Indice

1. INTRODUZIONE E AMBITO DI APPLICAZIONE

Nel presente documento vengono indicati i principi e i comportamenti che ogni fornitore deve rispettare durante le fasi di fornitura, nonché l'insieme dei requisiti di sicurezza di base riguardo eventuali utilizzi e accessi alle informazioni di InfoTecna nell'ambito dei lavori intrapresi da un fornitore di InfoTecna. Tali requisiti vengono classificati secondo 3 livelli.

I requisiti del 1° livello, di cui alla sezione 3, fanno riferimento ai fornitori che eseguiranno i lavori essendo in possesso di informazioni limitate e di un accesso limitato ai sistemi amministrativi e alle reti di InfoTecna. I fornitori che rientrano in questa categoria non saranno tenuti a conformarsi agli altri requisiti disposti nel presente documento.

Le sezioni 4-7 del 2° livello sono obbligatorie per tutte le altre tipologie di lavori.

Per quanto riguarda il 3° livello, a seconda dell'ambito dei lavori potrebbero essere applicabili uno o più requisiti contenuti nelle sezioni 8-18. In caso di dubbio, rivolgersi al proprio rappresentante dell'approvvigionamento InfoTecna.

2. PRINCIPI NON DEROGABILI DURANTE TUTTA LA FASE DI FORNITURA

Durante tutta la fase di fornitura, il fornitore deve:

- Operare nel costante e rigoroso rispetto delle leggi e delle normative vigenti;
- Rispettare valori e parametri di obiettività, imparzialità, correttezza nel giudizio ed equità;
- Predisporre in modo corretto le offerte;
- Non denigrare I concorrenti;
- Garantire la conformità dei beni e servizi venduti rispetto a quanto previsto nell'ordine di acquisto di InfoTecna;
- Predisporre tutti i documenti necessari (DDT trasporto, eventuali documenti doganali ecc...);
- Garantire la congruità tra il valore del bene/servizio venduto e il corrispettivo ricevuto.

Oltre ai principi appena richiamati, **il fornitore deve garantire la tracciabilità, la presenza dei documenti obbligatori e la veridicità di essi**.

3. SICUREZZA DELLE INFORMAZIONI IN CASO DI ACCESSO LIMITATO

L'osservanza della sezione 3 costituisce l'unico requisito applicabile nel caso in cui il fornitore esegua lavori che comportino un accesso limitato alle informazioni in possesso di InfoTecna. Fatti salvi gli obblighi di riservatezza a cui possa essere soggetto, laddove il fornitore o il personale temporaneo acceda alle informazioni di InfoTecna, o dei clienti di InfoTecna (inclusi i dati personali), correlate a InfoTecna o ai fornitori di InfoTecna, il fornitore dovrà:

- fare in modo che tali informazioni (inclusi i dati personali) non vengano divulgate né consultate da personale temporaneo non impiegato direttamente nei lavori effettuati in InfoTecna;
- mantenere (e provvedere affinché tutto il personale temporaneo interessato mantenga) tali informazioni (inclusi i dati personali) in condizioni di sicurezza e riservatezza (ad

esempio, senza intento limitativo, mettendo in atto i sistemi e le procedure necessarie per salvaguardare la sicurezza di tutte le informazioni appartenenti a, o sotto il controllo di InfoTecna nella misura in cui siano in possesso o sotto il controllo del fornitore in conformità alle migliori prassi di settore e implementare tali sistemi e processi in modo rigoroso).

Le sezioni dalla 4 alla 7 incluse sono applicabili a tutti gli impegni dei fornitori nei confronti di InfoTecna (con l'eccezione dei fornitori che effettuano unicamente forniture con accesso limitato).

4. SICUREZZA DELLE INFORMAZIONI GENERALI

4.1 Il fornitore avrà cura di trasmettere prontamente a InfoTecna gli estremi del proprio referente per la sicurezza ed ogni eventuale variazione degli stessi.

4.2 Il fornitore provvederà a comunicare per iscritto al referente Security di InfoTecna, a mezzo PEC all'indirizzo infotecna@pec.it, le aree geografiche in cui vengono erogati i servizi principali, come viene assegnato il personale temporaneo interessato o vengono trattate o archiviate le informazioni di InfoTecna. Durante l'esecuzione del contratto, il fornitore dovrà inoltre comunicare ogni proposta di modifica dell'area geografica al referente Security di InfoTecna a mezzo PEC all'indirizzo infotecna@pec.it, affinché InfoTecna possa valutare nuovamente gli eventuali rischi a carico delle informazioni o dei clienti di InfoTecna.

4.3 Il fornitore provvederà affinché tutti i contratti con i subappaltatori interessati includano clausole scritte che impongano il rispetto, da parte dei subappaltatori stessi, dei requisiti di sicurezza per i fornitori di InfoTecna, nella misura in cui risultino applicabili. Queste condizioni devono essere stipulate tra il fornitore e il suo subappaltatore prima che quest'ultimo o un suo addetto possano accedere ai sistemi di InfoTecna e alle informazioni di InfoTecna.

4.4 Il fornitore non potrà avvalersi delle informazioni di InfoTecna per finalità diverse da quelle per cui tali informazioni gli sono state trasmesse da InfoTecna e unicamente nella misura necessaria per consentirgli di dare esecuzione al contratto. Il fornitore avrà l'obbligo di trattare o utilizzare le informazioni di InfoTecna secondo modalità coerenti con i requisiti contenuti nel presente documento, nonché in conformità alla legislazione vigente in materia.

4.5 Il fornitore avrà cura di informare il referente Security di InfoTecna a mezzo PEC all'indirizzo infotecna@pec.it, qualora si trovi ad essere soggetto a procedure di fusione, acquisizione o cambiamento di proprietà, affinché sia possibile valutare nuovamente gli eventuali rischi a carico di InfoTecna, delle informazioni di InfoTecna o delle informazioni dei clienti di InfoTecna.

4.6 Con cadenza almeno annuale e ogni volta che sopraggiungano variazioni alle forniture o alle modalità con cui vengono fornite, il fornitore dovrà riesaminare i presenti requisiti di sicurezza al fine di accertarne la conformità a tutti i requisiti di sicurezza applicabili.

