Allegato al Capitolato Tecnico

Requisiti di sicurezza NIS applicabili alla fornitura

Sommario

1. Premessa 2
2. Baseline di Sicurezza 3
2.1 Affidabilità fornitori – Supplier Governance 3
2.2 Ruoli e responsabilità nell'ambito della fornitura – Governance della sicurezza 3
2.3 Affidabilità risorse umane – Gestione del personale 4
2.4 Conformità e audit – Governance della sicurezza 4
2.5 Formazione del personale e consapevolezza – Security Awareness 4
2.6 Sicurezza dei dati – Data Protection 5
2.7 Gestione e segnalazione degli incidenti – Incident Response 5
2.8 Subappalto, subfornitura o relativi potenziali requisiti di sicurezza lungo la catena di fornitura – Supplier Lifecycle Management 5

1. PREMESSA

Il presente allegato al Capitolato Tecnico definisce la Baseline di sicurezza applicabile all'appalto in oggetto, individuata in coerenza con i principi e le finalità della Direttiva (UE) 2022/2555, cosiddetta Direttiva NIS2, e del relativo decreto di recepimento nell'ordinamento nazionale, decreto legislativo 4 settembre 2024, n. 138, recante misure per un livello comune elevato di cybersicurezza nell'Unione europea.

I requisiti riportati nel presente allegato sono finalizzati a presidiare, secondo criteri di proporzionalità e adeguatezza rispetto alla natura e alle caratteristiche della fornitura, i rischi di sicurezza connessi all'affidabilità del Fornitore, alla governance della sicurezza, alla gestione del personale, alla protezione dei dati, alla gestione degli incidenti e alla sicurezza della catena di approvvigionamento.

Tali requisiti costituiscono obblighi contrattuali del Fornitore, ferma restando l'applicazione degli ulteriori obblighi previsti dalla normativa vigente qualora il Fornitore, uno dei soggetti coinvolti nell'esecuzione della fornitura o i servizi oggetto dell'affidamento rientrino nel campo di applicazione della disciplina NIS.

2. BASELINE DI SICUREZZA

2.1 AFFIDABILITÀ FORNITORI – SUPPLIER GOVERNANCE

Il Fornitore si impegna a dimostrare, con evidenze documentali, la gestione strutturata della propria affidabilità rispetto alla fornitura, con riferimento a:

- l'adozione di un sistema di gestione della sicurezza proporzionato alla natura della fornitura — certificazione ISO/IEC 27001 o equivalente ove la fornitura coinvolga prodotti, sistemi o componenti tecnologici, oppure misure organizzative e procedurali documentate per forniture di altra natura;

- la gestione strutturata delle vulnerabilità pertinenti — ivi incluse quelle informatiche ove applicabili;

- la qualità dei prodotti e servizi forniti, dimostrata attraverso standard, certificazioni o processi di controllo pertinenti alla natura della fornitura;

- un piano di continuità operativa verificabile che garantisca approvvigionamento, assistenza e manutenzione nel tempo e, ove disponibili, gli esiti delle valutazioni coordinate delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

A comprova dell'adempimento, rende disponibili a Consip, su richiesta, le seguenti evidenze:

a) documentazione del sistema di gestione della sicurezza adottato, proporzionato alla natura della fornitura, da cui risultino anche le misure adottate per garantire la qualità complessiva dei prodotti e servizi forniti;

b) documentazione del processo strutturato di gestione delle vulnerabilità pertinenti, con evidenza delle criticità rilevate e del loro stato di risoluzione;

c) piano di continuità operativa proporzionato alla natura della fornitura, con indicazione delle misure previste per garantire approvvigionamento, assistenza e manutenzione nel tempo.

2.2 RUOLI E RESPONSABILITÀ NELL'AMBITO DELLA FORNITURA – GOVERNANCE DELLA SICUREZZA

Il Fornitore si impegna a designare uno o più referenti per la sicurezza della fornitura e a comunicarne tempestivamente le variazioni a Consip. Provvede inoltre a formalizzare i ruoli e le responsabilità di sicurezza delle figure coinvolte nella fornitura e a mantenerli aggiornati.

A comprova dell'adempimento, rende disponibili a Consip, su richiesta, le seguenti evidenze:

a) elenco dei referenti per la sicurezza con nominativo, ruolo, recapito telefonico e indirizzo e-mail dedicato;

b) documento che formalizzi i ruoli e le responsabilità di sicurezza delle figure coinvolte nella fornitura — nella forma più adeguata alla struttura organizzativa del fornitore (es. atto di nomina,

matrice RACI, organigramma annotato) — con indicazione delle responsabilità assegnate a ciascun ruolo e della data di ultimo aggiornamento.

2.3 AFFIDABILITÀ RISORSE UMANE – GESTIONE DEL PERSONALE

Il Fornitore si impegna a verificare l'affidabilità del personale assegnato alla fornitura prima dell'avvio dell'incarico, con modalità proporzionate al ruolo e alla natura della fornitura. Provvede inoltre a garantire che il personale con accesso a informazioni, sistemi o aree rilevanti — incluso quello di subfornitori e consulenti — sottoscriva un impegno formale di riservatezza prima dell'avvio delle attività, con obblighi applicabili anche dopo la cessazione dell'incarico.

A comprova dell'adempimento, rende disponibili a Consip, su richiesta, le seguenti evidenze:

a) documentazione del processo di verifica dell'affidabilità del personale assegnato alla fornitura, con indicazione delle tipologie di controllo applicate in funzione del ruolo e del livello di accesso previsto;

b) modello di impegno formale di riservatezza adottato, con indicazione degli obblighi previsti e della loro applicabilità dopo la cessazione dell'incarico, esteso al personale dei subfornitori coinvolti, corredato da attestazione di avvenuta sottoscrizione da parte del personale assegnato.

