Requisiti di *Cybersecurity*

Requisiti per i contratti di Tipo 3:	**1 a 13**
Requisiti per i contratti di Tipo 2:	**1 a 24**
Requisiti per i contratti di Tipo 1:	**1 a 33**
Requisiti aggiuntivi per i contratti di Tipo 1 con risorse specifiche del contratto:	**34 a 67**

Indice

PREMESSA

I presenti Requisiti di *Cybersecurity* definiscono il quadro standard e minimo delle regole che devono essere rispettate dal Fornitore e dai suoi eventuali subappaltatori nel contesto dell'esecuzione del Contratto.

Tali regole devono essere specificate nel Piano di Sicurezza per i Contratti di Tipo 1.
Per i Contratti di Tipo 2 o 3 possono essere specificate in un Piano di Sicurezza.

I Requisiti di *Cybersecurity* non prevarranno o vanificheranno l'applicazione (i) delle leggi e dei regolamenti applicabili in materia di *cybersecurity* dei Sistemi e dei Dati e (ii) di norme applicabili più precise e rigorose in materia di *cybersecurity* dei Sistemi e dei Dati, quali le certificazioni ai sensi di norme quali ISO, ETSI o Cybersecurity Europea applicabili al Fornitore, ai suoi prodotti, alle sue procedure e/o ai suoi servizi, il Regolamento Interno e le regole altrimenti concordate dalle Parti.

Si ricorda che alcuni Sistemi Informativi e le loro Risorse, a causa della loro sensibilità, possono essere soggetti a normative, in particolare in termini di riservatezza (ad es. segreto difensivo), obblighi tecnici, umani e organizzativi, controllo e Audit, qualificazione e accreditamento, gestione degli allarmi e delle crisi, ecc.
Ai e sui presenti Requisiti di *Cybersecurity* si applicheranno e prevarranno anche il Regolamento Interno specifico (compresa la Policy per la sicurezza dei sistemi informatici) e le norme contrattuali specifiche.

Per quanto riguarda la Tecnologia AI, si applicheranno ulteriori procedure e disposizioni obbligatorie quando tali tecnologie sono destinate a essere utilizzate all'interno di infrastrutture critiche (in particolare ai sensi della Direttiva (UE) 2022/2557) o di sistemi e reti sensibili o vitali della Società, o soggetti a specifiche normative di *cybersecurity*. Lo stesso vale per tutti i sistemi AI ad alto rischio (ai sensi della legge sull'IA). Le previsioni contenute nei presenti requisiti per l'AI non possono sostituire o applicarsi di default a tali casi.

I riferimenti al Fornitore devono essere intesi come comprensivi del Fornitore e dei suoi subappaltatori, e gli obblighi del Fornitore si estendono ai Sistemi Informativi e alle Risorse dei suoi subappaltatori.

1 Termini e definizioni

I termini definiti di seguito si applicano esclusivamente ai requisiti di sicurezza - non possono in alcun modo essere utilizzati o utilizzati come riferimento negli altri documenti contrattuali del Contratto.

Tecnologia AI: Qualsiasi modello o sistema di intelligenza artificiale incorporato, utilizzato e/o gestito nell'ambito del Contratto e rientrante nel campo di applicazione del Regolamento (UE) 2024/1689 del 13 giugno 2024 (di seguito “Legge sull'AI”).

Audit: Insieme di verifiche volte ad assicurare la conformità del Fornitore, dei suoi servizi o beni, agli obblighi legali e contrattuali in termini di *Cybersecurity*.
Tipi di audit: organizzativo, di conformità, di configurazione e tecnico (intrusioni, code review, ecc.).

Autenticazione: Un metodo per verificare l'identità di un utente che accede al Sistema Informativo.

CERT (Computer Emergency Response Team) TotalEnergies: Entità (Computer Emergency Response Team) responsabile del coordinamento della risposta agli incidenti informatici e di *cybersecurity* e della valutazione della *cybersecurity* delle entità della Società e dei loro Fornitori.
Vedere https://totalenergies.com/cert

Classificazione: La classificazione di una Risorsa da parte del Cliente fornisce al Fornitore un'indicazione concisa della sua importanza e della necessità di un livello di protezione adeguato.

Profilo di Classificazione: L'approccio di classificazione, che consiste nell'assegnare un valore corrispondente all'impatto potenziale dei Rischi che possono interessare le Risorse analizzate secondo i tre criteri considerati.
Ad ogni Risorsa viene quindi assegnato, per ciascuno dei criteri di Disponibilità, Integrità e Riservatezza, un livello di sensibilità (da 0=Livello di impatto basso a 4=Livello di impatto elevato).

Contratto: Si riferisce all'insieme dei documenti che regolano il rapporto contrattuale tra il Fornitore e il Cliente per un servizio definito.

Risorse Specifiche del Contratto: Include le Risorse sotto la responsabilità del Fornitore e dei subappaltatori del Fornitore che sono implementate specificamente per il Contratto, incluse in particolare le postazioni di lavoro dei dipendenti coinvolti nel Contratto e le Risorse dedicate all'esecuzione del Contratto con il Fornitore.

Dati del Cliente: I dati, compresi i dati personali, a cui il Fornitore ha accesso sulla base del Contratto, nonché i dati (compresi i log e i metadati) generati dai Sistemi.

***Cybersecurity*:** Tutte le Misure tecniche e organizzative necessarie e proporzionate per proteggere i Sistemi Informativi e le Risorse della Società, le Risorse Specifiche del Contratto, i Dati del Cliente, gli utenti e i terzi che potrebbero essere interessati, da eventi o azioni che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei Sistemi Informativi e delle Risorse, nonché i Dati del Cliente e i servizi che offrono o rendono accessibili.

Incidente di *Cybersecurity*: Ogni Evento osservato che possa mettere in discussione la *Cybersecurity* o il normale funzionamento di una Risorsa del Sistema Informativo (o di un

servizio fornito dalla funzione IS) del Cliente o di una Risorsa Specifica del Contratto e che possa compromettere la disponibilità, l'integrità o la riservatezza della relativa Risorsa o dei Dati del Cliente.

