NIS2

CLAUSOLE CONTRATTUALI PER I FORNITORI

INDICE

1. CONTESTO NORMATIVO, STRUTTURA DOCUMENTALE E DEFINIZIONI

La Direttiva (UE) 2022/2555 e relativa normativa di recepimento – D.lgs. 138/2024 (indicati complessivamente nel prosieguo come "Direttiva" o "NIS2") introducono un quadro regolamentare aggiornato nell'ottica di rafforzare la sicurezza delle reti e dei sistemi informativi nell'Unione Europea, mirando a migliorare la resilienza e la sicurezza informatica, soprattutto alla luce delle minacce emergenti e dell'evoluzione tecnologica.
Tra gli obblighi individuati in capo ai soggetti "essenziali" o "importanti", rientrano anche quelli connessi alla sicurezza della propria *supply chain*, ovvero l'insieme dei rapporti tra il soggetto e i suoi fornitori. L'obiettivo primario è quello di garantire una efficace gestione dei rischi derivanti dalla catena di approvvigionamento: conoscere e prevenire possibili vulnerabilità all'interno di questa diventa, ai sensi della Direttiva, uno degli elementi centrali per garantirne il rispetto.
Alla luce dell'approccio multirischio individuato dalla stessa Direttiva, i presidi di sicurezza riguardanti soggetti terzi critici rispetto alla struttura del soggetto "essenziale" o "importante" passano anche attraverso l'individuazione di una disciplina contrattuale, che individui specifici obblighi in base ai rischi della fornitura.

La Società si è quindi dotata di un set di clausole contrattuali volte a disciplinare elementi di cybersicurezza nei rapporti negoziali con le proprie controparti, declinando i vari obblighi in ragione del livello di criticità NIS2 della catena di approvvigionamento come emerso a seguito delle attività di mappatura e di valutazione dei rischi effettuate dalla Società nel rispetto dei criteri individuati dalla Direttiva.

I modelli di clausole contrattuali standard di cui al presente documento sono state quindi predisposte per disciplinare aspetti di cybersicurezza a seconda delle tipologie di relazione contrattuale, in particolare:

A. Rapporti con fornitori non critici NIS2
B. Rapporti con fornitori critici NIS2

Nelle clausole di seguito indicate, sono adottate le seguenti definizioni:

- "Società": si intende il soggetto giuridico che ha adottato il presente documento come meglio identificato nell'intestazione dello stesso;
- "Fornitore": si intende la persona fisica o giuridica che di volta in volta fornisce prodotti o eroga servizi alla Società;

2. ASPETTI DI CYBER SICUREZZA NEI RAPPORTI TRA LA SOCIETA' ED I PROPRI FORNITORI NIS2 NON CRITICI

La clausola standard di seguito riportata è volta a perimetrare le responsabilità contrattuali in tema di cybersecurity nei rapporti tra la Società ed i fornitori dalla stessa valutati non critici NIS2.

OBBLIGHI DEL FORNITORE IN TEMA DI CYBERSICUREZZA
1. Il Fornitore si impegna a garantire, per tutta la durata del presente Contratto, l'adozione, il mantenimento e il costante aggiornamento di misure tecniche e organizzative adeguate a garantire la sicurezza, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di rete, delle infrastrutture di comunicazione elettronica e dei canali di trasmissione dei dati utilizzati per l'esecuzione delle attività oggetto del presente Contratto. Nell'esecuzione del presente Contratto, il Fornitore si impegna altresì a garantire livelli di sicurezza conformi alle normative vigenti, quali a titolo meramente esemplificativo e non esaustivo il D.lgs. 138/2024 di recepimento della Direttiva (UE) n. 2022/2555 (c.d. "NIS2"), e alle linee guida e best practices di settore tempo per tempo applicabili, tali da consentire il corretto e costante adempimento degli obblighi assunti con la Società e garantire a quest'ultima la costante disponibilità, senza ritardi e/o interruzioni, delle attività pattuite e la conformità delle stesse alle normative tempo per tempo vigenti nel corso di validità del presente Contratto. L'elenco aggiornato delle misure minime di sicurezza adottate dal Fornitore è indicato all'Allegato "Misure di sicurezza NIS2" del presente Contratto, eventuali modifiche delle stesse dovranno risultare da atto sottoscritto dalle Parti a pena di nullità. 2. Il Fornitore si impegna a svolgere attività periodiche di verifica sui sistemi e/o reti propri e di eventuali sub-fornitori di cui si avvale per l'esecuzione del Contratto, per monitorarne la funzionalità e sicurezza. A tal fine il Fornitore si impegna a consegnare alla Società, previa richiesta di quest'ultima, senza indebiti ritardi e in ogni caso entro 15 (quindici)

giorni dalla richiesta, le risultanze di tali attività di verifica dallo stesso svolte. Il Fornitore si impegna altresì a consentire alla Società – direttamente per il tramite del proprio personale specializzato o con l'ausilio di terzi individuati dalla Società e debitamente vincolati ad obblighi di riservatezza – di svolgere tali attività di verifica presso il Fornitore medesimo. Qualunque non conformità che dovesse emergere da tali attività di verifica, fermo restando ogni diritto di legge ivi compreso il risarcimento del danno, dovrà essere risolta dal Fornitore sopportandone i relativi costi e/o oneri e comunque in un ragionevole lasso di tempo, in ogni caso non superiore a 30 (trenta) giorni di calendario, salvo oggettive, motivate e comprovate ragioni che non permettano il rispetto di tale termine e/o salvo motivi di urgenza tali da raccomandare un adeguamento entro un termine più breve.

3. Il Fornitore dichiara e garantisce che le attività di cui al Contratto saranno eseguite nel rispetto delle modalità e tempistiche pattuite come meglio dettagliate nell'Allegato "Service Level Agreement" al presente Contratto: eventuali modifiche delle stesse dovranno risultare da atto sottoscritto da entrambe le Parti a pena di nullità.
4. Il Fornitore altresì si impegna, sotto propria diretta responsabilità, a imporre nei confronti dei propri sub-fornitori, quantomeno obblighi in materia di sicurezza analoghi a quelli assunti dal Fornitore con il presente Contratto, assicurando l'adozione da parte dei propri sub-fornitori quantomeno delle misure di cui all'Allegato "Misure di sicurezza NIS2" di cui al presente Contratto.
5. Fatte salve ulteriori specifiche concordate con la Società, il Fornitore è tenuto a comunicare via PEC alla Società qualsiasi incidente e/o potenziale incidente di sicurezza informatica dallo stesso subito, senza indebiti ritardi e comunque entro 24 ore dal momento in cui il Fornitore ne sia venuto a conoscenza, fornendo in detta PEC indicazioni circa le specifiche e le potenziali conseguenze dell'incidente per la Società, gli eventuali ritardi e/o interruzioni nell'erogazione dei servizi pattuiti ai sensi del presente Contratto, oltre alle tempistiche e le misure di ripristino adottate e relative tempistiche di implementazione. Entro i successivi 5 (cinque) giorni lavorativi il Fornitore si impegna altresì a fornire alla Società una relazione tecnica dettagliata dell'incidente, in cui oltre alle informazioni di cui sopra dovranno essere opportunamente descritte le cause

dell'incidente occorso e le misure adottate per evitare futuri incidenti simili. Il Fornitore si impegna altresì a cooperare pienamente con la Società per valutare le conseguenze dell'incidente, limitare i danni e ripristinare la normale operatività.

