

sicurezza, oppure accesso o utilizzo non autorizzati di strutture dati, informazioni, sistemi o altre risorse di sua proprietà.

14. Dispositivi mobili e portatili

Il Fornitore dovrà:

14.1 Ricorrere alla crittografia avanzata per proteggere tutte le Informazioni riservate e i Dati personali archiviati su dispositivi mobili e portatili.

14.2 Non archiviare alcuna Informazione riservata e Dato personale su dispositivi mobili o computer portatili, né memorizzare Informazioni riservate e Dati personali su dispositivi rimovibili, senza proteggere tali dati mediante crittografia avanzata.

14.3 Ricorrere alla crittografia avanzata per proteggere tutte le Informazioni riservate e i Dati personali trasmessi o ai quali si è avuto accesso mediante dispositivi mobili e portatili con funzionalità di rete:

a. Qualora si utilizzino dispositivi mobili e portatili con funzionalità di rete, diversi da computer portatili, per archiviare e/o accedere alle Informazioni riservate e ai Dati personali, tali dispositivi devono essere in grado di eliminare tutte le copie di tali informazioni e dati archiviati, dopo aver ricevuto via rete un comando adeguatamente autenticato (nota: tale funzionalità è definita anche “remote wipe”).
b. Adottare regolamenti, procedure e standard documentati per garantire che il soggetto autorizzato che dovrebbe controllare fisicamente un dispositivo mobile e portatile con funzionalità di rete, diverso da un computer portatile, utilizzato per archiviare le Informazioni riservate e i Dati personali, avvii tempestivamente l’eliminazione di tutte le informazioni e dei dati in caso di furto o smarrimento di tale dispositivo.
c. Adottare regolamenti, procedure e standard documentati per garantire che i dispositivi mobili e portatili, diversi da computer portatili, sprovvisti di funzionalità di rete, procedano all’eliminazione automatica di tutte le copie delle Informazioni riservate e dei Dati personali dopo tentativi di accesso consecutivi con esito negativo.

14.4 Adottare regolamenti, procedure e standard documentati per garantire che i dispositivi mobili e portatili utilizzati per archiviare e/o accedere alle Informazioni riservate e ai Dati personali:

a. siano fisicamente posseduti da soggetti autorizzati;
b. siano posti in luoghi sicuri quando non si trovano fisicamente in possesso dei soggetti autorizzati;
c. siano sottoposti all’eliminazione tempestiva e sicura di tutti i dati archiviati quando non si trovano fisicamente in possesso dei soggetti autorizzati, non sono posti in un luogo sicuro, oppure dopo 10 tentativi di accesso con esito negativo.

14.5 Prima di consentire l'accesso alle Informazioni riservate e dai Dati personali archiviati su dispositivi mobili o portatili, o mediante l'utilizzo di essi, adottare e utilizzare una specifica procedura volta a garantire:

a. l’autorizzazione dell’accesso da parte dell’utente; e
b. l’autenticazione dell’identità dell’utente.

14.6 Applicare un regolamento che vieti l'archiviazione e/o l'accesso a Informazioni riservate e Dati personali mediante dispositivi mobili o portatili che non siano amministrati e/o gestiti dal Fornitore o da CWT.

14.7 Rivedere, almeno una volta all'anno, le procedure di utilizzo e di controllo di tutti i dispositivi mobili e portatili amministrati o gestiti dal Fornitore, per garantirne la conformità alle Misure di sicurezza tecniche e organizzative applicabili.

15. Sicurezza durante il trasporto

Il Fornitore dovrà:

15.1 Ricorrere alla crittografia avanzata per trasportare le Informazioni riservate e i Dati personali all'esterno delle reti controllate dal Fornitore o da CWT stesso, oppure in caso di trasmissione di tali informazioni e dati tramite reti non sicure.