2.4 CONFORMITÀ E AUDIT – GOVERNANCE DELLA SICUREZZA

Il Fornitore si impegna a dichiarare il rispetto dei requisiti di sicurezza contrattualmente applicabili alla fornitura e a rendersi disponibile alle verifiche di Consip. Provvede inoltre a verificare periodicamente il proprio stato di conformità e a pianificare le azioni correttive per gli scostamenti rilevati.

A comprova dell'adempimento, rende disponibili a Consip, su richiesta, le seguenti evidenze:

a) dichiarazione di conformità firmata dal legale rappresentante o da suo delegato, con indicazione dei requisiti di sicurezza contrattualmente applicabili dichiarati rispettati e della data di sottoscrizione; per contratti pluriennali, rinnovata con cadenza coerente con il ciclo contrattuale;

b) report di autovalutazione con indicazione, per ciascun requisito applicabile, dello stato di adempimento (conforme / parzialmente conforme / non conforme), degli scostamenti rilevati e delle azioni correttive pianificate con responsabili e scadenze.

2.5 FORMAZIONE DEL PERSONALE E CONSAPEVOLEZZA – SECURITY AWARENESS

Il Fornitore si impegna a garantire che il personale assegnato alla fornitura abbia ricevuto una formazione di base sui rischi di sicurezza pertinenti al ruolo. Provvede inoltre a strutturare la formazione per profilo o ruolo, ad aggiornarla con frequenza adeguata all'evoluzione delle minacce e alle variazioni del personale e a verificarne il completamento.

A comprova dell'adempimento, rende disponibili a Consip, su richiesta, le seguenti evidenze:

a) attestazione del completamento della formazione di base da parte del personale assegnato alla fornitura, con indicazione dei contenuti trattati e della data di erogazione;

b) programma formativo strutturato con indicazione dei contenuti per profilo o ruolo, della frequenza di aggiornamento prevista e delle modalità di adeguamento in caso di variazioni del personale o evoluzione delle minacce, corredato da evidenza del completamento da parte del

personale assegnato con indicazione nominativa o per ruolo della data di completamento e dei contenuti erogati.

2.6 SICUREZZA DEI DATI – DATA PROTECTION

Il Fornitore si impegna a trattare i dati di Consip esclusivamente per le finalità autorizzate nell'ambito della fornitura e a proteggerli da accessi, modifiche, perdita o divulgazione non consentiti.

A comprova dell'adempimento, rende disponibile a Consip, su richiesta, la seguente evidenza:

a) documentazione delle misure adottate per il trattamento dei dati di Consip — nella forma più adeguata (es. clausole contrattuali, procedure interne, policy di protezione dei dati) — con indicazione delle finalità autorizzate, del divieto di utilizzo per scopi diversi e delle misure adottate per prevenire accessi, modifiche, perdita o divulgazione non consentiti; ove la fornitura comporti il trattamento di dati personali per conto di Consip, corredata da bozza o estratto dell'atto di nomina a Responsabile del trattamento con indicazione delle misure tecniche e organizzative adottate.

2.7 GESTIONE E SEGNALAZIONE DEGLI INCIDENTI – INCIDENT RESPONSE

Il Fornitore si impegna a notificare a Consip senza ingiustificato ritardo gli incidenti che coinvolgano o possano coinvolgere sistemi, servizi o dati della fornitura, trasmettendo le informazioni necessarie entro i termini definiti contrattualmente in funzione della severità, e a disporre di una procedura interna che definisca classificazione, ruoli, responsabilità e flussi di comunicazione verso Consip.

A comprova dell'adempimento, rende disponibili a Consip, su richiesta, le seguenti evidenze:

a) riferimenti operativi del canale dedicato (nominativo, indirizzo e-mail, recapito telefonico e finestre di copertura), corredati da procedura o istruzione che descriva i criteri di qualificazione degli eventi e i tempi di risposta attesi per severità;

b) procedura di gestione degli incidenti che definisca la classificazione degli eventi, i ruoli e le responsabilità nella risposta, i flussi di comunicazione verso Consip e i termini di notifica contrattualmente previsti, con allegato il modello di notifica adottato con indicazione dei campi minimi richiesti.

2.8 SUBAPPALTO, SUBFORNITURA O RELATIVI POTENZIALI REQUISITI DI SICUREZZA LUNGO LA CATENA DI FORNITURA – SUPPLIER LIFECYCLE MANAGEMENT

Il Fornitore si impegna a mantenere aggiornato l'elenco dei subfornitori rilevanti e a comunicarne preventivamente le variazioni. Provvede inoltre a valutare la criticità di ciascun subfornitore e a mantenere informazioni aggiornate sul perimetro di intervento e sugli accessi rilevanti.

A comprova dell'adempimento, rende disponibili a Consip, su richiesta, le seguenti evidenze:

a) elenco aggiornato dei subfornitori rilevanti, con indicazione per ciascuno di ragione sociale, ruolo, ubicazione della sede operativa rilevante e descrizione sintetica delle attività affidate, corredato da evidenza della comunicazione preventiva a Consip delle variazioni con indicazione della data e della natura della variazione;

b) registro esteso dei subfornitori che integri le informazioni di base con perimetro specifico di intervento, tipologia di dati e sistemi a cui il subfornitore ha accesso (logico o fisico) e livello di criticità stimato (Alto / Medio / Basso) con motivazione sintetica coerente con il tipo di accesso dichiarato.