4.7 Il fornitore dovrà gestire in condizioni di sicurezza tutti i beni materiali di InfoTecna e/o gli articoli di InfoTecna assegnatigli dalla stessa InfoTecna:

- quando inutilizzati, i beni materiali di InfoTecna e gli articoli di InfoTecna dovranno essere immagazzinati in condizioni di sicurezza; tali materiali includono, senza intento limitativo, token di accesso remoto, computer portatili di InfoTecna, apparecchiature di rete, server e documentazione;

- i beni materiali di InfoTecna non potranno essere allontanati dal luogo di lavoro senza previa autorizzazione.

4.8 In relazione all'approvvigionamento delle forniture, il fornitore dovrà attuare procedure formali di gestione degli incidenti riguardanti la sicurezza con responsabilità definite e trattamento “riservato” di tutte le informazioni relative a tali incidenti. Il fornitore provvederà ad informare il referente Security di InfoTecna a mezzo PEC all'indirizzo infotecna@pec.it, entro un ragionevole lasso di tempo da quando giunga a conoscenza di un qualsiasi incidente:

- che comporti perdite di materiali, corruzione, danneggiamento o uso improprio di informazioni di InfoTecna, Beni materiali di InfoTecna, articoli di InfoTecna oppure un accesso improprio o non autorizzato ai sistemi di InfoTecna e alle informazioni di InfoTecna, oppure una violazione degli obblighi del fornitore ai sensi dei presenti requisiti di sicurezza;

- che abbia come conseguenza l'incapacità di effettuare le forniture in conformità al contratto;

- che sia stato causato da azioni che violano i requisiti del presente documento sulla sicurezza.

Dietro richiesta, il fornitore trasmetterà sollecitamente a InfoTecna una relazione scritta contenente un piano di ripristino che includa un calendario e le misure da porre in atto al fine di evitare il reiterarsi dell'incidente.

4.9 Il fornitore dovrà garantire un pronto intervento a fronte di ogni rischio identificato a carico della riservatezza, integrità o disponibilità delle informazioni di InfoTecna o dei processi o sistemi del fornitore.

4.10 InfoTecna avrà facoltà di condurre la valutazione dei rischi relativamente a qualsiasi aspetto pertinente del servizio (ad esempio i subappaltatori coinvolti nel servizio) allo scopo di identificare ulteriori rischi a carico di InfoTecna per effetto dell'approvvigionamento delle forniture, a seconda dei casi. InfoTecna potrà quindi precisare le opportune contromisure aggiuntive atte a contrastare tali rischi. Gli eventuali costi associati all'attuazione delle contromisure saranno oggetto di accordo tra le parti.

4.11 Il fornitore dovrà dotarsi di processi e politiche sulla sicurezza e mantenere una documentazione (di cui copie da mettere a disposizione in lingua inglese) che attesti la

conformità ai presenti requisiti di sicurezza, mettendo inoltre a disposizione di InfoTecna l'accesso alle prove in ottemperanza alla sezione 8.

4.12 Il fornitore disporrà, affinché siano in atto procedure e controlli atti a proteggere il trasferimento di informazioni di InfoTecna, tramite l'impiego di servizi di comunicazione e-mail, voce, fax e video (accertandosi ad esempio che durante le riunioni in videoconferenza tutti i partecipanti siano autorizzati a discutere di informazioni relative a InfoTecna).

4.13 Il fornitore avrà l'obbligo di implementare procedure atte a contrastare le minacce alla sicurezza dirette o mirate a InfoTecna o contro un soggetto terzo operante al servizio di InfoTecna al fine di tutelare adeguatamente le informazioni di InfoTecna.

4.14 Il fornitore provvederà affinché le attività lavorative remote e a domicilio aventi attinenza con informazioni di InfoTecna e sistemi di InfoTecna siano soggette a regolari controlli sulla sicurezza nell'ambito dell'organizzazione del fornitore stesso, quali, a titolo di esempio e senza intento limitativo, l'autenticazione avanzata da applicare all'accesso remoto da parte degli utenti.

4.15 Alla risoluzione o scadenza del contratto, il fornitore provvederà, e farà in modo che il personale temporaneo e i subappaltatori provvedano, a distruggere in sicurezza e in conformità del presente documento, tutte le informazioni di InfoTecna possedute o controllate dal fornitore o dai suoi subappaltatori, salvo diversamente specificato da InfoTecna, o imposto in forza di un obbligo legislativo o regolamentare. Le informazioni archiviate devono essere poste al di fuori della possibilità di accesso nel corso delle attività aziendali correnti.

4.16 Il fornitore dovrà conservare le informazioni di InfoTecna per tutto il tempo necessario a svolgere il servizio, ma non oltre un massimo di due anni, tranne che un diverso periodo di conservazione sia stato specificato da InfoTecna o sia imposto in osservanza di requisiti legislativi o regolamentari.

4.17 Secondo il contratto stipulato, il fornitore dovrà garantire la disponibilità, qualità, integrità e capacità adeguata di offrire le prestazioni di sistema richieste o le forniture con una disponibilità senza interruzioni, assicurando che:

- i dati di sistema critici siano protetti;
- in caso di guasti o incidenti venga applicata una soluzione alternativa, se ciò costituisce un requisito concordato;
- il sistema o servizio possa essere ripristinato dopo un guasto o un incidente di grave entità;
- le copie di backup delle informazioni e del software, a seconda dei casi, vengano effettuate e testate regolarmente in conformità ad una politica di backup concordata allo scopo di garantire il ripristino dei dati senza alterazioni;

- il controllo di ripristino dei dati venga messo in pratica almeno con cadenza annuale.