6. Nello svolgimento delle attività oggetto del presente Contratto, il Fornitore si impegna a impiegare esclusivamente personale che presenti requisiti di comprovata competenza tecnica, professionalità, affidabilità e integrità, adeguati alle attività pattuite.
7. Laddove l'esecuzione delle attività pattuite tra le Parti comporti l'accesso da parte del Fornitore a reti e/o sistemi della Società, il Fornitore dichiara e garantisce che ciascun utente afferente alla propria organizzazione – per tali intendendosi, a titolo esemplificativo e non esaustivo, dipendenti e/o collaboratori e/o terzi autorizzati dal Fornitore – a tal fine:
   - Ove forniti dalla Società al Fornitore in esecuzione del presente Contratto, utilizzi esclusivamente gli strumenti e le modalità di autenticazione ai sistemi e reti della Società indicate da quest'ultimo;
   - In tutti gli altri casi, utilizzi sistemi adeguati a garantire la conformità ai principi di univocità ed esclusività degli accessi, nel rispetto degli obblighi normativi vigenti e delle linee guida e best practices di settore tempo per tempo applicabili, nonché delle politiche di accesso adottate dalla Società.
8. In tutti i casi di cessazione, a qualsiasi causa dovuta, del presente contratto, il Fornitore si impegna, ove applicabile in base alle attività pattuite, a:
   - Restituire tutti i dati e/o le informazioni di proprietà della Società dallo stesso conservati, in un formato leggibile e comunemente utilizzato, nelle modalità e tempistiche che la Società andrà ad indicare, fatti salvi eventuali vincoli di natura tecnica che il Fornitore si obbliga a dichiarare. Una volta concluse le attività di restituzione, il Fornitore si impegna a darne comunicazione scritta alla Società;
   - Terminate le attività di restituzione, il Fornitore dovrà altresì cancellare immediatamente e definitivamente da qualsivoglia supporto per la conservazione nella propria disponibilità, tutti i dati e/o informazioni di proprietà della Società, dando comunicazione scritta alla Società dell'avvenuta cancellazione, fatti salvi eventuali

obblighi di legge che determino un'ulteriore conservazione da parte del Fornitore: in tali casi, il Fornitore si impegna a comunicare, senza indebito ritardo, tali obblighi;

- Fornire ragionevole assistenza e supporto per la migrazione dei dati a un nuovo fornitore, qualora richiesto dalla Società;
- Indicare per iscritto alla Società l'elenco degli accessi a reti/sistemi applicativi della medesima attivi alla data di cessazione del presente Contratto, così da consentire alla Società stesso la chiusura/disattivazione dei predetti accessi;
- Garantire che tutte le fasi sopra indicate siano comunque presidiate dalle misure di sicurezza sussistenti in vigenza di contratto o almeno parificabili, per quanto applicabili.

9. La violazione degli obblighi previsti dal presente articolo costituirà causa di grave inadempimento contrattuale e la Società potrà risolvere il contratto senza preavviso alcuno, ai sensi e per gli effetti di cui all'art. 1456 Cod. Civ., mediante semplice comunicazione scritta (a mezzo raccomandata a/r o via pec), restando salvo il risarcimento di eventuali danni.

3. ASPETTI DI CYBER SICUREZZA NEI RAPPORTI TRA LA SOCIETA' ED I PROPRI FORNITORI NIS2 CRITICI

La clausola di seguito riportata è volta a perimetrare le responsabilità contrattuali in tema di cybersecurity nei rapporti tra la Società ed i fornitori dalla stessa valutati critici NIS2.

OBBLIGHI DEL FORNITORE IN TEMA DI CYBERSICUREZZA

1. <u>Ruoli e responsabilità in tema di cybersicurezza</u>

1.1 Nell'esecuzione del Contratto, ove non diversamente pattuito per iscritto le Parti riconoscono ed accettano che la Società:

A. definisce i requisiti di sicurezza, continuità, riservatezza e tracciabilità applicabili;

B. verifica la conformità del Fornitore alle normative applicabili ed agli obblighi negoziali assunti, a tal fine esercitando il diritto di audit come previsto dal presente Contratto.

1.2 Nell'esecuzione del Contratto, ove non diversamente pattuito per iscritto le Parti riconoscono ed accettano che il Fornitore:

i. è responsabile dell'esecuzione sicura e conforme del Contratto, nel rispetto delle normative applicabili e del presente Contratto;

ii. adotta tutte le misure tecniche e organizzative indicate dalla Società e in ogni caso quanto necessario per garantire la disponibilità, integrità, riservatezza e resilienza dei sistemi e dei dati della Società, nel rispetto delle normative applicabili e del presente Contratto.

1.3 Il Fornitore e la Società si impegnano reciprocamente a garantire una collaborazione trasparente, tempestiva e continuativa per l'intera durata del Contratto, al fine di assicurare la sicurezza, l'efficacia e la resilienza delle attività pattuite e garantire la conformità al Contratto e alle normative applicabili in materia di sicurezza, protezione dei dati e continuità operativa.

2. <u>Affidabilità delle risorse umane e formazione del personale</u>

2.1 Per l'esecuzione delle attività oggetto del presente Contratto, il Fornitore dichiara e garantisce:

i. di aver accuratamente selezionato e di impiegare esclusivamente personale che presenti requisiti di comprovata competenza tecnica, esperienza, professionalità, affidabilità ed integrità, adeguati alla natura e alla complessità delle prestazioni da svolgere, nel pieno rispetto delle normative tempo per tempo vigenti. Il Fornitore si impegna a mantenere tale adeguatezza per tutta la durata del Contratto.

ii. che, alla data di sottoscrizione del presente Contratto, non sussistono situazioni di conflitto di interessi nei confronti della Società, per tale intendendosi ai fini del presente Contratto qualsiasi situazione, anche solo potenziale, in cui il Fornitore, i suoi soci, amministratori, dipendenti, collaboratori, consulenti o subappaltatori, direttamente o indirettamente, abbiano un interesse personale, finanziario o professionale che possa interferire, anche solo in apparenza, con l'imparzialità, l'indipendenza o la correttezza nell'esecuzione del Contratto. A titolo esemplificativo ma non esaustivo costituiscono conflitto di interessi:

- l'esistenza di rapporti societari, economici o professionali tra il Fornitore (o soggetti a esso riconducibili) e la Società o suoi concorrenti anche indiretti;

- ogni situazione in cui l'interesse privato del Fornitore o di suoi incaricati possa prevalere o interferire con il corretto adempimento delle obbligazioni contrattuali.