Sistemi Informativi Aziendali (EIS): Gli EIS sono sistemi informatici che comprendono servizi e applicazioni destinati alla gestione aziendale (automazione d'ufficio, risorse umane, relazioni con i clienti, finanza, tesoreria, acquisti, ecc.).

Evento: Informazione generata da un componente del Sistema Informativo che viene registrata in un log**.**

Sistemi Informativi Industriali (IIS): Gli IIS sono Sistemi Informativi che comprendono sistemi e componenti che contribuiscono direttamente ai processi produttivi, all'integrità, alla sicurezza e alla protezione dei siti (sistemi di controllo dei comandi, gestione dei laboratori, sistemi di gestione tecnica, ecc.).

Sistema Informativo: Un insieme organizzato di Risorse per l'elaborazione dei dati e la fornitura di servizi. Il Sistema Informativo è essenziale per le attività della Società. Comprende il Sistema Informativo Aziendale (EIS) e il Sistema Informativo Industriale (IIS).

Regolamento Interno: Si riferisce alle regole del Cliente, in particolare alle regole e alle procedure interne specifiche del Sistema Informativo o dei siti del Cliente trasmessi dal Cliente al Fornitore o accessibili dalla Intranet del Cliente.

Incidente Grave di *Cybersecurity*: Ogni Incidente di *Cybersecurity* con conseguenze, secondo i livelli indicati nel Piano di Sicurezza.

Codice Dannoso: Ogni programma sviluppato con lo scopo di danneggiare o per mezzo di un Sistema informatico o di una rete.

Misura (di *Cybersecurity*): Mezzo per gestire un Rischio, che può essere di natura amministrativa, tecnica, di gestione o legale, compresi in particolare la policy, le procedure, le linee guida e le pratiche o strutture organizzative.

Accesso Privilegiato: Autorizzazione ad accedere a una Risorsa per eseguire operazioni di amministrazione della risorsa (ad esempio, leggere la configurazione, modificare la configurazione, eseguire un comando riservato a un amministratore, cancellare file, ecc.).

Rimedio: Implementazione di mezzi o misure di sicurezza per risolvere errori, falle, difetti o carenze della *Cybersecurity*.

Risorsa (del Sistema Informativo): Include tutti o parte dei mezzi, servizi e processi coinvolti nel funzionamento del Sistema Informativo del Cliente, quali, in particolare, applicazioni, dati, mezzi tecnici, attrezzature, reti (locali, aziendali, ecc.). Si precisa che le Risorse comprendono i mezzi, i servizi e i processi dei Fornitori che partecipano al Sistema Informativo del Cliente,

compresi i fornitori di servizi Cloud o SaaS, i fornitori di servizi gestiti direttamente o in outsourcing, ecc.

Rischio (di *Cybersecurity*): Un Rischio caratterizzato da:

- una Minaccia o un'azione dannosa di origine interna o esterna sui Sistemi Informativi;
- una Minaccia o un'azione non dannosa, come un guasto, una negligenza o un errore dei Sistemi Informativi.

Comitato per la Sicurezza (COSEC): Organo decisionale e di monitoraggio dei piani d'azione e degli indicatori di *Cybersecurity*.

Piano di Sicurezza (PAS): Documento che descrive i termini di esecuzione del Contratto dal punto di vista della *Cybersecurity*. Detto documento descrive gli indicatori di *Cybersecurity*, l'organizzazione della *Cybersecurity* e le misure specifiche di *Cybersecurity* implementate.

Centro Operativo di Sicurezza (Security Operations Center, SOC): Un SOC è una funzione centralizzata all'interno di un'organizzazione che impiega persone, processi e tecnologie per monitorare e migliorare continuamente la posizione di sicurezza dell'organizzazione, prevenendo, rilevando, analizzando e rispondendo agli incidenti di *Cybersecurity*.

Stato dell'arte: Principi e nozioni fondamentali sulla sicurezza dei Sistemi Informativi descritti in particolare nelle norme (ISO, IEC) e nei testi pubblicati da organismi ufficiali (ANSSI, NIST, ENISA).

Autenticazione Forte: Autenticazione basata su almeno 2 dei seguenti elementi:

- un elemento segreto noto solo all'utente (password, PIN);
- un oggetto di proprietà dell'utente (card che genera password monouso, smart card, chiavetta USB);
- una caratteristica fisica dell'utente (impronta digitale, impronta retinica, struttura della mano o qualsiasi altro elemento biometrico).

Sistemi: Si riferisce ai Sistemi Informativi del Cliente o del Fornitore utilizzati nel contesto del Contratto.

Minaccia (alla *Cybersecurity*): Causa potenziale di un Rischio di *Cybersecurity*, che può danneggiare un Sistema Informativo o un'organizzazione.

Livelli di Vulnerabilità: Il CERT definisce e specifica i livelli di vulnerabilità (ad es. P0, P1, Standard) e che sono inclusi nel Piano di Sicurezza, se applicabile.

2 Requisiti per i contratti di Tipo 1, 2 e 3

1. Sensibilizzazione del personale sulla *Cybersecurity*	Sensibilizzazione e formazione sulla *Cybersecurity*
Il Fornitore deve condurre azioni di sensibilizzazione tra il personale coinvolto nell'esecuzione del Contratto (compresi i subappaltatori), per garantire che siano a conoscenza delle regole di *Cybersecurity* da applicare.	

2. Gestione degli Incidenti relativi a Codici Dannosi	Protezione contro i codici dannosi
Il Fornitore deve definire e implementare processi e procedure per la gestione delle Minacce e dei Codici Dannosi. Il Fornitore è tenuto a rispettare gli obblighi contrattuali e legali in materia di segnalazione al Cliente degli Incidenti di Sicurezza, compresa la violazione di dati personali o non personali.	