5. VERIFICHE E REVISIONI DELLA SICUREZZA

Il fornitore, in relazione alle forniture e fermo restando il rispetto della riservatezza delle informazioni riguardanti i suoi altri clienti, dovrà consentire (e fare in modo che tutto il personale temporaneo consenta), dietro richiesta, a InfoTecna o ai suoi rappresentanti autorizzati, l'accesso alle strutture, ai sistemi e ai registri del fornitore e dei subappaltatori interessati, contenenti informazioni di InfoTecna e dei clienti di InfoTecna (inclusi i dati personali) nei modi ragionevolmente necessari per accertare la conformità del fornitore ai presenti requisiti di sicurezza.
Ciò potrebbe includere una valutazione di tutti gli elementi dei controlli fisici e logici nonché la validazione dei sistemi del fornitore in cui sono contenute informazioni di InfoTecna. Il fornitore dovrà facilitare tali accertamenti consentendo a InfoTecna di raccogliere, conservare e analizzare le informazioni riguardanti l'approvvigionamento delle forniture, se del caso, al fine di individuare eventuali rischi per la sicurezza, oltre ad assecondare le ragionevoli richieste di invio di relazioni e di partecipazione a riunioni.
Su richiesta di InfoTecna, il fornitore parteciperà ad un controllo di integrità on-line da remoto volto ad accertare la conformità di base alle clausole dei presenti requisiti di sicurezza.

6. ACCERTAMENTI

Qualora InfoTecna abbia motivo di sospettare che si sia verificata una violazione, da parte del fornitore di un subappaltatore, delle disposizioni dei presenti requisiti di sicurezza, tale da ripercuotersi sui sistemi di InfoTecna e/o sulle informazioni di InfoTecna, InfoTecna ne darà informazione al referente per la sicurezza del fornitore. Il fornitore si impegna a collaborare senza riserve con InfoTecna in ogni eventuale accertamento che ne consegua condotto da InfoTecna e/o dalle autorità preposte all'applicazione della legge, autorizzando ad esempio l'accesso alle informazioni di InfoTecna presenti presso le strutture del fornitore, previo ragionevole preavviso.
Nel corso degli accertamenti, il fornitore avrà l'obbligo di collaborare con InfoTecna, fornendo l'opportuna assistenza e le strutture necessarie per l'indagine della violazione. InfoTecna avrà facoltà di richiedere che il fornitore isoli a scopo di valutazione eventuali beni materiali o immateriali appartenenti al fornitore per favorire gli accertamenti. Il fornitore non potrà in tal caso opporsi alla richiesta o prorogarne i tempi di risposta senza un ragionevole motivo.

7. POLITICA E REQUISITI GENERICI DI SICUREZZA

L'osservanza delle clausole contenute nella sezione 7 ha carattere vincolante se il fornitore ha accesso a “informazioni sensibili” (come da definizione), oppure svolge funzioni di sviluppo, installazione, manutenzione e supporto di reti o fornisce servizi professionali di IT.

7.1 Il fornitore dovrà essere in possesso di certificazione ISO27001 o conformarsi ai requisiti di sicurezza della certificazione ISO27001 o di politiche di sicurezza allineate alla ISO27001 e/o avere avviato la procedura di ottenimento della certificazione ISO27001 entro un lasso di tempo concordato con InfoTecna.

7.2 Se previsto, InfoTecna potrà periodicamente aggiornare politiche, linee guida e requisiti correlati alla sicurezza e altre disposizioni obbligatorie. InfoTecna integrerà gli aggiornamenti in questione nell'ambito di una versione riveduta dei presenti requisiti di sicurezza mediante una richiesta di modifica contrattuale notificata per iscritto al fornitore da InfoTecna. Gli eventuali costi associati all'introduzione dei nuovi requisiti di sicurezza saranno oggetto di accordo tra le parti.

7.3 Il fornitore metterà a disposizione di InfoTecna copie delle Certificazioni di sicurezza e una dichiarazione di applicabilità relativa ai servizi erogati a sostegno delle prove di *messa* in conformità rispetto a questo piano.

8. SICUREZZA FISICA - STRUTTURE DI INFOTECNA

L'osservanza delle clausole contenute nella sezione 8 ha carattere vincolante se il fornitore effettua forniture presso le strutture di InfoTecna.

8.1 Tutti i membri del personale temporaneo impegnato presso le strutture di InfoTecna dovranno essere in possesso di una tessera che li identifichi come “fornitore autorizzato” o altro documento analogo fornito da InfoTecna. Questa tessera dovrà essere utilizzata permanentemente da ciascun membro del personale temporaneo come strumento di verifica dell'identità presso le strutture di InfoTecna.

8.2 Solo server conformi agli standard di InfoTecna, e dispositivi terminali altamente affidabili potranno essere connessi direttamente (mediante inserimento di cavo nella porta LAN o connessione wireless) ai domini InfoTecna. Il fornitore non potrà (e, quando opportuno, disporrà affinché il personale temporaneo non possa) collegare un’apparecchiatura non approvata da InfoTecna a un qualsiasi dominio InfoTecna senza l'autorizzazione preliminare del referente Security di InfoTecna (a mezzo PEC all'indirizzo infotecna@pec.it). Il referente Security di InfoTecna fornirà l'autorizzazione scritta contestualmente all'avvio del processo di concessione della politica di sicurezza interna di InfoTecna da parte del referente InfoTecna del fornitore.

8.3 Nessuna informazione di InfoTecna potrà essere rimossa dalle strutture InfoTecna e nessuna apparecchiatura o nessun software potranno essere rimossi o installati presso le strutture InfoTecna senza l'autorizzazione preliminare di InfoTecna.

8.4 Le linee guida in materia di protezione fisica e di lavori all'interno delle Strutture di InfoTecna dovranno essere rigorosamente rispettate, ad esempio predisponendo un accompagnamento in caso di attraversamento delle zone protette. Ogni ulteriore ordine o istruzione impartito da InfoTecna ad un rappresentante del fornitore si intenderà trasmesso direttamente al fornitore.

8.5 Laddove il fornitore sia autorizzato a concedere al personale temporaneo un accesso non accompagnato alle aree interne alla proprietà di InfoTecna, il firmatario autorizzato non InfoTecna e il personale temporaneo dovranno aderire a tutte le raccomandazioni impartite da InfoTecna. Inoltre, il firmatario autorizzato di InfoTecna e il personale temporaneo dovranno essere sottoposti a controlli pre-impiego di livello minimo.