Il Fornitore si impegna a comunicare immediatamente e per iscritto alla Società qualsiasi situazione, anche sopravvenuta, che possa dar luogo a un conflitto di interessi, anche solo potenziale.

iii. che tutte le risorse impiegate nell'esecuzione del Contratto sono vincolate da specifici ed adeguati obblighi di riservatezza, formalizzati per iscritto, e sono state adeguatamente istruite e formate in materia di protezione dei dati personali, sicurezza delle informazioni, e rispetto delle applicabili procedure aziendali della Società dalla stessa comunicate al Fornitore.

2.2 La Società, senza che ciò comporti variazioni rispetto ai corrispettivi pattuiti tra le Parti, potrà richiedere la sostituzione di una o più risorse del Fornitore impiegate nell'esecuzione del Contratto, qualora si verifichi anche una sola delle seguenti condizioni:

i. Carenze tecniche o professionali accertate a insindacabile giudizio della Società e tali da compromettere la qualità, l'efficacia e/o la sicurezza delle attività pattuite;

ii. Condotte incompatibili con gli obblighi di riservatezza, integrità e affidabilità richiesti per le attività pattuite;

iii. Situazioni di conflitto di interesse, anche potenziale, tra la risorsa incaricata e la Società o soggetti terzi.

In tali casi il Fornitore, ricevuta richiesta scritta dalla Società, dovrà procedere alla sostituzione della risorsa contestata entro e non oltre 5 (cinque) giorni lavorativi, designando un sostituto con pari o superiore qualifica ed esperienza, previa approvazione della Società e, in ogni caso, garantendo la continuità dell'esecuzione delle attività pattuite.

2.3 Su richiesta scritta del Società, senza indebiti ritardi e in ogni caso entro e non oltre 5 (cinque) giorni lavorativi dalla richiesta, il Fornitore si impegna a mettere a disposizione della Società:

i. l'elenco nominativo delle risorse umane impiegate nell'esecuzione del Contratto aggiornato alla data della predetta richiesta;
ii. idonea documentazione attestante l'avvenuta formazione periodica svolta da tali risorse in materia di protezione dei dati personali e sicurezza delle informazioni;
iii. idonea documentazione da cui risultino gli adeguati obblighi di riservatezza assunti da tali risorse e la sussistenza in capo alle stesse dei requisiti tecnici e professionali richiesti dall'incarico.

3. <u>Conformità e audit di sicurezza</u>

3.1 Il Fornitore si impegna a svolgere, con frequenza periodica, audit interni sulla sicurezza dei sistemi, delle reti e in generale dell'infrastruttura informatica dallo stesso utilizzati nell'esecuzione del presente Contratto, al fine di verificarne, quantomeno, la conformità ai requisiti previsti dal presente Contratto e dalla normativa tempo per tempo vigente. Il Fornitore garantisce di effettuare tali audit secondo standard internazionali e/o best practices e/o linee guida di settore, con frequenza almeno annuale nonché ogniqualvolta si verifichino eventi o sospetti eventi di sicurezza che possano compromettere l'integrità, la disponibilità e/o la riservatezza dei servizi o dei dati trattati per conto della Società. Il Fornitore si impegna a comunicare le risultanze di tali audit entro 15 (quindici) giorni lavorativi dalla richiesta scritta della Società.

3.2 Laddove il Fornitore, nell'esecuzione del Contratto, si affidi a terzi sub-fornitori, si impegna a svolgere con cadenza periodica audit presso i sub-fornitori, al fine di verificarne quantomeno la conformità ai requisiti previsti dal presente Contratto e dalla normativa tempo per tempo vigente. Il Fornitore garantisce di effettuare tali audit secondo standard internazionali e/o best practices e/o linee guida di settore, con frequenza almeno annuale nonchè ogniqualvolta si verifichino eventi o sospetti eventi di sicurezza che possano compromettere l'integrità, la disponibilità e/o la riservatezza dei servizi o dei dati della Società. Il Fornitore si impegna a redigere un report sintetico dell'audit svolto contenente quantomeno una breve descrizione delle attività di audit svolte ed il dettaglio di eventuali criticità, non conformità o inadempimenti rilevati nel sub-fornitore, provvedendo a comunicarlo alla Società entro 15 (quindici) giorni lavorativi dalla data di svolgimento dell'audit. In caso di

criticità, non conformità o inadempimenti rilevati, il Fornitore dovrà avviare con il subfornitore un piano di azioni correttive tale da risolvere qualsiasi non conformità in un ragionevole lasso di tempo, in ogni caso non superiore a 30 (trenta) giorni lavorativi decorrenti dalla data di svolgimento dell'audit. Il Fornitore si impegna a sostituire tempestivamente il sub-fornitore qualora non sia possibile risolvere le non conformità entro le tempistiche sopra indicate, ovvero laddove la Società ritenga a proprio insindacabile giudizio che le non conformità siano tali da compromettere la sicurezza e/o la continuità dell'esecuzione delle attività pattuite. In ogni caso, il Fornitore resta direttamente responsabile nei confronti della Società per ogni danno, disservizio o violazione derivante da condotte e/o omissioni del sub-fornitore e/o dalla mancata risoluzione di eventuali non conformità che dovessero emergere dagli audit effettuati.

3.3 La Società, anche per il tramite di soggetti terzi dalla stessa designati e debitamente vincolati ad obblighi di riservatezza, ha altresì il diritto di effettuare audit e verifiche tecniche, organizzative e documentali presso il Fornitore, al fine di accertare il rispetto degli obblighi contrattuali e normativi assunti con il presente Contratto. Gli audit potranno essere svolti con cadenza annuale nonchè ogniqualvolta si verifichino eventi o sospetti eventi di sicurezza che possano compromettere l'integrità, la disponibilità e/o la riservatezza dei servizi o dei dati trattati per conto della Società, e previo preavviso scritto di almeno 10 (dieci) giorni lavorativi. A tal fine, ii Fornitore si impegna a garantire alla Società ed ai terzi da questa autorizzati l'accesso fisico e/o remoto a infrastrutture, ambienti, documentazione, log e strumenti coinvolti nell'esecuzione del Contratto, nonché a fornire senza indebiti ritardi tutte le informazioni ed i documenti ragionevolmente richiesti dalla Società per lo svolgimento dell'audit. La Società si impegna a ridurre al minimo le interferenze rispetto all'operatività del Fornitore.