3. Sicurezza dei dispositivi mobili utilizzati per il Contratto	Sicurezza dei sistemi mobili, delle postazioni di lavoro e delle attrezzature
Il Fornitore deve garantire l'esistenza di Misure specifiche e adeguate per la sicurezza dei propri dispositivi mobili (tutti i tipi di apparecchiature connesse) utilizzati dal proprio personale (e/o da quello dei propri subappaltatori) nell'ambito dell'esecuzione del Contratto.	

4. Sicurezza dei supporti digitali utilizzati per il Contratto	Sicurezza dei supporti digitali
Il Fornitore deve implementare Misure atte a proteggere i supporti digitali su cui vengono copiati, salvati e/o archiviati (backup) i Dati del Cliente derivanti dall'esecuzione del Contratto. I supporti informatici devono essere oggetto di una Classificazione formalizzata e devono essere in linea con la tipologia di dati copiati, salvati e/o archiviati (backup). L'inventario dei supporti informatici deve essere disponibile e aggiornato. I supporti di backup e di archiviazione informatica devono essere messi in sicurezza e protetti da atti illeciti e Rischi ambientali. Il trasporto dei supporti informatici deve essere soggetto a una procedura documentata.	

5. Allerta in caso di Incidente Grave di Sicurezza	Gestione degli Incidenti di *Cybersecurity*
Gli Incidenti Gravi di Sicurezza devono essere segnalati al CERT TotalEnergies entro quattro (4) ore dal momento in cui il Fornitore ne viene a conoscenza, specificando in particolare la natura e l'entità dell'Incidente Grave di Sicurezza, verificati o potenziali nonché tutte le informazioni che consentano al Cliente di valutarne le conseguenze. Il Fornitore collabora attivamente con il Cliente e aggiorna e completa regolarmente queste informazioni.	

6. Risposta alle richieste di un'unità di crisi del Cliente	Gestione degli Incidenti di *Cybersecurity*
Il Fornitore deve disporre di un'organizzazione di gestione delle crisi che gli consenta di rispondere alle richieste dell'unità di crisi del Cliente nel più breve tempo possibile.	

7. Verifica della continuità operativa relativa al Contratto	Requisiti di continuità operativa
Il Fornitore deve effettuare test sistematici delle proprie soluzioni organizzative, umane e tecniche per garantire continuità operativa e *disaster recovery*, al termine della loro implementazione o evoluzione, integrati da test ed esercitazioni periodiche per valutare il funzionamento di tutti i piani di continuità e *disaster recovery* che ha definito.	

8. Favorire l'uso di strumenti collaborativi	Strumenti collaborativi e spazi di lavoro condivisi
Negli scambi con il Cliente, il Fornitore deve utilizzare, per quanto possibile, gli strumenti di lavoro collaborativo suggeriti o messi a disposizione dal Cliente. In alcuni casi, in particolare per motivi di riservatezza, il Fornitore sarà obbligato a utilizzare gli strumenti di lavoro collaborativo del Cliente.	

9. Cancellare i messaggi di posta elettronica e i documenti relativi al Contratto al termine del Contratto	Strumenti collaborativi e spazi di lavoro condivisi
Salvo ove diversamente stabilito in un documento contrattuale che prevale sui presenti requisiti e salvo che non vi sia un obbligo di legge inderogabile o ai fini della certificazione del prodotto o del servizio oggetto del Contratto, il Fornitore deve cancellare dalle proprie Risorse, comprese le Risorse Specifiche del Contratto, i Dati del Cliente e i messaggi e i documenti elettronici, entro il termine massimo di un mese dalla cessazione del Contratto per qualsiasi motivo.	

10. Rispetto delle regole che disciplinano la messaggistica e gli strumenti collaborativi	Strumenti collaborativi e spazi di lavoro condivisi
Il Fornitore deve rispettare le regole delle buone pratiche associate agli strumenti di messaggistica e collaborativi che gli vengono forniti dal Cliente.	

11. Dichiarare le Tecnologie AI utilizzate nel Contratto	Conoscenza delle Tecnologie AI
Il Fornitore è tenuto a dichiarare per iscritto al Cliente, prima di qualsiasi utilizzo, le Tecnologie AI che intende utilizzare nell'ambito del Contratto, a far data dalla sua sottoscrizione e in qualsiasi momento della sua esecuzione. Lo stesso vale in caso di modifica delle Tecnologie AI durante l'esecuzione del Contratto. Il Cliente può opporsi per iscritto all'uso delle Tecnologie AI, senza doverne dare giustificazione e senza alcun risarcimento o indennizzo al Fornitore, con il Contratto che continuerà alle condizioni inizialmente concordate fino alla sua scadenza. Le Tecnologie AI autorizzate alla data di sottoscrizione del Contratto sono esaustivamente specificate nell'Allegato - Descrizione dei Servizi.	

12. Conformità delle Tecnologie AI utilizzate nel Contratto	Conformità delle Tecnologie AI

Il Fornitore garantisce per sé e per i suoi subappaltatori che le Tecnologie AI:

- non includono alcuna forma di AI vietata (ai sensi della Legge sull'AI) e che nessuna forma di AI vietata è stata precedentemente utilizzata in relazione alle Tecnologie AI nell'esecuzione del Contratto;
- non includono forme di AI ad alto rischio, salvo previo consenso scritto del Cliente e previa applicazione di specifiche e preventive procedure, condizioni contrattuali e tecniche previste dalla Legge sull'AI;
- sono conformi a tutte le leggi applicabili, comprese le disposizioni della Legge sull'AI, e saranno aggiornate in base alle modifiche delle leggi applicabili, entro i termini di legge, senza costi aggiuntivi per il Cliente;
- non sono state soggette, negli ultimi sei (6) mesi, a interruzioni derivanti dall'uso di qualsiasi meccanismo di emergenza per impedire alle Tecnologie AI di eseguire o svolgere una particolare funzione;
- sono implementate nell'ambito di specifiche, progettazione e protocolli di controllo e supervisione rigorosi per limitare l'accesso alle Tecnologie AI e ai dati di addestramento, test, verifica e miglioramento, e che non vi è stato alcun accesso non autorizzato all'algoritmo o al software che incorpora le Tecnologie AI o ai dati di addestramento, test e verifica utilizzati per addestrare e/o migliorare le Tecnologie AI.

