Sicurezza delle Informazioni
Policy per i Fornitori

1. Versione del documento

Rev.	Data	Motivo	Redatto	Verificato	Approvato
00	29/05/2021	Prima emissione	D. Catellani	M. Scalvenzi	F. Bellelli
01	*05/03/2026*	*Aggiornamento generale Allineamento Direttiva NIS2*	*A. Pilotto*	*M. Scalvenzi*	*D. Catellani*

2. Scopo e campo di applicazione

Il presente documento definisce i requisiti di sicurezza che i Fornitori, a cui *Tinexta Innovation Hub ovvero le società appartenenti al "Gruppo Tinexta Innovation Hub" (di seguito ciascuna singolarmente definita "Committente")* affida servizi *e/o forniture*, sono tenuti a rispettare nel rapporto di collaborazione con *la Committente* al fine di salvaguardare la sicurezza delle Informazioni.

Il Fornitore che opera per conto *della Committente* deve allinearsi alle Politiche di sicurezza della stessa relativamente ai requisiti dello standard ISO 27001 *e della Direttiva NIS2*.

Il Fornitore che tratta dati personali per conto *della Committente* viene censito nel Privacy Management System e nominato*, ove applicabile,* Responsabile al Trattamento.

È responsabilità del Fornitore verificare di volta in volta la disponibilità della versione più aggiornata del presente Regolamento, al fine di assicurare il pieno rispetto dei requisiti di sicurezza richiesti; la data di emissione del Regolamento coincide con la data di inizio della sua validità. La Committente si riserva la facoltà di aggiornare il presente Regolamento in qualsiasi momento e senza obbligo di preavviso; gli aggiornamenti diventano efficaci dalla loro pubblicazione.

L'esecuzione delle attività implica accettazione della versione tempo per tempo vigente del presente Regolamento.

3. Riferimenti

La presente procedura è armonizzata con:

- Modello di Organizzazione Gestione e Controllo ai sensi della 231/2001;
- Codice Etico;
- UNI EN ISO 9001:2015;
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- MAN_Q&C_01_xx_IT_Manuale Sistema Gestione;
- REG_IT_02_xx_IT_Regolamento per l'utilizzo degli strumenti di lavoro assegnati in uso.
- *Direttiva (UE) 2022/2555 ("NIS2")*
- *D.Lgs. 4 settembre 2024, n. 138 – recepimento NIS2*
- *Determinazioni e Linee guida ACN*

4. Classificazione dei Fornitori Tecnologici

Per Fornitore Tecnologico si intende la terza parte (persona giuridica o fisica) che fornisce prodotti o servizi ICT (a titolo esemplificativo e non esaustivo: hardware, software, sviluppo e manutenzione applicativa, integrazione/API, servizi cloud IaaS/PaaS/SaaS, connettività/rete, cybersecurity gestita SOC/MSP/MSSP, hosting/data center, backup/DR, strumenti DevSecOps) ovvero, limitatamente alle persone giuridiche (no liberi professionisti), che, nell'ambito della fornitura, accede -fisicamente o logicamente- o può influenzare dati, sistemi, reti o processi informativi della Committente e/o dei clienti finali della Committente, direttamente o indirettamente, anche tramite sub-fornitori e/o subappaltatori lungo la supply chain.

La Società classifica i Fornitori Tecnologici in quattro categorie:

a) Fornitore critico per il business (T1);
b) Fornitore critico per la sicurezza delle informazioni (T1);
c) Fornitore critico (business e sicurezza delle informazioni) (T1);
d) Fornitore non critico (T2).

La classificazione deriva dalla valutazione congiunta di Impatto sul business ed Impatto sulla sicurezza delle informazioni ed è mappata come T1 (Critico) e T2 (Non critico).
I fornitori tecnologici che appartengono alle categorie T1 o T2 devono rispettare le misure indicate nel capitolo Baseline Sicurezza Fornitori Tecnologici.