15.2 La documentazione contenente Informazioni riservate e Dati personali conservata in formato cartaceo, su microfiche o supporti elettronici fisicamente trasferibili dovrà essere trasportata mediante servizi di corriere verificati o altri metodi tracciabili di consegna e imballata in modo sicuro, secondo le specifiche del fabbricante. Tutte le Informazioni riservate e i Dati personali dovranno essere trasportati in contenitori sigillati.

16. Sicurezza durante l'archiviazione

Il fornitore dovrà:

16.1 Ricorrere alla crittografia avanzata per proteggere tutte le Informazioni riservate e i Dati personali durante l'archiviazione.

16.2 Non archiviare le Informazioni riservate e i Dati personali in formato elettronico all'esterno del proprio ambiente di rete (o della rete informatica sicura di CWT) solo se il dispositivo di archiviazione (ad esempio, nastro di backup, computer portatile, scheda di memoria, hard disk) è protetto mediante crittografia avanzata.

16.3 Nonarchiviare le Informazioni riservate e i Dati personali su supporti rimovibili (ad esempio, flash drive, chiavette USB, schede di memoria, nastri, CD o hard disk esterni), fatta eccezione per i seguenti casi: (a) in caso di backup, gestione della continuità operativa, ripristino d'emergenza e scambio di dati, nei termini consentiti e previsti dal Contratto, e (b) utilizzando una protezione mediante crittografia avanzata.

16.4 Archiviare adeguatamente e mettere al sicuro la documentazione in formato cartaceo o su microfiche, contenente Informazioni riservate e Dati personali, collocandola in aree con accesso consentito esclusivamente al personale autorizzato.

16.5 Salvo diversa indicazione espressa da CWT in forma scritta, il Fornitore, al momento della raccolta o della creazione di Informazioni riservate e di Dati personali in formato cartaceo o su supporti di backup eseguita, per mezzo di o per conto di CWT, oppure sotto il marchio CWT, dovrà garantire che tali informazioni corrispondano esattamente alle Informazioni riservate e ai Dati personali e, ove possibile, contrassegnarle come "riservate". Il Fornitore riconosce che le Informazioni riservate e i Dati personali rimarranno in possesso di CWT, indipendentemente da qualunque tipo di contrassegno o di assenza dello stesso.

17. Reso, distruzione e smaltimento

Il fornitore dovrà:

17.1 Fornire copie di qualsiasi Informazione riservata e Dato personale a CWT stessa entro trenta (30) giorni dalla richiesta e senza alcun onere aggiuntivo a carico di CWT. Il Fornitore dovrà, altresì, restituire o distruggere, a discrezione di CWT, qualsiasi informazione riservata o dato personale, comprese eventuali copie elettroniche o cartacee, secondo quanto indicato del Contratto o, nel caso non sia indicato nel Contratto, entro novanta (90) giorni in seguito all'evento, tra i seguenti, che si verifica prima: (a) termine previsto o risoluzione del Contratto, (b) richiesta da parte di CWT di restituzione delle proprie Informazioni riservate e Dati personali, oppure (c) data in cui il Fornitore non necessita più di tali Informazioni riservate e Dati personali per fornire i servizi e i prodotti disciplinati dal Contratto.

17.2 Nel caso in cui CWT autorizzi la distruzione come alternativa alla restituzione di Informazioni riservate e Dati personali, fornire prova scritta delle azioni volte a rendere irrecuperabili le Informazioni riservate e i Dati personali.Distruggere completamente ogni copia delle Informazioni riservate e dei Dati personali di CWT conservata in qualsiasi luogo e sistema di archiviazione, compresi, a titolo esemplificativo ma non esaustivo, luoghi e sistemi di proprietà dei Soggetti Terzi precedentemente autorizzati dal Fornitore stesso. Tale attività dovrà avvenire mediante una procedura standard di settore che assicuri la distruzione completa dei dati, come, ad esempio, gli standard DOD 5220.22M o NIST Special Publication 800-88, oppure utilizzando un prodotto per la demagnetizzazione dei sistemi interessati consigliato dal fabbricante. Prima di distruggere i dati, applicare tutte le Misure di sicurezza tecniche e organizzative pertinenti per tutelare la sicurezza, la privacy e la riservatezza delle Informazioni riservate e dei Dati personali.