9. SICUREZZA FISICA - STRUTTURE DEL FORNITORE

L'osservanza delle clausole contenute nella sezione 9 ha natura vincolante se il fornitore effettua le forniture da strutture non InfoTecna e include l'insieme di personale temporaneo, subappaltatori e dipendenti, subappaltatori e agenti del fornitore. A tal fine, si richiede di rispettare ed attuare tutte le misure in conformità a quanto indicato dal regolamento europeo 2016/679 e dalle disposizioni indicate nella normativa ISO 27001 e ISO 22301 in particolare:

- che nei locali o nelle reti, dove sono presenti informazioni o apparecchiature di InfoTecna, possa accedere solo il personale debitamente formato e autorizzato;
- aver attivato procedure atte a contrastare le minacce alla sicurezza dirette contro le apparecchiature di InfoTecna o dei clienti di InfoTecna o contro un soggetto terzo al servizio di InfoTecna al fine di salvaguardare le informazioni di InfoTecna e dei clienti di InfoTecna presso il Sito del fornitore;
- che vi siano delle politiche per garantire la continuità operativa e attuare i piani di emergenza dovuta a guasti agli impianti causati dall'interruzione di servizi essenziali o altri fattori di influenza ambientale;
- che le zone protette all'interno delle strutture del fornitore (ad esempio le sale per comunicazioni di rete), siano segregate e protette mediante adeguati controlli all'ingresso per fare in modo che possa accedervi unicamente il personale autorizzato;
- che vi siano delle politiche atte ad impedire e prevenire l'accesso alle informazioni del personale non autorizzato;
- che siano adottate tutte le misure per garantire la sicurezza fisica dei locali e garantire la continuità operativa.

10. PREDISPOSIZIONE DI UN AMBIENTE DI HOSTING

L'osservanza delle clausole contenute nella sezione 10 ha carattere vincolante se il fornitore predispone un ambiente di hosting destinato ad apparecchiature di InfoTecna o dei clienti di InfoTecna.

10.1 Nel caso in cui predisponga un'area ad accesso protetto alle proprie strutture per l'hosting di apparecchiature di InfoTecna o di clienti InfoTecna ("Sito del fornitore"), il fornitore garantirà:

- che nei locali non InfoTecna o nelle reti, dove sono presenti delle informazioni possa accedere solo il personale debitamente formato e autorizzato;
- che vi siano delle politiche per garantire la continuità operativa e attuare i piani di emergenza;
- di aver attivato procedure atte a contrastare le minacce alla sicurezza dirette contro le apparecchiature di InfoTecna o dei clienti di InfoTecna o contro un soggetto terzo

al servizio di InfoTecna al fine di salvaguardare le informazioni di InfoTecna e dei clienti di InfoTecna presso il Sito del fornitore;

- che le zone protette all'interno delle strutture del fornitore siano segregate e protette mediante adeguati controlli all'ingresso al fine di assicurare e che possa accedervi unicamente il personale autorizzato.

10.2 InfoTecna avrà l'obbligo di trasmettere le seguenti informazioni al fornitore:

- un registro dei beni materiali di InfoTecna o del cliente di InfoTecna presenti presso il Sito del fornitore;

- estremi dei dipendenti, subappaltatori e agenti di InfoTecna che hanno necessità di accedere (continuativamente) al sito del fornitore.

11. SVILUPPO DELLE FORNITURE

L'osservanza delle clausole contenute nella sezione 11 ha carattere vincolante se il fornitore si occupa dello sviluppo di forniture per uso da parte di InfoTecna o dei clienti di InfoTecna (sono inclusi “componenti standard”, configurazioni del software e componenti di fabbricazione relativi alle forniture).

11.1 Il fornitore avrà l'obbligo di attuare misure di sicurezza concordate in tutti i componenti forniti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle forniture agendo nel modo seguente:

- conservando l'opportuna documentazione relativamente all'attuazione delle misure di sicurezza e farà in modo che sia la documentazione che la sicurezza siano conformi alle migliori prassi del settore;

- contenendo al minimo il rischio che soggetti non autorizzati (ad esempio, pirati informatici) possano accedere ai sistemi o reti InfoTecna causando potenziali interruzioni di servizio e dati e/o perdite di proventi.

11.2 Il fornitore sarà tenuto a dimostrare, su richiesta, che ogni versione software o hardware (sia essa speciale o standard) fornita a InfoTecna è identica a quella concordata con InfoTecna. Il fornitore si impegna a preservare l'integrità delle versioni, inclusi gli aggiornamenti, i sistemi operativi e le applicazioni, dai reparti produttivi agli uffici.

11.3 Il fornitore dovrà dimostrare che lo sviluppo di sistemi destinati all'utilizzo da parte di InfoTecna o che la realizzazione e la manutenzione dell'hardware di proprietà di InfoTecna sono soggetti a protezione avanzata in linea con i requisiti di sicurezza di InfoTecna, se forniti dal team operativo di InfoTecna, oppure con le migliori prassi del settore.

11.4 Il fornitore farà in modo che gli ambienti di sviluppo e prova non contengano dati reali e siano segregati rispetto all'ambiente reale. I dati di prova forniti da InfoTecna dovranno essere eliminati al termine di un periodo stabilito dal proprietario dei dati InfoTecna.

11.5 Il fornitore garantisce che è stato compiuto ogni ragionevole sforzo al fine di assicurare che il software e/o l'hardware (unitamente alla documentazione consegnata in formato elettronico) non contengono il seguente software dannoso (elenco non esaustivo), in qualsiasi forma disponibile:

- "possesso elettronico" e "bombe logiche";
- "virus" e "worm" eventualmente rilevati utilizzando il più recente (alla data di invio) software anti-virus disponibile sul mercato; e
- "spyware", "adware" e altre forme di malware.

Al momento dell'accettazione e successivamente a questa, il fornitore garantisce che il software e/o l'hardware funzioneranno in conformità alle specifiche funzionali per l'intero periodo di garanzia, inoltre, il fornitore si avvarrà unicamente di materiali, tecniche e requisiti di sicurezza di elevato livello qualitativo nel dare esecuzione al contratto e applicherà sistematicamente i requisiti di sicurezza con la cura, abilità e diligenza richiesti dalle buone prassi informatiche e dalle metodologie di codifica sicure.