13. Monitoraggio delle operazioni eseguite sulle Tecnologie AI	Rispetto degli obblighi relativi alle Tecnologie AI

Il Fornitore:

- fornisce al Cliente tutta la documentazione tecnica e funzionale relativa alle Tecnologie AI;
- adempie tutti gli obblighi definiti nella Legge sull'AI, in particolare le misure di garanzia della qualità, la gestione del rischio, la supervisione umana, l'informazione e la trasparenza;
- conserva le informazioni in forma leggibile e facilmente accessibile per il Cliente o le autorità di regolamentazione, spiegando le operazioni svolte, i risultati prodotti e le decisioni prese o facilitate dalle Tecnologie AI.

3 Requisiti aggiuntivi per i contratti di Tipo 1 e 2

14. Nomina di un responsabile della sicurezza	**Governance della *Cybersecurity***
Il Fornitore deve designare un responsabile della sicurezza. Tale responsabile della sicurezza è il punto di contatto unico per la sicurezza per tutta la durata del Contratto. Deve essere facilmente raggiungibile dal Cliente, in modo sicuro e le modalità di comunicazione devono essere stabilite all'inizio del Contratto.	

15. Nomina di un responsabile per l'attuazione dei rimedi	**Governance della *Cybersecurity***
Il Fornitore deve designare, all'interno dei propri team, una persona responsabile dell'attuazione dei Rimedi, in relazione al Cliente.	

16. Produrre prove documentali della qualificazione	**Certificazioni di *Cybersecurity* del Fornitore**
Il Fornitore deve produrre al Cliente ogni certificazione/accreditamento/denominazione/riferimento a sostegno della propria competenza, in particolare nel settore della *Cybersecurity* e di quella dei suoi dipendenti e subappaltatori nell'ambito del Contratto. Devono essere rese disponibili anche le prove documentali di qualifiche definite previste in un quadro normativo specifico.	

17. Mantenimento delle qualifiche in tema di *Cybersecurity*	**Certificazioni di *Cybersecurity* del Fornitore**
Il Fornitore è responsabile del mantenimento delle certificazioni, degli accreditamenti e delle denominazioni richieste. Le certificazioni di *Cybersecurity* richieste dal Contratto devono essere valide almeno per la durata del Contratto.	

18. Comunicazione della perdita della qualifica	**Certificazioni di *Cybersecurity* del Fornitore**
Il Fornitore deve comunicare al Cliente il prima possibile, e al più tardi entro sette (7) giorni lavorativi, in caso di perdita dell'accreditamento, della denominazione o della certificazione, sia essa una certificazione "aziendale" o una o più certificazioni richieste che si applicano al personale, alle attrezzature, ai servizi o ai processi del Fornitore o dei suoi subappaltatori.	

19. Formazione del personale su questioni di *Cybersecurity*	**Sensibilizzazione e formazione sulla *Cybersecurity***
Il Fornitore deve garantire che i dipendenti assegnati all'esecuzione del Contratto (compresi gli *stakeholder* dei subappaltatori) acquisiscano le conoscenze e le competenze necessarie per l'esecuzione dei compiti loro affidati e per le questioni relative alla *Cybersecurity*. Il Fornitore deve attuare le azioni di formazione necessarie per mantenere le competenze di tutti i dipendenti e degli *stakeholder* interessati. Il Fornitore deve, su richiesta, fornire prove dell'esistenza di un programma di sensibilizzazione e formazione.	

20. Sicurezza delle postazioni di lavoro utilizzate nell'ambito del Contratto	Sicurezza dei sistemi mobili, delle postazioni di lavoro e delle attrezzature
Il Fornitore deve garantire il rafforzamento delle postazioni di lavoro utilizzate dal proprio personale (e/o dai subappaltatori) nell'ambito dell'esecuzione del Contratto, in modo che tali apparecchiature non costituiscano un vettore di violazione della sicurezza delle Risorse utilizzate per l'esecuzione del Contratto (ad esempio, il furto di apparecchiature con conseguente divulgazione di informazioni riservate o perdita di dati essenziali, la propagazione di Codici Dannosi o l'intrusione logica e l'accesso illecito a Risorse sensibili).	

21. Validazione delle Misure di *Cybersecurity* implementate	Progettazione - implementazione - evoluzione delle Risorse Specifiche del Contratto
Il Fornitore deve procedere, prima della consegna, alla verifica tecnica delle Misure di *Cybersecurity* implementate e restituire tali esiti al Cliente al termine di ogni campagna di controllo. Ove applicabile, il report menzionerà gli scostamenti dalle specifiche di sicurezza precedentemente convalidate e i Rischi di sicurezza residui identificati.	

22. Implementazione di un processo di gestione degli Incidenti di *Cybersecurity*	Gestione degli Incidenti di *Cybersecurity*
Il Fornitore deve mettere in atto i mezzi tecnici, umani e organizzativi per rilevare, allertare, supportare e porre rimedio alle allerte o agli Incidenti di *Cybersecurity*, e in particolare per segnalare al Cliente gli Incidenti di *Cybersecurity* riguardanti le Risorse Specifiche del Contratto o i Dati del Cliente utilizzati nell'ambito del Contratto, per reagire efficacemente in base alla natura e alla gravità degli incidenti rilevati, per limitarne l'impatto e per risolvere rapidamente e formalmente tutti gli Incidenti di *Cybersecurity.*	

23. Protezione dei Dati del Cliente utilizzati nell'ambito del Contratto	Strumenti collaborativi e spazi di lavoro condivisi
Il Fornitore deve garantire che tutti i dati e i documenti relativi al Cliente (compresi i Dati del Cliente o quelli generati dal servizio definito nel Contratto o i dati di inventario) rimangano negli ambienti dedicati e sicuri. Il trasferimento di dati o documenti al di fuori di tali ambienti è severamente vietato. In particolare, i documenti e i messaggi scambiati sulla base del Contratto non devono essere comunicati a terzi senza il preventivo consenso del Cliente. Il Fornitore è tenuto a criptare i messaggi elettronici - relativi ai Dati del Cliente - scambiati con il Cliente allo stato dell'arte.	