17.3 Smaltire le Informazioni riservate e i Dati personali in modo tale che non possano essere recuperati e resi utilizzabili. La documentazione su carta, diapositive, microfilm, microfiche e pellicola fotografica dovrà essere bruciata o distrutta tramite triturazione incrociata. I materiali contenenti Informazioni riservate e Dati personali in attesa di distruzione possono essere riposti in contenitori sicuri e trasportati mediante un soggetto terzo verificato.

18. Mantenimento della documentazione

Il fornitore dovrà:

18.1 Verificare con il proprio referente CWT gli opportuni requisiti di conservazione dei dati prima di acquisire qualsiasi informazione riservata o dato personale, ai fini di una dichiarazione di prestazione d'opera o di un ordine di acquisto.

18.2 Proteggere le copie di backup delle Informazioni riservate e dei Dati personali che vengono creati automaticamente dai servizi, sistemi, dispositivi o supporti del Fornitore stesso ("**Copie d'archivio**"). Se non diversamente specificato nel Contratto, entro 90 giorni solari dal termine previsto o dalla risoluzione del Contratto, oppure precedentemente, previa richiesta ragionevole da parte di CWT, distruggere definitivamente tutte le Copie d'archivio delle Informazioni riservate e dei Dati personali, impiegando una procedura standard di settore non meno stringente rispetto agli standard DOD 5220.22M o NIST Special Publication 800-88.

19. Risposta di emergenza e obblighi di notifica

Il Fornitore dovrà:

19.1 Adottare e applicare un Processo di gestione degli incidenti e tutte le procedure correlate, assegnando le responsabilità di tale Processo di gestione degli incidenti e delle relative procedure a personale qualificato. Immediatamente e, in ogni caso, non oltre ventiquattro (24) ore, inviare una notifica a CWT nel caso in cui si verifichi o si sospetti l'attacco, l'intrusione, l'accesso non autorizzato,

la perdita o qualsiasi altro incidente a danno dei dati, dei sistemi e di altre risorse di proprietà di CWT.

19.2 In seguito a tale notifica, aggiornare periodicamente CWT, menzionando, ad esempio, le azioni intraprese per risolvere l'incidente, a intervalli concordati per tutta la durata dell'incidente e quanto prima in seguito alla risoluzione di questo, nonché inviare a CWT una relazione scritta che descriva l'incidente, le azioni intraprese dal Fornitore in risposta e il piano di quest'ultimo per implementare azioni volte ad evitare incidenti simili in futuro.

19.3 Non riportare né diffondere notizia di tale violazione ai dati, ai sistemi e ad altre risorse di proprietà di CWT senza prima aver opportunamente avvisato CWT e collaborato direttamente con questa per segnalare l'evento all'amministrazione locale, statale o regionale di competenza o ai servizi di monitoraggio del credito, ai soggetti direttamente interessati da tale violazione e ai mezzi di comunicazione opportuni, secondo quanto stabilito dalle normative.

19.4 Disporre di un processo per l'identificazione tempestiva delle violazioni ai controlli sulla sicurezza, che comprenda quanto stabilito nei presenti Requisiti di sicurezza delle informazioni. Tale processo dovrà essere applicato da personale alle dipendenze del Fornitore. Il personale del Fornitore individuato sarà soggetto alle azioni disciplinari opportune, secondo quanto stabilito dalle normative pertinenti. In deroga alle disposizioni precedenti, il personale del Fornitore resterà sotto l'autorità del Fornitore stesso. CWT non sarà considerata il datore di lavoro del personale del Fornitore.