Il fornitore si impegna a collaborare con InfoTecna al fine di assicurare la conformità ai requisiti di sicurezza nell'ambito del quadro di sicurezza appropriato a spese del fornitore; ciò potrebbe richiedere che le forniture vengano periodicamente testate di conseguenza in materia di sicurezza.

Ogni eventuale carenza nella sicurezza delle forniture individuata da InfoTecna o dal fornitore sarà rettificata a spese del fornitore nei tempi che InfoTecna avrà opportunamente cura di richiedere.

12. ACCESSO ALLE INFORMAZIONI

Applicabile se specificato nei requisiti.

12.1 Entro 14 giorni dalla richiesta scritta di InfoTecna e a discrezione di InfoTecna:

- le parti, facendosi carico ciascuna delle proprie spese, sottoscriveranno e consegneranno alla controparte un accordo di accesso alle informazioni nella forma dell'accordo di accesso alle informazioni oppure:
- il fornitore, a proprie spese, sottoscriverà un accordo di deposito in garanzia sostanzialmente nella forma dell'accordo relativamente a tutte le informazioni e documentazione aventi attinenza alle forniture (inclusi, senza intento limitativo, il software, tutto il codice sorgente, dati di collegamento, elenchi software, dati

tecnici completi, note dei programmatori, il complesso delle informazioni e della documentazione correlate al software necessarie per aggiornare, modificare e correggere il software, nonché fornire ogni livello di supporto per il software) (di seguito, le "informazioni sul deposito di garanzia") e depositerà in garanzia presso NCC Escrow International Limited (di seguito, "agente depositario") una copia aggiornata delle informazioni sul deposito di garanzia. Il fornitore si adopererà affinché tali informazioni sul deposito di garanzia consentano a InfoTecna e/o a eventuali terzi competenti a nome di InfoTecna, di:

- adempiere agli obblighi pendenti del fornitore ai sensi del contratto, inclusi, senza intento limitativo, gli obblighi che sarebbero insorti (quali l'obbligo di evadere gli eventuali ordini che InfoTecna avrebbe potuto trasmettere in forza del contratto) qualora il contratto non fosse stato risolto da InfoTecna (salvo ai sensi del paragrafo 4 della clausola a titolo "risoluzione") prima dell'estinzione della sua durata normalmente prevista (nella quale sarà incluso ogni eventuale proroga concessa nell'ambito della possibilità di InfoTecna di prolungare la durata iniziale); e

- comprendere facilmente le informazioni sul deposito di garanzia, aggiornare (anche tramite upgrade), modificare, migliorare e correggere le informazioni sul deposito di garanzia e le forniture.

12.2 Il fornitore garantisce che le informazioni sul deposito di garanzia effettuato presso InfoTecna o presso l'agente depositario, a seconda dei casi, sono e saranno tenute opportunamente aggiornate in modo da consentire ad un programmatore o analista adeguatamente preparato di aggiornare o migliorare il software senza l'ausilio di altre persone o riferimenti. Il fornitore si impegna altresì a mantenere le informazioni sul deposito di garanzia perfettamente aggiornate per l'intera durata.

12.3 Qualora si verifichi un qualsiasi evento tale da consentire a InfoTecna o all'agente depositario, a seconda dei casi, di utilizzare e/o divulgare le informazioni sul deposito di garanzia, il fornitore sarà tenuto a fornire immediatamente a InfoTecna, per un periodo ragionevole, la consulenza, il supporto, l'assistenza, i dati, le informazioni, l'accesso al personale chiave del fornitore stesso o del suo concessore di licenza software nella misura necessaria allo scopo di comprendere, aggiornare (anche tramite upgrade), migliorare, modificare e correggere in tutto o in parte le informazioni sul deposito di garanzia e/o il software.

12.4 Fermo restando ogni altro diritto che possa aver maturato, InfoTecna acquisirà automaticamente il diritto non esclusivo, perenne, irrevocabile e valido in tutto il mondo, di utilizzare le informazioni sul deposito di garanzia, dopo la loro divulgazione, al fine di mantenere e supportare le forniture, nonché il diritto non esclusivo, perenne, irrevocabile, valido nel mondo intero ed esente da qualsiasi pagamento, di utilizzare, copiare, aggiornare (anche tramite upgrade), modificare, adattare, migliorare e correggere le forniture e le eventuali forniture modificate, adattate, migliorate e/o corrette, nonché di concedere tali forniture a terzi (entro i limiti delle licenze concesse

al fornitore), unitamente al diritto di autorizzare soggetti terzi ad agire come sopra a nome di InfoTecna.

12.5 La presente condizione sopravvivrà alla scadenza o risoluzione del contratto.

12.6 Se necessario allo scopo di garantire la conformità in materia di sicurezza, il referente per la sicurezza di rete InfoTecna (e/o i suoi addetti, nominati tra i dipendenti di InfoTecna) godranno di diritti analoghi (mutatis mutandis) se richiesto nell'ambito delle forniture, della familiarizzazione e della validazione (come da definizione contenuta nell'accordo di accesso alle informazioni) relativamente al materiale di base (come da definizione contenuta nell'accordo di accesso alle informazioni).

13. ACCESSO AI SISTEMI INFOTECNA

L'osservanza delle clausole contenute nella sezione 13 ha carattere vincolante se il personale temporaneo del fornitore ha necessità di accedere ai sistemi InfoTecna per poter effettuare le forniture.

13.1 A propria discrezione assoluta e nella misura ritenuta opportuna, InfoTecna potrà consentire al fornitore l'accesso unicamente ai fini dell'approvvigionamento delle forniture.