3.4 Qualunque non conformità che dovesse emergere nel corso dell'attività di audit, fermo restando ogni diritto di legge e di accordo ivi compreso il risarcimento del danno, dovrà essere risolta dal Fornitore sopportandone i relativi costi e/o oneri e comunque in un ragionevole lasso di tempo, in ogni caso non superiore a 30 (trenta) giorni di calendario, salvo oggettive e comprovate ragioni che non permettano il

rispetto di tale termine e/o salvo motivi di urgenza tali da raccomandare un adeguamento entro un termine più breve. Successivamente alla soluzione delle non conformità eventualmente rilevate, pertanto, l'esecuzione delle attività pattuite tra le Parti dovrà essere perfettamente aderente alle obbligazioni assunte dal Fornitore sulla base delle pattuizioni con la Società ed alle disposizioni normative e/o regolamentari tempo per tempo applicabili.

4. <u>Gestione delle vulnerabilità, continuità operativa e ripristino</u>

4.1 Il Fornitore si impegna a implementare un processo strutturato e continuo di vulnerability management, finalizzato all'identificazione tempestiva delle vulnerabilità che possano compromettere la sicurezza dei sistemi, reti, applicazioni e infrastrutture utilizzati nell'ambito dell'erogazione dei servizi disciplinati dal presente contratto.

A tal fine, il Fornitore si impegna quantomeno a:

i. monitorare costantemente fonti ufficiali (quali a titolo esemplificativo ma non esaustivo, CSIRT-Italia, ACN, CERT, ENISA etc.) e fornitori tecnologici al fine di essere costantemente aggiornato sulle nuove vulnerabilità ed adottare adeguate contromisure;

ii. utilizzare strumenti automatizzati di vulnerability scanning aggiornati con cadenza almeno mensile;

iii. adottare una metodologia formale per la classificazione delle vulnerabilità individuate. La priorità di trattamento è definita in funzione della criticità e del potenziale impatto sull'esecuzione del Contratto, nel rispetto dell'Allegato "Service Level Agreement" di cui al presente Contratto;

iv. garantire l'applicazione regolare e tracciata delle patch di sicurezza su sistemi e software impiegati nell'esecuzione del Contratto, nel rispetto dell'Allegato "Service Level Agreement" di cui al presente Contratto;

v. tenere un registro aggiornato delle vulnerabilità rilevate, delle patch applicate e delle date di implementazione e delle contromisure temporanee adottate. Tale documentazione dovrà essere resa tempestivamente disponibile alla Società ove da questa richiesta.

a. Il Fornitore garantisce la continuità operativa e la resilienza dei sistemi e delle reti utilizzate nell'esecuzione del Contratto tramite l'adozione e il mantenimento:

i. di un Business Continuity Plan (BCP) documentato, aggiornato almeno annualmente e condiviso con la Società;

ii. un Disaster Recovery Plan (DRP) relativo a tutte le infrastrutture di rilievo per l'esecuzione del Contratto, coerenti con i livelli di servizio pattuiti nell'Allegato "Service Level Agreement" di cui al presente Contratto;

iii. meccanismi di backup regolari, con verifica periodica del ripristino.

In caso di evento che comprometta la continuità operativa o sia conseguenza di una vulnerabilità, il Fornitore deve attivare immediatamente i piani di continuità e ripristino adottati nel rispetto delle tempistiche pattuite, informando la Società entro 2 (due) ore dalla rilevazione dell'evento. In tali casi il Fornitore si impegna altresì a mantenere costantemente aggiornata la Società sullo stato dell'evento, cooperando con la stessa per eventuali comunicazioni verso le competenti Autorità e/o terzi nel rispetto di quanto contrattualmente pattuito, e provvedendo a documentare adeguatamente tutte le azioni intraprese.

b. In caso di impossibilità tecnica di rispettare i termini pattuiti di cui all'Allegato "Service Level Agreement", ne informerà per iscritto la Società tempestivamente e in ogni caso prima della decorrenza di detti termini, provvedendo in tale comunicazione a indicare le misure compensative idonee a contenere il rischio adottate (quali a titolo esemplificativo ma non esaustivo blocchi firewall, disabilitazione servizi, isolamento temporaneo etc.). In ogni caso, il Fornitore garantisce il monitoraggio continuo della situazione e si impegna ad aggiornare senza indebiti ritardi la Società sulle evoluzioni del caso.

5. Gestione dell'autenticazione, delle identità digitali e del controllo accessi

5.1 Laddove l'esecuzione del Contratto comporti l'accesso da parte del Fornitore a reti e/o sistemi della Società, ciascun utente afferente all'organizzazione del Fornitore – per tali intendendosi, a titolo esemplificativo e non esaustivo, dipendenti e/o

collaboratori e/o terzi autorizzati dal Fornitore – deve a tal fine utilizzare esclusivamente le modalità di autenticazione ai sistemi e reti della Società fornite da quest'ultima, ovvero utilizzare sistemi adeguati a garantire la conformità ai principi di univocità ed esclusività degli accessi, nel rispetto degli obblighi normativi vigenti e delle linee guida e best practices di settore tempo per tempo applicabili, nonché delle politiche di accesso messe a disposizione dalla Società. I soggetti che avranno accesso a sistemi e/o reti della Società dovranno essere preventivamente individuati e comunicati per iscritto alla Società stessa alla data di sottoscrizione del presente Contratto; è obbligo del Fornitore mantenere aggiornata tale lista, provvedendo a comunicare per iscritto senza indebito ritardo eventuali modifiche alla Società.

5.2 Il Fornitore è e resta unico responsabile della corretta conservazione delle credenziali di accesso eventualmente rilasciate dalla Società. A tal fine si impegna a custodire adeguatamente le credenziali di accesso ai sistemi e/o ai servizi della Società e garantisce di utilizzarle esclusivamente per l'esecuzione delle attività pattuite con la Società, regolandone opportunamente l'uso da parte di propri dipendenti e manlevando la Società da qualsivoglia responsabilità al riguardo. Il Fornitore si impegna altresì a non comunicare dette credenziali a terzi senza la preventiva autorizzazione scritta della Società; e ad Informare la Società immediatamente in caso di smarrimento di dette credenziali, ovvero laddove il Fornitore sia venuto a conoscenza di un uso non autorizzato (effettivo o anche soltanto potenziale) delle stesse.