20. Gestione della continuità operativa e ripristino d'emergenza

Il Fornitore dovrà:

20.1 Sviluppare, applicare, gestire e rivedere i piani di gestione della continuità operativa e di ripristino d'emergenza per ridurre al minimo le conseguenze sui servizi o prodotti offerti dal Fornitore a CWT. I suddetti piani devono comprendere i nomi del personale specifico che ricopra le funzioni di gestione della continuità operativa e ripristino d'emergenza, gli obiettivi prestabiliti in relazione al tempo e al punto di ripristino, il backup giornaliero di dati e sistemi, l'archiviazione in strutture esterne dei supporti di backup e della documentazione, i piani di protezione della documentazione e di contingenza commisurati ai termini del Contratto, essere archiviati in strutture sicure ed esterne dallo stabilimento del Fornitore e risultare accessibili al Fornitore in caso di bisogno.

20.2 Fornire a CWT, previa richiesta da parte di questa, un piano di gestione della continuità operativa documentato, che garantisca la capacità del Fornitore di adempiere ai propri obblighi contrattuali, nonché di rispettare i requisiti delle dichiarazioni di prestazione d'opera e degli accordi sul livello del servizio pertinenti. Il ripristino previsto dai suddetti piani dovrà tutelare l'integrità e la segretezza delle Informazioni riservate e dei Dati personali.

20.3 Adottare procedure documentate per il backup e il ripristino sicuri delle Informazioni riservate e dei Dati personali, che dovranno comprendere, almeno, le procedure per il trasporto, l'immagazzinamento e lo smaltimento delle copie di backup delle Informazioni riservate e dei Dati personali e, previa richiesta da parte di questa, fornire suddette procedure documentate a CWT stessa.

20.4 Garantire che il backup di tutte le Informazioni riservate e dei Dati personali archiviati e di tutti i software e le configurazioni dei sistemi utilizzati da CWT venga effettuato con cadenza almeno settimanale.

20.5 Simulare periodicamente e a proprie spese l'applicazione dei piani di gestione della continuità operativa e di ripristino d'emergenza, con cadenza almeno annuale o in seguito a qualsiasi modifica sostanziale dei piani stessi. Tali simulazioni sono volte a garantire il funzionamento adeguato delle tecnologie interessate e a favorire la conoscenza dei piani da parte del personale interno.

20.6 Rivedere tempestivamente il proprio piano di gestione della continuità operativa affinché includa la risoluzione di minacce o situazioni aggiuntive o non previste in precedenza e inviare a CWT una sintesi ad alto livello dei piani e dello svolgimento dei test entro un ragionevole periodo, in seguito alla richiesta da parte di CWT.

20.7 Garantire che tutte le strutture di proprietà del Fornitore o da questo prese in locazione per l'archiviazione o l'elaborazione delle Informazioni riservate e dei Dati personali siano sottoposti a monitoraggio contro eventuali intrusioni, incendi, allagamenti e altri rischi ambientali 24 ore su 24.

21. Conformità e accreditamenti

Il fornitore dovrà:

21.1 Conservare la documentazione completa e accurata relativa all'adempimento degli obblighi risultanti dai presenti Requisiti di sicurezza delle informazioni e della conformità al presente documento, in un formato tale da consentirne la valutazione o la verifica per un periodo non inferiore a tre (3) anni o superiore, se così previsto in virtù di un provvedimento giudiziario o di un procedimento civile o amministrativo. In deroga alle disposizioni precedenti, il Fornitore dovrà conservare i registri di sicurezza per almeno sei (6) mesi dopo l'esecuzione del Contratto.