13.2 In relazione all'accesso, il fornitore provvederà (e, quando opportuno, disporrà affinché il personale temporaneo provveda) a quanto segue:

- accertarsi che gli identificativi degli utenti, le password, i PIN, i token e l'accesso per le conferenze siano destinati ai singoli membri del personale temporaneo e non siano oggetto di condivisione. I dati devono essere archiviati in modo sicuro e tenuti separati dal dispositivo utilizzato per effettuare l'accesso. Se un'altra persona giunge a conoscenza di una password, questa dovrà essere cambiata immediatamente;

- dietro ragionevole richiesta, trasmettere a InfoTecna i rapporti richiesti in merito al personale temporaneo autorizzato ad accedere ai sistemi InfoTecna;

- impedire il collegamento ai sistemi InfoTecna se non specificamente approvato e autorizzato dal referente di InfoTecna a mezzo PEC all'indirizzo infotecna@pec.it;

- adoperarsi nella misura del possibile per far sì che non venga introdotto alcun virus o codice dannoso (secondo l'accezione generale di tali espressioni nell'industria informatica), riducendo pertanto il rischio di danneggiamento dei sistemi InfoTecna e delle informazioni InfoTecna;

- adoperarsi nella misura del possibile per far sì che gli archivi personali contenenti informazioni, dati o materiali multimediali privi di attinenza con le forniture non vengano memorizzati nei server InfoTecna, nei computer portatili e desktop forniti

da InfoTecna, nei sistemi di archiviazione centralizzati InfoTecna o nei sistemi InfoTecna.

13.3 Nel caso in cui InfoTecna abbia concesso al fornitore un accesso ad Internet/Intranet, il fornitore stesso accederà (e farà in modo che il personale temporaneo acceda) a tali reti in modo adeguato ai fini dell'approvvigionamento delle forniture. Sarà compito del fornitore accertarsi che le seguenti istruzioni in materia di utilizzo improprio di Internet e della posta elettronica vengano trasmesse al personale temporaneo interessato con cadenza almeno annuale.
Non è consentito l'accesso a materiale che potrebbe essere ritenuto:

- osceno, a sfondo sessuale, sessista o politicamente offensivo;
- un atto suscettibile di ledere la reputazione di InfoTecna o di singole persone;
- attinente alla gestione di un'attività privata;
- una violazione di diritti d'autore;
- telefonia o messaggistica tramite Internet, quale Skype;
- in grado di superare il firewall o altri meccanismi di sicurezza di InfoTecna mediante operazioni di aggiramento o tunneling;
- tale da contribuire alla pubblicazione di siti o dichiarazioni online che potrebbero essere ragionevolmente interpretate come il punto di vista di InfoTecna;
- inaccettabile o pericoloso e tale pertanto da dover essere bloccato agli utenti.

13.4 Il fornitore contatterà immediatamente InfoTecna qualora un membro del personale temporaneo interessato non necessiti più dei diritti di accesso ai sistemi InfoTecna o cambi ruolo per qualsiasi motivo previsto dall'accordo, consentendo così a InfoTecna di disabilitare o modificare i diritti di accesso agli stessi sistemi InfoTecna.

14. ACCESSO ALLE INFORMAZIONI INFOTECNA CONTENUTE NEI SISTEMI DEL FORNITORE

L'osservanza delle clausole contenute nella sezione 14 ha carattere vincolante se le informazioni InfoTecna sono archiviate o trattate nei sistemi del fornitore.

14.1 Nel caso in cui al personale temporaneo venga consentito l'accesso ai sistemi del fornitore relativamente alla consegna di prodotti e/o servizi a InfoTecna, il fornitore dovrà:

- assicurarsi che ciascun individuo disponga di una password e di un identificativo utente univoci (in conformità alle buone prassi standard di settore) noti unicamente al detto individuo per proprio uso esclusivo nell'ambito del processo di log-in sicuro;

- consentire l'accesso ai sistemi di proprietà del fornitore in cui sono contenuti sistemi InfoTecna o informazioni InfoTecna o da cui è possibile accedervi unicamente nella misura strettamente necessaria al fine di consentire al personale temporaneo di assolvere alle proprie mansioni ai sensi dell'accordo;

- stabilire procedure formali di controllo dell'assegnazione, revisione, revoca e/o cessazione dei diritti di accesso;

- assicurarsi che l'assegnazione e l'utilizzo dei privilegi avanzati e dell'accesso a strutture e strumenti sensibili nei sistemi del fornitore siano controllati e limitati unicamente agli utenti che ne hanno necessità per scopi aziendali. L'accesso alle console dei sistemi e il loro utilizzo devono aver luogo in un ambiente sicuro commisurato ai beni abitualmente gestiti. Misure appropriate di sicurezza fisica devono essere messe in atto al fine di scongiurare ogni rischio di accesso non autorizzato;

- assicurarsi che l'assegnazione delle password utente ai sistemi di proprietà del fornitore in cui sono contenute o da cui si accede alle informazioni InfoTecna sia controllata mediante un processo formale di gestione verificabile;

- condurre revisioni periodiche dei diritti di accesso degli utenti;

- assicurarsi che l'accesso fisico alle apparecchiature informatiche da cui si accede o in cui sono archiviate le informazioni InfoTecna avvenga unicamente mediante carte di prossimità o a microprocessore (o sistemi di sicurezza equivalenti) e che il fornitore conduca verifiche interne periodiche per accertare il rispetto di tali disposizioni;

- dimostrare che gli utenti aderiscono a buone prassi di sicurezza nella gestione delle password;

- introdurre un sistema di gestione delle password che preveda un dispositivo sicuro ed efficace tale da garantire la qualità delle password;

- assicurarsi che le sessioni utente vengano interrotte allo scadere di un periodo predefinito di inattività;

- assicurarsi che vengano generati e gestiti in condizioni di sicurezza registri di controllo in cui vengano riportate le attività degli utenti e gli eventi pertinenti in materia di sicurezza. I registri dovranno essere conservati per un periodo ragionevole al fine di agevolare eventuali accertamenti, essendo esclusa ogni possibilità per il fornitore di consentire l'accesso non autorizzato ai registri di controllo o la modifica degli stessi;

- assicurarsi che il monitoraggio dei registri di controllo e degli eventi, unitamente ai rapporti di analisi relativi a comportamenti anomali e/o a tentativi di accesso non autorizzato venga effettuato da personale del fornitore indipendente dagli utenti soggetti a monitoraggio.