24. Rispetto delle *best practice* di sviluppo sicuro	Progettazione - implementazione - evoluzione

I programmi e le applicazioni sviluppati dal Fornitore sulla base del Contratto devono essere conformi allo stato dell'arte, in termini di sicurezza degli sviluppi informatici e in particolare alle raccomandazioni di ENISA, ANSSI e OWASP (Open Web Application Security Project). Tali best practice sono descritte nel Piano di Sicurezza e sono convalidate dal Comitato per la Sicurezza.
Il Fornitore applicherà inoltre i principi di “security by design”, “security by default”, considerando, ove opportuno, le specificità imposte dal trattamento dei dati personali.
Il Cliente può fornire un documento di requisiti specifici sulla *Cybersecurity* in base alle tecnologie implementate.

4 Requisiti aggiuntivi per i contratti di Tipo 1

25. Definizione di ruoli e responsabilità in materia di *Cybersecurity*	Governance della *Cybersecurity*
Il Fornitore deve implementare una governance della *Cybersecurity* per garantire il livello di sicurezza atteso dal Cliente e per soddisfare tutti i requisiti di *Cybersecurity*, generali e specifici, previsti dal Contratto e da tutti i suoi allegati. In caso di subappalto, il Fornitore deve stabilire una propria governance con i suoi subappaltatori. Tale governance si basa in particolare sulla partecipazione del Fornitore al Comitato per la Sicurezza (COSEC) che si riunirà secondo i termini definiti dalle parti in un Piano di Sicurezza (PAS). I temi del Comitato per la Sicurezza si concentreranno sul raggiungimento dei livelli di sicurezza attesi dal Cliente, sugli Incidenti di Sicurezza che si sono verificati, su eventuali deroghe alla sicurezza che impattano sul Cliente, sugli Incidenti di Sicurezza in corso, sui risultati degli Audit o delle certificazioni condotte. I piani d'azione risultanti dalle analisi dei Rischi o dagli Audit di *Cybersecurity* devono essere rivisti durante i Comitati per la Sicurezza. Le procedure per i Rimedi, di rilevamento e di reazione devono essere convalidate dal Comitato per la Sicurezza.	

26. Reporting delle azioni di Rimedio nell'ambito del Contratto	Gestione dei Rimedi
Il Fornitore deve redigere e fornire, secondo i termini e la frequenza definiti nel Piano di Sicurezza, i rapporti definiti dal Comitato per la Sicurezza.	

27. Responsabilità degli amministratori	Amministrazione delle Risorse
Il Fornitore deve garantire che il proprio personale (e quello dei suoi subappaltatori) assegnato alle funzioni di amministratore sia ritenuto responsabile delle azioni svolte in virtù dei privilegi concessi. Il processo di responsabilizzazione degli amministratori con riferimento alle rispettive azioni deve essere formalizzato (documentato) e tracciabile.	

28. Garanzia che le postazioni di lavoro degli amministratori rimangano sempre sicure	Gestione delle postazioni di lavoro degli amministratori
Il Fornitore deve garantire che le postazioni di lavoro utilizzate per l'amministrazione siano mantenute in condizioni di sicurezza per tutta la durata del Contratto, e in particolare mantenute aggiornate e prive di virus o Codici Dannosi, al fine di non rappresentare una minaccia per il Sistema Informativo aziendale.	

29. Limitazione dell'accesso a Internet dalle postazioni di lavoro degli amministratori	Gestione delle postazioni di lavoro degli amministratori
Gli account degli amministratori e le postazioni di lavoro utilizzate per l'amministrazione devono essere configurati in modo da limitare l'accesso a Internet (posta elettronica, navigazione) allo stretto necessario per l'esecuzione del Contratto.	

30. Applicazione del principio del privilegio minimo per gli amministratori	Gestione delle postazioni di lavoro degli amministratori
I dipendenti del Fornitore (e quelli dei suoi subappaltatori) con diritti di amministratore devono avere account personali e univoci (nessun account condiviso) e rispettare la separazione dei ruoli per l'operato dell'amministratore. I diritti di amministratore devono essere assegnati e gestiti in conformità al principio del privilegio minimo.	

31. Crittografia dei dati delle postazioni di lavoro dell'amministratore	Gestione delle postazioni di lavoro degli amministratori
Tutti i supporti di memorizzazione utilizzati per l'amministrazione del Sistema Informativo del Cliente devono essere crittografati. Le sessioni dell'amministratore devono essere automaticamente interrotte dopo un periodo di inattività specificato e in conformità con lo stato dell'arte.	

32. Garanzia della sicurezza fisica delle postazioni di lavoro dell'amministratore	Gestione delle postazioni di lavoro degli amministratori
Il Fornitore deve garantire di implementare dispositivi antifurto e per la prevenzione di indiscrezioni visive. Le operazioni dell'amministratore non devono in nessun caso essere eseguite in uno spazio aperto al pubblico o visibile al pubblico.	

33. Report sugli Incidenti di *Cybersecurity*	Gestione degli Incidenti di *Cybersecurity*
Il Fornitore deve aggiornare i report relativi agli Incidenti di *Cybersecurity* e inviarli al Cliente secondo la periodicità e con le informazioni previste nel Piano di Sicurezza.	