21.2 CWT potrà, senza alcun onere e previa notifica con ragionevole anticipo, sottoporre le Misure di sicurezza tecniche e organizzative del Fornitore a valutazioni o verifiche periodiche di sicurezza, durante le quali CWT consegnerà al Fornitore questionari scritti e richieste per l'ottenimento della documentazione. Per tutte le richieste, il Fornitore dovrà inoltre rispondere immediatamente in forma scritta e fornendo prove, se possibile, oppure secondo quanto concordato tra le parti. In seguito alla richiesta di verifica formulata da CWT, il Fornitore dovrà programmare una verifica sulla sicurezza entro dieci (10) giorni lavorativi dalla richiesta. CWT potrà richiedere l'accesso alle strutture, ai sistemi, ai processi o alle procedure, al fine di valutare l'ambiente di controllo della sicurezza implementato dal Fornitore.

21.3 Previa richiesta da parte di CWT, dichiarare che il Fornitore sta agendo in conformità con il presente documento e con le certificazioni delle versioni più recenti degli standard PCI-DSS, ISO 27001/27002, SOC 2 o simili, attribuite al Fornitore. Qualora il Fornitore non sia in grado di garantire una certificazione di conformità, dovrà fornire una relazione scritta che specifichi le aree di non conformità e il piano d'azione per diventare ottemperante.

21.4 Nel caso in cui CWT, a propria discrezione, reputi che si sia verificata una violazione alla sicurezza che non sia stata notificata a CWT, secondo quanto previsto da questo documento e dal processo di gestione degli incidenti del Fornitore, quest'ultimo dovrà prevedere l'inizio della verifica o della valutazione entro ventiquattro (24) ore dal ricevimento della richiesta di CWT di esecuzione delle stesse.

21.5 Entro trenta (30) giorni solari dal ricevimento del risultato della valutazione o della relazione della verifica, inviare a CWT una relazione scritta, che delinei le azioni correttive intraprese o proposte, indicandone le tempistiche e lo stato attuale di ciascuna. Fornire a CWT aggiornamenti circa tale relazione ogni trenta (30) giorni solari, segnalando lo stato di tutte le azioni correttive, fino alla data di implementazione delle stesse. Implementare tutte le azioni correttive entro novanta (90) giorni

dal ricevimento della relazione della valutazione o della verifica, oppure entro un periodo di tempo alternativo, purché tale periodo sia stato concordato in forma scritta dalle parti entro trenta (30) giorni dal ricevimento della relazione della valutazione o della verifica.

21.6 Attenersi a tutti gli standard di sicurezza delle informazioni e i requisiti di segnalazione stabiliti imposti a livello governativo, nonché allo standard ISO 27001/27002. Laddove debba gestire i numeri di conti di pagamento e qualsiasi altro dato di pagamento, dovrà attenersi alla versione più recente dello standard Payment Card Industry (PCI-DSS) per l'intera durata della gestione di tali dati mediante i propri sistemi. Nel caso in cui non risulti più conforme allo standard PCI-DSS durante il periodo di gestione dei dati disciplinati dal PCI mediante i propri sistemi, il Fornitore dovrà segnalarlo tempestivamente a CWT, procedere immediatamente, senza ingiustificato ritardo, a porre rimedio a tale situazione e aggiornare periodicamente CWT circa le azioni di rimedio, previa richiesta da parte di questa.

22. Modelli, migliori pratiche, regolamenti e normative

Il Fornitore dovrà:

Laddove il Fornitore effettui l'elaborazione, l'accesso, la visualizzazione, l'archiviazione o la gestione di Informazioni riservate e Dati personali, riguardanti il personale, i soci e le Consociate di CWT, i suoi clienti o i dipendenti, gli appaltatori o i subappaltatori dei clienti di CWT, applicare Misure di sicurezza tecniche e organizzative non meno stringenti delle linee guida, dei regolamenti, delle direttive e delle normative vigenti a livello globale, regionale, nazionale e locale.

23. Emendamenti

CWT si riserva il diritto di aggiornare o emendare i presenti Requisiti di sicurezza delle informazioni e di pubblicarne la versione più aggiornata sul proprio sito web.

Versione 2.0

Data : 15 Dicembre 2017