14.2 Il fornitore avrà l'obbligo di introdurre sistemi in grado di rilevare e registrare ogni tentativo di danneggiamento, modifica o accesso non autorizzato alle informazioni InfoTecna contenute nei sistemi del fornitore (ad esempio, sistemi di registrazione e controllo dei processi, IDS, IPS ecc.).

14.3 Introdurre controlli atti a rilevare e contrastare malware e fare in modo che vengano attuate procedure adeguate di sensibilizzazione degli utenti.

14.4 Provvedere affinché, con cadenza almeno mensile, l'eventuale software non autorizzato venga identificato e rimosso dai sistemi del fornitore che contengono, trattano o accedono a informazioni InfoTecna.

14.5 Verificare che l'accesso alle porte di diagnosi e gestione, nonché gli strumenti diagnostici siano controllati in maniera sicura.

14.6 Assicurarsi che l'accesso agli strumenti di controllo del fornitore sia limitato al personale temporaneo interessato e che l'utilizzo degli stessi sia monitorato.

14.7 Disporre affinché un team indipendente dagli sviluppatori conduca riesami dei codici e prove di penetrazione sull'intero software di produzione interna utilizzato per trattare le informazioni InfoTecna.

14.8 I server utilizzati ai fini di approvvigionamento delle forniture non dovranno essere installati su reti non affidabili (poste al di fuori del perimetro di sicurezza o del controllo amministrativo, ad esempio esposti a Internet) senza adeguati controlli di sicurezza.

14.9 Ogni modifica apportata a singoli sistemi del fornitore che contengono o trattano informazioni InfoTecna e/o che vengono utilizzati per fornire prodotti e/o servizi a InfoTecna devono essere controllati e sottoposti a procedure formali di controllo delle modifiche.

14.10 Tutti i sistemi devono avere gli orologi interni sincronizzati rispetto a una fonte attendibile.

15. HOSTING DELLE INFORMAZIONI INFOTECNA DA PARTE DEL FORNITORE

L'osservanza delle clausole contenute nella sezione 15 ha carattere vincolante se il fornitore si affida a servizi esterni di hosting per le informazioni InfoTecna classificate almeno come riservate in un ambiente di servizi cloud, oppure in un ambiente server di fornitori o subappaltatori.

In relazione alle forniture, il fornitore provvederà affinché gli ambienti in cui vengono gestite in hosting le informazioni InfoTecna siano conformi ai requisiti dei contratti di Hosting riportati nel punto 10.

16. SICUREZZA DI RETE

L'osservanza delle clausole contenute nella sezione 16 ha carattere vincolante se il fornitore realizza, sviluppa o supporta reti INFOTECNA o infrastrutture di rete.

16.1 In relazione alle forniture, il fornitore avrà l'obbligo di attuare misure concordate di sicurezza in tutti i componenti forniti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle reti InfoTecna e/o delle infrastrutture InfoTecna. Il fornitore metterà a disposizione di InfoTecna la documentazione completa relativa all'implementazione della sicurezza di rete correlata alle forniture e si impegnerà al fine di:

- soddisfare ogni requisito legale e normativo;
- impedire al meglio delle proprie capacità che soggetti non autorizzati (ad esempio, pirati informatici) accedano a elementi di gestione della rete e ad altri elementi accessibili tramite le reti InfoTecna;
- adoperarsi al meglio delle proprie capacità al fine di contenere il rischio di uso improprio delle reti InfoTecna tale da causare perdite potenziali di proventi o interruzioni di servizio, da parte di individui autorizzati ad accedervi;
- dover al meglio delle proprie capacità al fine di individuare le violazioni della sicurezza effettivamente perpetrate, attivando la rapida correzione degli eventuali problemi che ne conseguano, nonché l'identificazione degli individui che hanno ottenuto l'accesso e delle modalità seguite per ottenerle;
- ridurre al minimo il rischio di errata configurazione delle reti InfoTecna, ad esempio concedendo il numero minimo di autorizzazioni necessarie per adempiere al ruolo oggetto del contratto.

16.2 Il fornitore dovrà adottare tutte le misure ragionevoli allo scopo di mettere in sicurezza tutte le interfacce presenti nei componenti forniti, senza presupporre che questi vengano fatti funzionare in un ambiente sicuro.

16.3 Il fornitore avrà l'obbligo di comunicare al referente per la sicurezza di rete InfoTecna i nominativi, gli indirizzi (e altri dati che InfoTecna avrà facoltà di richiedere) di tutti i membri del personale temporaneo che di volta in volta sarà direttamente coinvolto nell'installazione, manutenzione e/o gestione delle forniture prima che intraprendano tali operazioni.

16.4 Relativamente alle attività di supporto svolte sul territorio del Regno Unito, il fornitore si affiderà ad un team specializzato in sicurezza composto da almeno un cittadino del

Regno Unito disponibile per fungere da collegamento con il referente per la sicurezza di rete InfoTecna (o i suoi addetti) e per partecipare alle riunioni che il suddetto referente potrà richiedere periodicamente.

16.5 Il fornitore trasmetterà al referente per la sicurezza di rete InfoTecna un prospetto (opportunamente aggiornato) di tutti i componenti attivi contenuti nelle forniture con indicazione delle rispettive fonti.

16.6 Il fornitore comunicherà gli estremi dei membri del suo personale che assicurano il collegamento con il team per la gestione delle vulnerabilità (CERT) in relazione alla discussione sulle vulnerabilità individuate da InfoTecna e dal fornitore nelle forniture. Il fornitore comunicherà puntualmente a InfoTecna informazioni sulle vulnerabilità, e adempierà ai ragionevoli obblighi ad esso notificati di volta in volta dal referente per la sicurezza di rete InfoTecna, a proprie spese. Il fornitore informerà InfoTecna in ordine alle vulnerabilità con sufficiente anticipo, in modo da consentire l'introduzione di controlli di mitigazione prima che il fornitore stesso divulghi pubblicamente le vulnerabilità.