5 Requisiti aggiuntivi per contratti di Tipo 1 con Risorse Specifiche del Contratto

I seguenti requisiti si applicano solo se il Contratto include risorse (attrezzature) sotto la responsabilità del Fornitore e dei suoi subappaltatori che sono implementate specificamente per il Contratto, comprese in particolare le postazioni di lavoro dei dipendenti coinvolti nel Contratto e le Risorse dedicate all'esecuzione del Contratto.

34. Mappatura delle Risorse Specifiche del Contratto	**Conoscenza delle Risorse**
Il Fornitore deve mappare le Risorse Specifiche del Contratto implementate sulla base del Contratto sotto forma di schemi architettonici e deve mantenere un inventario che descriva in dettaglio le principali caratteristiche necessarie per mantenere la sicurezza. Tale mappatura deve essere convalidata dal Comitato per la Sicurezza.	

35. Mantenere aggiornata la mappatura delle Risorse Specifiche del Contratto	**Conoscenza delle Risorse**
Il Fornitore deve mantenere aggiornata la mappatura delle Risorse Specifiche del Contratto. Le modifiche principali devono essere presentate al Comitato per la Sicurezza entro un lasso di tempo sufficiente e ragionevole prima di essere implementate.	

36. Classificazione delle Risorse Specifiche del Contratto	**Conoscenza delle Risorse**
Il Fornitore deve identificare le varie Risorse Specifiche del Contratto e stabilire, in collaborazione con il Cliente e in base al sistema di riferimento del Cliente, una Classificazione di tali Risorse.	

37. Formare gli operatori sulla classificazione delle Risorse Specifiche del Contratto	**Conoscenza delle Risorse**
Il Fornitore deve formare qualsiasi soggetto coinvolto nell'uso o nella gestione delle Risorse Specifiche del Contratto sul Profilo di Classificazione di tali Risorse. Gli amministratori devono padroneggiare le Misure di *Cybersecurity* applicabili.	

38. Analisi dei Rischi di *Cybersecurity* per le Risorse Specifiche del Contratto	**Gestione dei Rischi di *Cybersecurity***
Il Fornitore deve effettuare e mantenere aggiornata l'Analisi dei Rischi di *Cybersecurity* delle Risorse Specifiche del Contratto, inclusi i dati elaborati da tali Risorse, secondo un metodo di analisi concordato di comune accordo. Il Fornitore deve essere in grado di fornire in qualsiasi momento un rapporto dettagliato su tutti i Rischi identificati, classificati in base alla sensibilità, ai mezzi di prevenzione o mitigazione e di rivelare i Rischi residui.	

39. Applicazione di un piano d'azione per ridurre i Rischi identificati	**Gestione dei Rischi di *Cybersecurity***
Il Fornitore deve mettere in atto, a proprie spese, un piano d'azione in relazione all'Analisi dei Rischi di *Cybersecurity* o ai risultati di un Audit di *Cybersecurity*, per ridurre o prevenire il verificarsi di tali Rischi di *Cybersecurity* o per limitarne le conseguenze. Il Fornitore deve implementare le misure correttive necessarie a seguito delle notifiche del Cliente come parte del suo programma contro il *data leak*.	

40. Protezione delle Risorse Specifiche del Contratto da Codici Dannosi	Protezione contro i codici dannosi
Il Fornitore deve mettere in atto, per le sue Risorse Specifiche del Contratto, un dispositivo di protezione contro i Codici Dannosi.	

41. Report periodico sullo stato delle azioni per combattere i Codici Dannosi	Protezione contro i codici dannosi
Il Fornitore deve presentare regolarmente al Comitato per la Sicurezza un rapporto di monitoraggio quantitativo (completezza) e qualitativo (efficacia) dei mezzi di lotta contro i Codici Dannosi implementati per proteggere le Risorse Specifiche del Contratto, secondo una periodicità da definire al momento della prima riunione del Comitato per la Sicurezza.	

42. Rafforzare i sistemi di base delle Risorse Specifiche del Contratto	Sicurezza dei sistemi di base, delle postazioni di lavoro e delle apparecchiature mobili
Il Fornitore deve implementare le Misure tecniche, umane e organizzative necessarie e pertinenti, per garantire la sicurezza dei Sistemi di base (Sistemi operativi, *middleware*, applicazioni e relativi servizi di comunicazione e sicurezza) delle Risorse Specifiche del Contratto. Tali Misure devono consentire di preservare la riservatezza, la disponibilità e l'integrità dei dati elaborati.	

43. Protezione dei dati delle Risorse Specifiche del Contratto	Sicurezza dei sistemi di base, delle postazioni di lavoro e delle apparecchiature mobili
Il Fornitore deve documentare e implementare i mezzi necessari e pertinenti per proteggere l'amministrazione, la manutenzione e il funzionamento dei sistemi di base (Sistemi operativi, *middleware*, applicazioni e servizi di comunicazione e sicurezza correlati) delle Risorse Specifiche del Contratto.	

44. Protezione della rete utilizzata dalle Risorse Specifiche del Contratto	Sicurezza di Rete
Il Fornitore deve implementare e aggiornare le Misure di sicurezza, necessarie, pertinenti e conformi allo stato dell'arte, per garantire la sicurezza delle reti utilizzate dalle Risorse Specifiche del Contratto, per prevenire o limitare le conseguenze dei Rischi di *Cybersecurity.*	

45. Adottare una procedura di autorizzazione per l'accesso alle Risorse Specifiche del Contratto	Controlli di accesso logico e Autorizzazioni
La gestione dell'accesso logico alle Risorse Specifiche del Contratto, implementata dal Fornitore ai fini del Contratto, deve essere descritta in un Piano di Sicurezza (se presente) o in un documento inviato al Cliente prima dell'inizio dei Servizi/Fornitura e ogni volta che viene aggiornato. L'accesso al Sistema Informativo del Cliente è soggetto solo alle regole e alle procedure del Cliente.	