5.3 L'accesso a sistemi e reti della Società può essere effettuato esclusivamente per l'adempimento di quanto concordato tra le Parti e nel rispetto delle modalità indicate dalla Società anche successivamente alla sottoscrizione del presente Contratto. Il Fornitore si impegna al rispetto delle istruzioni indicate dalla Società. Eventuali modifiche alle modalità di accesso troveranno applicazione solo previa autorizzazione scritta da parte della Società.

A titolo esemplificativo e non esaustivo, è fatto espresso divieto al Fornitore di:

a. Consentire l'accesso a sistemi e/o reti della Società a soggetti diversi da quelli individuati e dichiarati nei confronti della Società;

b. Non porre in essere comportamenti tali da causare violazioni a normative tempo per tempo applicabili, quali quelle in materia di copyright, licenze d'uso di software e regolamenti dei fornitori di connettività di rete;
c. Effettuare attività non previste contrattualmente e che possano comportare malfunzionamenti, interruzioni e/o alterazioni della regolare operatività, danni di qualsivoglia natura alla utilizzabilità delle reti e/o sistemi della Società;
d. Accedere a banche dati diverse da quelle funzionali alla regolare attività del Fornitore;
e. Effettuare, ove consentito in base ai privilegi connessi all'utenza, azioni di upload/download e/o tentativi di intercettazione di dati e informazioni in transito sull'infrastruttura della Società;
f. Compiere azioni in violazione delle norme applicabili ai dati e/o informazioni presenti su sistemi e reti della Società accedute dal Fornitore, tra cui, a titolo esemplificativo, privative di proprietà intellettuale.

Il Fornitore riconosce e accetta che la Società potrà effettuare il monitoraggio – anche automatico e continuativo – delle attività svolte dal Fornitore sui sistemi e/o reti della Società, riconoscendo altresì a quest'ultima la facoltà, a insindacabile giudizio della stessa, di sospendere e/o impedire gli accessi ai sistemi e/o reti concessi al Fornitore, senza necessità di preventivo avviso, qualora ciò si renda necessaria a preservare l'integrità e l'operatività dei propri sistemi e/o reti, e in ogni caso ogni qualvolta il Fornitore, per il tramite di suoi dipendenti e/o collaboratori e/o terzi autorizzati, violi gli obblighi assunti con la Società e/o violi normative applicabili.

5.4 Il Fornitore dichiara e garantisce di aver implementato e mantenere un sistema sicuro e documentato per la gestione delle identità digitali e degli account utente dei sistemi, applicazioni e reti utilizzati per l'esecuzione del Contratto, assicurando che l'accesso a tali sistemi, applicazione e reti:

i. È concesso esclusivamente sulla base di ruoli predefiniti, coerenti con le attività assegnate;
ii. Viene monitorato e registrato, con conservazione dei log secondo i termini di legge;

iii. È revocato tempestivamente in caso di cessazione del rapporto lavorativo o cambio mansione;

iv. Prevede la scadenza programmata degli account temporanei e di quelli inutilizzati;

v. Viene gestito attraverso un sistema di Identity & Access Management (IAM) o equivalente;

vi. adotta meccanismi di autenticazione multi-fattore (MFA) basati su meccanismi robusti per tutti gli account con privilegi amministrativi o di accesso a dati e servizi critici della Società e, ove tecnicamente possibile, anche per gli utenti standard

6. <u>Protezione delle reti, delle comunicazioni e dei dati e informazioni</u>

6.1 Il Fornitore si impegna a garantire, per tutta la durata del presente Contratto, l'adozione, il mantenimento e il costante aggiornamento di misure tecniche e organizzative volte ad assicurare un livello di sicurezza proporzionato ai rischi connessi all'esecuzione del Contratto, ed a garantire la sicurezza, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di rete, delle infrastrutture di comunicazione elettronica e dei canali di trasmissione dei dati utilizzati nell'esecuzione delle attività oggetto del presente Contratto e dei dati e delle informazioni della Società trattate in esecuzione del Contratto.

Tali misure perseguono i seguenti obiettivi generali:

i. garantire la disponibilità, integrità, riservatezza e autenticità dei dati e delle informazioni trattate;

ii. assicurare la continuità operativa e la resilienza dei sistemi e delle reti per la Società;

iii. prevenire, rilevare e rispondere efficacemente a incidenti di sicurezza informatica;

iv. garantire livelli di sicurezza conformi alle disposizioni normative e regolamentari applicabili - quali a titolo meramente esemplificativo e non esaustivo il D.lgs. 138/2024 di recepimento della Direttiva (UE) n. 2022/2555 (c.d. "NIS2") e le linee guida e best practices di settore tempo per tempo applicabili - e tali da consentire il corretto e costante adempimento degli obblighi assunti con la Società e garantire a quest'ultima la costante disponibilità, senza ritardi e/o interruzioni, delle

attività pattuite e la conformità delle stesse alle normative tempo per tempo vigenti nel corso di validità del presente Contratto.

6.2 L'elenco aggiornato delle misure minime di sicurezza adottate dal Fornitore è indicato all'Allegato "Misure di sicurezza NIS2" di cui al presente Contratto. Il Fornitore è tenuto ad aggiornare le misure adottate ogni qualvolta intervengano modifiche normative, evoluzioni tecnologiche, nuovi rischi o eventi significativi: ogni proposta di modifica dovrà essere tempestivamente comunicata alla Società e formalmente approvata per iscritto da essa. In tali casi, l'allegato potrà essere aggiornato tramite scambio dell'allegato aggiornato debitamente sottoscritto dalle Parti, senza necessità di modificare l'intero Contratto.

7. Gestione e segnalazione degli incidenti

7.1 Il Fornitore si impegna a garantire la capacità continuativa di rilevamento, classificazione e gestione degli incidenti di sicurezza, anche potenziali, mediante l'impiego di sistemi automatizzati di monitoraggio e alerting; personale qualificato per l'analisi degli eventi e la risposta agli incidenti e processi formalizzati di gestione degli incidenti aggiornati almeno annualmente.

7.2 Il Fornitore si impegna a notificare, senza indebiti ritardi e comunque entro 2 (due) ore dalla rilevazione o dal fondato sospetto di un incidente di sicurezza che:

i. comprometta, anche potenzialmente, la riservatezza, integrità o disponibilità dei sistemi, dei dati o dei servizi forniti alla Società; e/o

ii. riguardi i sistemi, le reti e/o gli applicativi utilizzati dal Fornitore nell'esecuzione del Contratto; e/o

iii. abbia impatti, anche potenziali, su soggetti terzi quali a titolo esemplificativo ma non esaustivo clienti e/o della Società.

quali a titolo esemplificativo ma non esaustivo: accessi non autorizzati reti e/o sistemi informativi del Fornitore, utilizzi impropri degli account e/o delle credenziali di autenticazione fornite dalla Società.