16.7 Il fornitore dovrà concedere al referente per la sicurezza di rete InfoTecna e a chi da esso di volta in volta designato un accesso completo e incondizionato alle strutture in cui le forniture vengono sviluppate, prodotte o fabbricate perché vi possano condurre test e/o valutazione di conformità alla sicurezza. Il fornitore sarà peraltro tenuto a collaborare (e disporrà affinché l'intero personale temporaneo interessato faccia altrettanto) in tali verifiche della conformità.

16.8 Il fornitore dovrà accertarsi che tutti i componenti riguardanti la sicurezza contenuti nelle forniture, così come di volta in volta identificati da, o comunicati a InfoTecna, vengano valutati esternamente a spese del fornitore e con la ragionevole soddisfazione di InfoTecna.

16.9 In relazione alle informazioni trasmesse o ottenute da InfoTecna e accompagnate dalla dicitura “STRETTAMENTE RISERVATO” o la cui natura riservata sia facilmente riconoscibile, il fornitore dovrà provvedere affinché:

- l'accesso ad esse venga consentito unicamente al personale temporaneo appositamente autorizzato da InfoTecna per la visione e il trattamento e venga conservato un registro di tali accessi;
- esse vengano trattate, utilizzate e archiviate con estrema cura e criptate prima dell'archiviazione e in condizioni che assicurino un elevato grado di resistenza alla compromissione accidentale (ossia, adottando il più efficace algoritmo di crittografia disponibile o utilizzando una valida password) e che rendano rilevabile con grande probabilità l'azione o il tentativo di compromissione;
- non vengano, salvo autorizzazione scritta di InfoTecna, esportate al di fuori dello spazio economico europeo.

16.10 Il fornitore dovrà comunicare sollecitamente, e in ogni caso entro il termine di 7 giorni lavorativi, al referente per la sicurezza di rete InfoTecna i dettagli completi delle caratteristiche e funzionalità proprie delle forniture (o che sono pianificate nella tabella di marcia per le forniture) progettate per, o che potrebbero essere progettate per, l'intercettazione legale o altre forme di intercettazione del traffico delle telecomunicazioni che di volta in volta:

- il fornitore conosce;
- il referente per la sicurezza di rete InfoTecna ritiene ragionevolmente di conoscere e ne dà pertanto comunicazione al fornitore. Tali dettagli dovranno includere tutte le informazioni ritenute ragionevolmente necessarie per consentire al referente per la sicurezza di rete InfoTecna di comprendere appieno la natura, composizione e portata di tali caratteristiche e/o funzionalità.

16.11 Allo scopo di mantenere abilitato l'accesso ai sistemi e/o alle reti InfoTecna, il fornitore dovrà comunicare immediatamente a InfoTecna ogni eventuale modifica apportata al proprio metodo di accesso tramite i firewall, fornendo ad esempio la traduzione degli indirizzi di rete.

16.12 Non è consentito l'utilizzo di strumenti di monitoraggio in grado di visualizzare informazioni relative alle applicazioni.

16.13 La funzionalità IPv6 inclusa nei sistemi operativi deve essere disabilitata sugli host (dispositivi degli utenti finali, server) collegati ai domini di rete InfoTecna e quando non necessaria.

16.14 Il fornitore è tenuto a rispettare, e disporrà affinché le forniture rispettino, le politiche InfoTecna eventualmente vigenti e i requisiti di sicurezza. Ogni inosservanza dovrà essere concordata all'atto della firma del contratto o in sede di controllo delle modifiche.

16.15 Il fornitore provvederà affinché il personale temporaneo venga sottoposto a controlli pre-impiego adeguati rispetto al livello di accesso.

17. SICUREZZA DI RETE DEL FORNITORE

L'osservanza delle clausole contenute nella sezione 17 ha carattere vincolante se la rete del fornitore verrà utilizzata ai fini dell'approvvigionamento delle forniture (sono incluse reti LAN, WAN, Internet, wireless e radio).

In relazione alle forniture, il fornitore avrà l'obbligo di attuare misure concordate di sicurezza in tutte le reti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle informazioni InfoTecna. Le misure dovranno:

- soddisfare ogni requisito legale e normativo;
- impedire nella misura del possibile che soggetti non autorizzati (ad esempio, pirati informatici) accedano alla rete;

- contenere nella misura del possibile il rischio di uso improprio delle reti tale da causare potenziali perdite di proventi o interruzioni di servizio, da parte di individui autorizzati ad accedervi;

- individuare nella misura del possibile ogni violazione della sicurezza effettivamente perpetrata, attivando la rapida correzione degli eventuali problemi che ne conseguano, nonché l'identificazione degli individui che hanno ottenuto l'accesso e delle modalità seguite per ottenerle.

18. SICUREZZA DEL CLOUD

L'osservanza delle clausole contenute nella sezione 18 ha carattere vincolante quando il fornitore presta a InfoTecna servizi correlati al cloud.

18.1 Il fornitore dovrà dimostrare con prove adeguate che i servizi cloud forniti soddisfino i requisiti di controllo.

18.2 Le informazioni InfoTecna utilizzate nel commercio elettronico e circolanti nelle reti pubbliche dovranno essere protette in conformità al presente documento sia in transito che a riposo (incluse le copie di backup) contro attività fraudolente e ogni tentativo non autorizzato di divulgazione, accesso e modifica.

18.3 Gli accordi sui livelli di servizio relativi a reti e infrastrutture (siano essi gestiti internamente o esternalizzati) dovranno documentare con chiarezza controlli, capacità e livelli di servizio in materia di sicurezza, oltre ai requisiti di business o del cliente.

18.4 Il fornitore dovrà consentire l'effettuazione di prove di penetrazione e/o l'accesso ai verbali delle prove di penetrazione già effettuate dal fornitore riguardanti le forniture effettuate. L'ambito di applicazione e i tempi delle prove saranno oggetto di accordo con InfoTecna.

18.5 Il fornitore avrà l'obbligo di attuare misure di sicurezza concordate in tutti i componenti forniti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle forniture contenendo al minimo il rischio che soggetti non autorizzati (ad esempio, altri clienti sul cloud) accedano ad informazioni InfoTecna e a servizi InfoTecna.