46. Audit di *Cybersecurity* delle Risorse Specifiche del Contratto	Audit di *Cybersecurity*
Il Fornitore deve condurre Audit di Cybersecurity delle Risorse Specifiche del Contratto. Tali Audit riguardano principalmente la conformità ai requisiti stabiliti nel presente documento. Possono anche riguardare le Misure di *Cybersecurity* applicabili a normative specifiche, come quelle applicabili al trattamento dei dati personali. Tali Audit non escludono l'applicazione di altre disposizioni contrattuali relative agli Audit delle Risorse e dei Sistemi Informativi del Fornitore, inclusi i test di penetrazione/red team. Tali Audit ricadono sotto la responsabilità del Fornitore, salvo diverso accordo preventivo tra le Parti.	

47. Trasmissione degli esiti degli Audit di Cybersecurity sulle Risorse Specifiche del Contratto	Audit di Cybersecurity
I risultati degli Audit effettuati dal Fornitore sulle Risorse Specifiche del Contratto saranno comunicati al Cliente. Un certificato di Audit, nonché un riepilogo del report di Audit e l'avanzamento delle azioni di correzione e miglioramento, saranno forniti gratuitamente al Cliente entro e non oltre trenta (30) giorni lavorativi dalla data del report di Audit. Tutte le azioni di bonifica e miglioramento saranno a spese del Fornitore.	

48. Rimediare alle vulnerabilità delle Risorse Specifiche del Contratto	Gestione dei Rimedi
Il Fornitore deve definire e implementare una procedura di Rimedio per correggere le vulnerabilità e le configurazioni errate delle Risorse Specifiche del Contratto.	

49. Coordinare i Rimedi entro le scadenze contrattuali	Gestione dei Rimedi
Il Fornitore deve implementare i mezzi necessari per applicare i Rimedi alle Risorse Specifiche del Contratto, entro le scadenze definite nel Piano di Sicurezza per i livelli di vulnerabilità "Critico" o "P0", "Urgente" o "P1" e Standard (predefinito). I Rimedi P0 e P1 sono definiti da CERT TotalEnergies e comunicati al Fornitore.	

50. Separare gli ambienti dei Sistemi Informativi di produzione dagli ambienti non di produzione	Progettazione - implementazione - evoluzione delle Risorse Specifiche del Contratto
Il Fornitore deve garantire la separazione degli ambienti dei Sistemi Informativi di produzione e dei Sistemi Informativi non di produzione. I dati di produzione non devono essere utilizzati in ambienti non di produzione senza il previo consenso scritto del Cliente.	

51. Specifica delle Misure di *Cybersecurity* per soddisfare i requisiti per le evoluzioni delle Risorse Specifiche del Contratto	Progettazione - implementazione - evoluzione delle Risorse Specifiche del Contratto
Il Fornitore deve specificare e documentare le Misure di sicurezza da implementare per rispondere, nell'ambito della progettazione e/o evoluzione delle Risorse Specifiche del Contratto, i livelli di sicurezza e continuità del servizio richiesti dal Cliente. Il Fornitore deve avvisare il Cliente di una possibile incapacità di offrire Misure di *Cybersecurity* tali da soddisfare i requisiti di sicurezza richiesti.	

52. Protezione dell'accesso fisico alle Risorse Specifiche del Contratto	Categorizzazione delle zone di sicurezza
Il Fornitore deve garantire che siano in atto le Misure di sicurezza fisica adattate al livello di sensibilità delle Risorse Specifiche del Contratto, inclusi i dati trattati sulla base del Contratto, e in conformità con le normative applicabili. Il Fornitore deve garantire la protezione dell'accesso fisico alle varie zone di sicurezza in cui si trovano le Risorse Specifiche del Contratto mediante dispositivi graduati e pertinenti a seconda del tipo di zona da proteggere. Il Fornitore deve garantire che siano in atto le Misure di monitoraggio e controllo per i dispositivi di protezione dell'accesso fisico.	

53. Protezione antincendio delle Risorse Specifiche del Contratto	Protezione contro i Rischi ambientali
Il Fornitore deve garantire l'attuazione di Misure di sicurezza antincendio per proteggere le Risorse Specifiche del Contratto. Tali Misure devono includere, in particolare: - Mezzi di rilevamento incendi. - Mezzi di soppressione incendi. - Misure per la verifica periodica dei mezzi di protezione e antincendio. - Procedure da attuare in caso di incendio re. Il Fornitore deve comunicare al Cliente l'elenco delle Misure di protezione antincendio messe in atto.	

54. Protezione contro i danni causati dall'acqua	Protezione contro i Rischi ambientali
Il Fornitore deve garantire l'attuazione delle Misure di protezione contro i danni causati dall'acqua. Il Fornitore deve comunicare al Cliente l'elenco delle Misure di protezione contro i danni causati dall'acqua messe in atto.	

55. Garantire la fornitura di servizi essenziali per la protezione delle Risorse Specifiche del Contratto	Protezione contro i Rischi ambientali
Il Fornitore deve garantire l'installazione e la corretta manutenzione dell'alimentazione elettrica, dell'aria condizionata e la protezione delle Risorse Specifiche del Contratto.	

56. Trasmissione degli esiti dell'Audit di *Cybersecurity* sulle Risorse Specifiche del Contratto	Audit di *Cybersecurity*
I risultati degli Audit effettuati dal Fornitore sulle Risorse Specifiche del Contratto saranno comunicati al Cliente. Un certificato di Audit, nonché un riepilogo del report di Audit e l'avanzamento delle azioni di Rimedio e miglioramento, saranno forniti gratuitamente al Cliente entro e non oltre trenta (30) giorni lavorativi dalla data del report di Audit. Tutti i Rimedi e le azioni di miglioramento saranno a spese del Fornitore.	

57. Implementazione di un Centro Operativo di Sicurezza (SOC)	Tracciabilità e monitoraggio
Il Fornitore deve monitorare tramite un Centro Operativo di Sicurezza (SOC) le Risorse Specifiche del Contratto che non sono integrate nel SOC del Cliente. Il Fornitore dovrà stabilire, all'inizio del contratto, un protocollo di comunicazione tra il proprio SOC e quello del Cliente.	