7.3 La notifica iniziale dell'incidente dovrà avvenire agli indirizzi e-mail e PEC ed al contatto telefonico indicati dalla Società nel Contratto. Ove non diversamente

indicato dalla Società, anche le successive comunicazioni in merito all'incidente dovranno avvenire con le medesime modalità.

7.4 La notifica iniziale dell'incidente deve contenere almeno le seguenti informazioni:

i. data e ora della rilevazione;
ii. sintesi descrittiva dell'evento;
iii. asset coinvolti (sistemi, reti, servizi, dati);
iv. valutazione preliminare dell'impatto;
v. eventuali azioni correttive immediate adottate e/o pianificate;
vi. tempistiche di recupero della piena operatività.

7.5 Fino alla risoluzione dell'incidente, il Fornitore si impegna a fornire alla Società aggiornamenti sull'evento giornalieri e in ogni caso ove richiesto della Società, ed a trasmettere una relazione dettagliata dell'evento entro 5 (cinque) giorni lavorativi dalla chiusura dell'incidente. Tale relazione conclusiva dovrà indicare quantomeno:

i. cause e vulnerabilità sfruttate;
ii. cronologia degli eventi;
iii. misure correttive adottate;
iv. impatti sull'esecuzione del Contratto e sugli obblighi assunti dal Fornitore ai sensi dello stesso;
v. eventuali comunicazioni alle competenti autorità.

7.6 Il Fornitore si impegna altresì a:

i. assicurare la massima collaborazione con la Società per approfondire tutti gli aspetti necessari ed utili per precisare la violazione e per la gestione e l'analisi tecnica dell'incidente, a tal fine ove richiesto dalla Società fornendo a titolo esemplificativo ma non esaustivo accesso a log, evidenze forensi ed altri elementi utili;
ii. Supportare la Società in qualsiasi attività relativa ad eventuali notifiche verso autorità a cui la stessa sia obbligata, cooperando con le autorità competenti se richiesto dalla Società o ove imposto dalla normativa.

7.7 Nel caso in cui l'incidente coinvolga un subfornitore, il Fornitore mantiene l'obbligo di notifica alla Società secondo i termini sopra indicati e assicura che il subfornitore:

i. notifichi l'incidente con le stesse tempistiche e contenuti;
ii. consenta adeguate verifiche da parte della Società, ove da questa richiesto
iii. garantisca alla Società obblighi di collaborazione ed assistenza analoghi a quelli previsti dal presente Contratto

7.8 È fatto obbligo di mantenere l'assoluto riserbo sulle violazioni intercorse, fatte salve le comunicazioni obbligatorie per legge. Al riguardo, tali notizie non dovranno essere in alcun modo diffuse in qualunque forma, anche mediante la loro messa a disposizione o consultazione. La comunicazione della violazione di sicurezza è ammessa solo tra la Società e/o altro soggetto da questa indicato e il Fornitore, fatte salve quelle comunicazioni richieste dalla legge o da autorità pubbliche.

8. <u>Sviluppo sicuro del codice e sicurezza fin dalla progettazione e per impostazione predefinita</u>

8.1 Il presente comma trova applicazione nel caso in cui il Contratto preveda l'esecuzione di attività di sviluppo di software per conto della Società, ivi incluse a titolo esemplificativo ma non esaustivo scrittura di codice nell'esecuzione di attività manutentive adattive e/o evolutive.

8.2 Il Fornitore si impegna ad adottare e mantenere pratiche di sviluppo sicuro del software, assicurando che ogni sistema, applicazione o componente fornito alla Società sia progettato, realizzato e distribuito in conformità ai principi di sicurezza fin dalla progettazione (security by design) e sicurezza per impostazione predefinita (security by default). A tal fine, il Fornitore dichiara e garantisce quantomeno che tutto quanto rilasciato alla Società in esecuzione del Contratto incorpora misure di sicurezza sin dalla fase di progettazione, con approccio "zero trust" dove applicabile; è configurato con impostazioni predefinite orientate alla sicurezza (quali a titolo esemplificativo ma non esaustivo: disattivazione delle funzionalità non necessarie, logging abilitato, accessi limitati) e prevedere meccanismi per la gestione granulare dei privilegi e adeguata protezione dei dati.

8.3 Il Fornitore sin dalla fase di progettazione si impegna, senza corrispettivi ulteriori rispetto a quanto pattuito, a redigere, aggiornare e fornire alla Società previa richiesta di quest'ultima la documentazione tecnica del caso – per tale intendendo l'insieme di

documenti, requisiti funzionali e non funzionali, architetture, modelli dati, diagrammi logici e fisici, standard di sviluppo, configurazioni infrastrutturali e criteri di accettazione applicabili a quanto rilasciato e che includono requisiti di sicurezza formalizzati - per assicurare che i sistemi e i servizi sviluppati rispettino i principi di sicurezza previsti dalla normativa applicabile.

8.4 Il Fornitore garantisce che nell'esecuzione del Contratto:

i. sono utilizzati framework di sviluppo sicuro aggiornati e basati su standard riconosciuti (quali a titolo esemplificativo ma non esaustivo OWASP, NIST SP 800-218 SSDF);
ii. sono integrati strumenti di analisi statica e dinamica del codice sorgente;
iii. vengano eseguite quantomeno attività sistematiche di code review strutturate e test di sicurezza in ogni fase del ciclo;
iv. ogni versione sia rilasciata solo previo superamento di adeguati controlli di sicurezza interni e tali da impedire l'inserimento nei rilasci di componenti insicuri o non validati, mettendo a disposizione della Società i relativi rapporti/report ove dalla stessa richiesto;
v. quanto rilasciato alla Società sia dotato delle caratteristiche tecniche e delle funzionalità concordate, compresa, a titolo esemplificativo ma non esaustivo, l'interoperabilità con i sistemi, l'infrastruttura informativa e di rete e gli strumenti, anche forniti da terze parti, in uso presso la Società;
vi. di aver acquisito tutte le opportune autorizzazioni e/o licenze necessarie per consentire alla Società il legittimo utilizzo di quanto rilasciato in esecuzione del Contratto, impegnandosi a fornire alla Società, previa richiesta di quest'ultima e nel rispetto delle normative applicabili, tutte le opportune autorizzazioni e/o credenziali del caso. Il Fornitore è e resta l'unico responsabile per l'acquisizione ed il mantenimento di tutte le opportune autorizzazioni e/o licenze necessarie per l'esecuzione delle attività di sviluppo pattuite, manlevando integralmente la Società da qualsivoglia responsabilità al riguardo.

8.5 Il Fornitore è unico responsabile dell'integrazione, aggiornamento e monitoraggio delle librerie, moduli software e pacchetti di terze parti utilizzati nell'esecuzione del Contratto, garantendo che:

i. vengano utilizzati, nel rispetto di privative anche industriali di terzi, solo componenti opportunamente aggiornati e manutenuti e adeguati a consentire alla Società il raggiungimento degli scopi a cui il Contratto è volto, scopi che il Fornitore dichiara di ben conoscere;

ii. siano adeguatamente tracciate le modifiche (versioning, changelog, log di build e rilascio);

iii. venga eseguita regolare Software Composition Analysis (SCA); e

iv. vengano trattate con priorità le vulnerabilità identificate tramite il sistema CVE (Common Vulnerabilities and Exposures), per tale intendendosi un identificativo univoco assegnato da enti riconosciuti a una vulnerabilità di sicurezza nota, associata a una descrizione tecnica e a un punteggio di gravità secondo lo standard CVSS (Common Vulnerability Scoring System). A tal fine, il Fornitore dovrà monitorare settimanalmente i database pubblici di vulnerabilità ed informare la Società entro 24 ore in caso di vulnerabilità (CVE) che impattino su quanto oggetto del Contratto, adottando azioni correttive entro 24 ore per CVE critiche (CVSS ≥ 9.0) e 3 (tre) giorni lavorativi per CVE ad alto impatto (CVSS ≥ 7.0) e fornendo alla Società, su richiesta di quest'ultima, evidenza delle azioni di aggiornamento, mitigazione o isolamento adottate.

8.6 Le Parti riconoscono e accettano che ciascun rilascio dovrà essere oggetto di specifica verifica/collaudo le cui modalità di esecuzione saranno di volta in volta pattuite tra le Parti, restando in ogni caso inteso che:

i. Ciascuna verifica/collaudo si intenderà avvenuta con esito positivo soltanto qualora, sia sottoscritto tra le Parti verbale attestante l'esito positivo della stessa senza riserve o contestazioni;

ii. In caso di esito negativo, la Società potrà muovere contestazioni e comunicare a mezzo e-mail al Fornitore eventuali vizi, difetti e/o inidoneità, che il Fornitore è tenuto a eliminare, a propria cura e spese, prontamente e comunque entro e non

oltre 10 (dieci) giorni lavorativi decorrenti dalla segnalazione, salva l'azionabilità da parte della Società di qualsiasi rimedio previsto dalla legge. Entro 7 (sette) giorni lavorativi decorrenti dalla risoluzione dei vizi, difetti e/o inidoneità contestati, le Parti procederanno ad un ulteriore verifica/collaudo e, qualora la Società riscontri nuovamente vizi, difetti e/o inidoneità, avrà facoltà di risolvere il presente Contratto ai sensi e agli effetti dell'art. 1456 e ss. c.c., fatta salva la risarcibilità dell'eventuale maggior danno.

iii. Gli oneri sostenuti dal Fornitore per le attività di verifica/collaudo sono inclusi nel corrispettivo concordato tra le Parti ai sensi del presente Contratto.

iv. Eventuali pagamenti effettuati prima del superamento con esito positivo della verifica/collaudo finale, avranno unicamente valore di anticipo e non avranno valore di accettazione, neppure parziale, di quanto realizzato in esecuzione del presente Contratto.

9. <u>Dismissione della fornitura ivi compresa la restituzione e cancellazione dei dati</u>

9.1 In tutti i casi di cessazione del Contratto a qualsiasi causa dovuta, il Fornitore dovrà:

i. cessare immediatamente qualsiasi accesso a reti, sistemi, applicazioni e dati della Società, indicando per iscritto alla Società l'elenco degli accessi sussistenti alla data di cessazione del Contratto;

ii. avviare le procedure di restituzione e cancellazione di tutti i dati e/o le informazioni della Società, secondo i termini di seguito indicati;

iii. consegnare alla Società, entro 15 giorni lavorativi dalla cessazione una copia completa in un formato leggibile e comunemente utilizzato di tutti i dati, file, database, log, configurazioni e documentazione tecnica trattati o generati in esecuzione del Contratto. Il trasferimento sarà effettuato su supporto fornito dalla Società o tramite canale sicuro (quale a titolo esemplificativo ma non esaustivo: SFTP cifrato, VPN dedicata) concordato tra le Parti. Una volta concluse le attività di restituzione, il Fornitore si impegna a darne comunicazione scritta alla Società;

iv. entro 30 giorni dalla restituzione, cancellare in modo permanente e irreversibile tutti i dati e le informazioni della Società presenti su sistemi, backup, cloud o altri supporti gestiti dal Fornitore o dai suoi sub-fornitori, eseguendo procedure di secure

erase, Wipe o distruzione fisica secondo standard riconosciuti. Il Fornitore riconosce ed accetta che la Società avrà il diritto, a proprio insindacabile giudizio, di essere presente e/o richiedere la presenza di un verificatore indipendente durante le attività di cancellazione. Concluse tali attività, il Fornitore si impegna a darne comunicazione scritta alla Società inviando alla stessa specifico report sottoscritto attestante l'avvenuta cancellazione definitiva e distruzione di qualsiasi copia residua entro i successivi 5 (cinque) giorni lavorativi;

v. garantire che tutte le fasi sopra indicate siano comunque presidiate dalle misure di sicurezza sussistenti in vigenza di Contratto o almeno parificabili.

9.2 Il Fornitore resta responsabile anche per le attività svolte dai sub-fornitori, garantendo gli stessi obblighi di restituzione e cancellazione, con analoghi termini e modalità e provvedendo a fornire alla Società copia della relativa documentazione attestante l'avvenuta cancellazione da parte dei sub-fornitori nei termini sopra indicati.

9.3 Nel caso di obblighi normativi che non consentano al Fornitore di procedere con la cancellazione (quali a titolo esemplificativo ma non esaustivo: conservazione dati ai fini fiscali, contabili o di compliance), il Fornitore potrà conservare, in forma cifrata e separata, solo i dati e le informazioni strettamente necessari per ottemperare a detti obblighi normativi e alla data di cessazione del Contratto dovrà informare la Società di tale circostanza, documentando le relative motivazioni e indicando la durata prevista di conservazione e le modalità di isolamento adottate. Resta inteso che decorsi i termini di legge, il Fornitore dovrà provvedere alla cancellazione dei dati/informazioni della Società nel rispetto delle modalità sopra indicate.