58. Segnalazione di Incidenti di *Cybersecurity*	Gestione degli Incidenti di *Cybersecurity*
Il Fornitore deve notificare al CERT TotalEnergies qualsiasi incidente che influisca o possa incidere sulla *Cybersecurity* delle Risorse Specifiche del Contratto, entro i termini e secondo i termini concordati contrattualmente o in applicazione di un regolamento, tale termine è fissato di default a un massimo di ventiquattro ore dal momento in cui il Fornitore viene a conoscenza dell'Incidente di *Cybersecurity*.	

59. Trasmissione di eventi che consentono il monitoraggio della *Cybersecurity* di determinate Risorse Specifiche del Contratto	Tracciabilità e monitoraggio
Se necessario, il Comitato per la Sicurezza può definire specifici Eventi e gli scenari di rilevamento (log, eventi o regole di rilevamento) da trasmettere al SOC del Cliente in modo che sia in grado di rilevare l'accaduto. Questi eventi generati dalle Risorse Specifiche del Contratto devono essere indirizzati ai sistemi di raccolta dei log del Cliente.	

60. Implementazione di un Computer Emergency Response Team (CERT)	Gestione Incidenti di *Cybersecurity*
Il Fornitore deve descrivere nel Piano di Sicurezza la propria organizzazione di risposta a un Incidente di *Cybersecurity*, equivalente all'istituzione di un CERT (Computer Emergency Response Team) per il monitoraggio e la risposta agli Incidenti di *Cybersecurity* che coinvolgono Risorse Specifiche del Contratto che non sono integrate nei dispositivi SOC e CERT di TotalEnergies. Designa un punto di contatto in grado di inviare segnalazioni al CERT TotalEnergies. Il Fornitore deve stabilire un protocollo di comunicazione tra il proprio CERT e quello del Cliente.	

61. Utilizzo dei mezzi di Autenticazione forniti	Amministrazione delle Risorse Specifiche del Contratto
Il Fornitore utilizzerà i mezzi di Autenticazione messi a disposizione dalla Società per accedere ai Sistemi Informativi del Cliente. I mezzi di Autenticazione per accedere alle Risorse Specifiche del Contratto devono essere preventivamente convalidati dal Cliente.	

62. Protezione delle password per le Risorse Specifiche del Contratto	Amministrazione delle Risorse Specifiche del Contratto
Il personale assegnato al Contratto deve proteggere le proprie password e i propri mezzi di Autenticazione, in conformità con i metodi convalidati dal Comitato per la Sicurezza e avvisare senza indugio il SOC del Cliente in caso di compromissione o sospetto di compromissione.	

63. Protezione dei flussi di amministrazione delle Risorse Specifiche del Contratto	Amministrazione delle Risorse Specifiche del Contratto
Il Fornitore deve utilizzare i mezzi e i metodi di accesso convalidati dal Comitato per la Sicurezza per amministrare le Risorse Specifiche del Contratto. Il Fornitore si impegna a non tentare di eludere le Misure di *Cybersecurity* implementate dal Cliente.	

64. Monitoraggio delle azioni dell'amministratore in relazione alle Risorse Specifiche del Contratto	Amministrazione delle Risorse Specifiche del Contratto
Il Fornitore deve garantire che le azioni degli account amministrativi utilizzati con riferimento alle Risorse Specifiche del Contratto vengano registrate, conservate per un periodo predefinito di dodici (12) mesi consecutivi e che gli Eventi vengano sottoposti ad Audit per attività o azioni sospette.	

65. Garantire la disponibilità delle Risorse Specifiche del Contratto	Requisiti di continuità operativa
Il Fornitore deve valutare i Rischi di indisponibilità delle Risorse Specifiche del Contratto che potrebbero danneggiare il Cliente. Il Fornitore deve implementare soluzioni (tecniche, umane e organizzative) che coprano gli scenari di indisponibilità identificati e che consentano di garantire il livello minimo di servizio richiesto dal Cliente in una situazione di crisi e la ripresa del servizio in condizioni conformi alle soglie di tolleranza definite con il Cliente.	

66. Backup di emergenza	Continuità operativa
Il Fornitore deve eseguire backup di produzione separati e backup di backup che coprano tutte le Risorse Specifiche del Contratto (configurazione del sistema, delle apparecchiature di rete e di telecomunicazione, software di base, applicazioni e dati del Cliente). Il Fornitore deve esternalizzare il backup (utilizzato come parte dell'esecuzione dei piani di continuità) in una sede sufficientemente distante dal sito di produzione per non subire danni da un disastro che potrebbe avere un impatto su tale sito. Il Fornitore deve garantire la capacità di accedere in modo permanente a tutti i backup di emergenza, indipendentemente dalla loro posizione.	

67. Documentare la continuità operativa relativa al Contratto	Requisiti di continuità operativa
Il Fornitore deve eseguire test sistematici delle proprie soluzioni organizzative, umane e tecniche per garantire continuità operativa e *disaster recovery*, al termine della loro implementazione o evoluzione, integrati da test ed esercitazioni regolari per valutare il funzionamento di tutti i piani di continuità e *disaster recovery* che ha definito. Il Fornitore deve ottenere il consenso scritto del Cliente prima di condurre test ed esercitazioni basati su uno spegnimento parziale o completo e programmato delle Risorse Specifiche del Contratto o delle altre Risorse necessarie per la Fornitura (incluso qualsiasi passaggio a sistemi di backup). Tutti i test e le esercitazioni dei dispositivi di *disaster recovery* e continuità operativa devono seguire protocolli documentati dal Fornitore. La loro esecuzione deve essere oggetto di un bilancio che mostri i risultati in conformità con le aspettative e/o le anomalie rilevate, che il Fornitore deve trasmettere al Cliente e che sarà commentato nella riunione del Comitato per la Sicurezza.	

Fine del documento