9.4 Fatti salvi diversi accordi scritti tra le Parti nonché quanto diversamente disciplinato nel presente Contratto e/o eventuali danni subiti dalla Società, la Società sarà tenuta esclusivamente al pagamento dei corrispettivi dovuti per le attività effettivamente eseguite alla data di cessazione del Contratto.

10. <u>Subappalto, subfornitura o relativi potenziali requisiti di sicurezza lungo la catena di fornitura</u>

10.1 Il Fornitore non può affidare in tutto o in parte a terzi (di seguito, "sub-fornitori") l'esecuzione del presente Contratto senza la previa autorizzazione scritta della

Società. A tal fine, per consentire alla Società le opportune valutazioni del caso, nella richiesta di autorizzazione al subappalto o subfornitura presentata alla Società il Fornitore dovrà fornire quantomeno:

i. identificazione completa del sub-fornitore;
ii. indicazione dei servizi e attività affidati;
iii. valutazione del livello di rischio per la sicurezza, includendo il dettaglio delle misure tecniche e organizzative adottate dal sub-fornitore.

10.2 Il Fornitore dichiara e garantisce che ogni sub-fornitore:

i. è stato dallo stesso vincolato ad obblighi contrattuali equivalenti a quelli del presente Contratto, con particolare riguardo agli aspetti di riservatezza, sicurezza, protezione dati personali, continuità operativa e gestione del rischio e degli incidenti;
ii. adotta misure tecniche e organizzative quantomeno equivalenti a quelle adottate dal Fornitore ai sensi del presente Contratto e adeguate ai sensi dell'art. 32 del Regolamento (UE) 2016/679 (GDPR) ed agli standard internazionali applicabili. In particolare, il Fornitore dichiara e garantisce che ogni sub-fornitore ha implementato procedure documentate per la gestione degli incidenti di sicurezza e delle vulnerabilità, nonché piani di risposta e mitigazione tempestiva degli impatti;
iii. consente alla Società di effettuare audit nel rispetto delle modalità di cui al presente Contratto. La Società avrà altresì diritto di richiedere al Fornitore in qualsiasi momento adeguata documentazione attestante la conformità dei sub-fornitori, che il Fornitore si impegna a fornire entro 5 (cinque) giorni lavorativi dalla richiesta.

10.3 Il Fornitore resta pienamente responsabile verso la Società per ogni attività, atto, omissione, violazione e/o negligenza dei subfornitori di cui si avvale nell'esecuzione del Contratto e garantisce la tracciabilità completa della filiera di fornitura. A tal fine, il Fornitore si impegna a mantenere un registro aggiornato dei sub-fornitori coinvolti, con relativo ambito di attività ed a trasmetterlo alla Società con cadenza almeno annuale o su richiesta della stessa.

10.4 Il Fornitore si impegna a esercitare un controllo attivo e continuativo sulla catena di fornitura, verificando periodicamente l'effettiva conformità dei sub-fornitori agli obblighi di cui al presente Contratto e/o alla normativa tempo per tempo vigente. A tal fine il Fornitore si impegna a eseguire almeno una volta all'anno audit sui subfornitori impiegati, comunicando alla Società, entro 10 (dieci) giorni dalla chiusura dell'audit, gli esiti degli stessi, non conformità rilevate e azioni correttive adottate.

10.5 In caso di evento/incidente di sicurezza e/o violazione di dati, anche solo sospettati, che coinvolga uno o più subfornitori e che abbia un impatto, anche solo potenziale, diretto o indiretto sull'esecuzione del Contratto il Fornitore dovrà:

i. notificarlo alla Società senza ingiustificato ritardo e comunque entro 24 (ventiquattro) ore dalla scoperta;
ii. fornire un rapporto iniziale e aggiornamenti periodici sulla gestione dell'incidente e sulle azioni correttive intraprese;
iii. cooperare pienamente con la Società per valutare le conseguenze, limitare i danni e ripristinare la normale operatività.

10.6 La Società si riserva il diritto di chiedere la sostituzione di un subfornitore qualora si verifichi anche una sola delle seguenti condizioni:

i. Carenze tecniche o professionali del subfornitore accertate a insindacabile giudizio della Società e tali da compromettere la qualità, l'efficacia e/o la sicurezza dell'esecuzione del Contratto;
ii. Condotte del subfornitore incompatibili con gli obblighi di riservatezza, integrità e affidabilità richiesti per l'esecuzione del Contratto;
iii. situazioni di conflitto di interesse, anche potenziale, tra il subfornitore e la Società;
iv. violazione delle disposizioni normative o contrattuali da parte del subfornitore;
v. in ogni caso previsto dalle normative tempo per tempo vigenti.

In tali casi il Fornitore, ricevuta richiesta scritta dalla Società, dovrà procedere alla sostituzione del subfornitore contestato entro e non oltre 5 (cinque) giorni lavorativi, in ogni caso garantendo la continuità dell'esecuzione delle attività pattuite.

11. Violazione degli obblighi assunti e risoluzione del Contratto

11.1 La violazione anche di uno soltanto degli obblighi previsti dal presente articolo costituirà causa di grave inadempimento contrattuale e la Società potrà risolvere il contratto senza preavviso alcuno, ai sensi e per gli effetti di cui all'art. 1456 Cod. Civ., mediante semplice comunicazione scritta (a mezzo raccomandata a/r o via pec) al Fornitore a mezzo PEC o raccomandata A/R, fatti salvi ulteriori rimedi previsti dal presente Contratto nonché il risarcimento di eventuali danni subiti dalla Società.

4. ALLEGATI

4.1 RAPPORTI TRA LA SOCIETA' ED I PROPRI FORNITORI NIS2 NON CRITICI

- Modello documentale di "Misure di sicurezza NIS2 CONTRATTO FORNITORE" da adottare laddove il Fornitore non fornisca un proprio documento. Se del caso, modificare/dettagliare a seconda delle specifiche della fornitura e allegare al Contratto tra la Società ed il Fornitore non critico.
- Modello documentale di "Service Level Agreement", se del caso da modificare/dettagliare a seconda delle specifiche della fornitura e allegare al Contratto tra la Società ed il Fornitore non critico.

4.2 RAPPORTI TRA LA SOCIETA' ED I PROPRI FORNITORI NIS2 CRITICI

- Modello documentale di "Misure di sicurezza NIS2 CONTRATTO FORNITORE", se del caso da compilare/dettagliare a seconda delle specifiche della fornitura e allegare al Contratto tra la Società ed il Fornitore critico.
- Modello documentale di "Service Level Agreement", se del caso da modificare/dettagliare a seconda delle specifiche della fornitura e allegare al Contratto tra la Società ed il Fornitore critico.