5. Gestione degli accessi alle sedi aziendali

Il Fornitore che, a vario titolo, ha accesso ai locali aziendali deve registrarsi tramite la compilazione dell'apposito Registro predisposto.
In relazione al contesto di servizio/lavoro e ai rischi sulla Sicurezza delle Informazioni associati alla fornitura, il Fornitore deve garantire che le risorse umane, che saranno impiegate nell'erogazione del servizio, abbiano un livello di formazione sulle tematiche relative alla sicurezza delle informazioni adeguato alla funzione che dovranno ricoprire.
L'accesso fisico del personale del Fornitore a siti/aree richiede:

- *identificazione preventiva;*
- *rispetto del principio del minimo privilegio (aree/tempi/sistemi limitati e tracciati);*
- *revoca immediata dell'abilitazione alla cessazione del rapporto contrattuale.*

6. Modello comportamentale in caso di accesso alle reti aziendali

Tutte le informazioni/sistemi con cui il Fornitore entrerà in contatto dovranno essere trattati secondo quanto previsto dagli accordi contrattuali sottoscritti con la *Committente* e saranno da considerarsi di natura Confidenziale.
Fatti salvi gli obblighi di riservatezza a cui possa essere soggetto, laddove il fornitore acceda alle informazioni della *Committente* o dei clienti di della *Committente*, il fornitore dovrà:

- fare in modo che tali informazioni, e con particolare attenzione ai dati personali, non vengano divulgate né consultate da personale non autorizzato;
- mantenere (e provvedere affinché tutto il personale interessato mantenga) tali informazioni (inclusi i dati personali) in condizioni di sicurezza.

Il fornitore inoltre non potrà avvalersi delle informazioni della *Committente* per finalità diverse da quelle per cui tali informazioni gli sono state trasmesse dalla *Committente* e unicamente nella misura necessarie per consentirgli di dare esecuzione al contratto.
Il fornitore dovrà garantire la disponibilità, qualità, integrità e capacità adeguata di offrire il servizio richiesto con una disponibilità senza interruzioni, assicurando che sia attivo un piano di backup adeguato.
Ove applicabile, il fornitore deve garantire l'utilizzo esclusivo della mail fornita della *Committente nell'esecuzione dell'incarico ricevuto.*
Il fornitore può accedere alla mail fornita della *Committente* solo attraverso un browser e non può utilizzare nessun altro tipo di software o client di posta.
Il fornitore non deve effettuare l'inoltro della mail aziendale della *Committente* su altre caselle di posta.
Il fornitore deve garantire l'archiviazione della documentazione redatta come indicato dal Responsabile di Area della *Committente*; il fornitore non deve in nessun caso conservare copia dei documenti in archivi diversi da quelli definiti.
E' fatto divieto assoluto al fornitore di cedere a terzi le credenziali di accesso fornite della *Committente* per lo svolgimento dei servizi affidati.

Qualora i dati e le informazioni risiedono su sistemi e/o ambienti del Fornitore, quest'ultimo, per tutti gli accessi a tali sistemi/servizi, deve:

- *utilizzare autenticazione a più fattori (MFA) e canali cifrati;*
- *applicare hardening, patching regolare e EDR/antimalware;*
- *garantire segregazione degli ambienti (dev/test/prod) e ciclo di vita delle vulnerabilità (scansioni periodiche di sicurezza);*
- *assicurare la continuità operativa (backup/restore/test) e capacità di crisis management (Disaster Recovery / Business Continuity).*

7. Due Diligence e monitoraggio continuativo (Due Care)

Prima dell'affidamento, per i fornitori tecnologici classificati critici, la Società si riserva di richiedere e valutare:

- *evidenze sul sistema di gestione (es. ISO/IEC 27001) e controlli eventualmente adottati;*
- *risultati di vulnerability management, pen-test, patching;*
- *formazione del personale, piani di continuità e test;*
- *sub-fornitori coinvolti (catena di fornitura);*
- *capacità di notifica incidenti secondo NIS2/ACN;*

con diritto di audit e richiesta di piani di rimedio qualora necessari.

8. Utilizzo dei dispositivi di memorizzazione rimovibili

E' vietato inoltre l'uso di dispositivi rimovibili per l'archiviazione di informazioni professionali legati ai servizi affidati dalla *Committente*.
Il fornitore si assume la responsabilità di eventuali incidenti di sicurezza derivanti dall'utilizzo di dispositivi rimovibili.

Per lo scambio di documentazione di lavoro da parte di Collaboratori, è obbligatorio l'utilizzo di strumenti di condivisione cloud messi a disposizione dalla *Committente* (es. Onedrive).

9. Dispositivi mobili e PC

Il Fornitore deve assicurare una adeguata protezione delle informazioni professionali legati ai servizi affidati dalla *Committente* e memorizzate su dispositivi mobili e PC (smartphone, tablet e notebook).
In particolare, il Fornitore garantisce che tali apparati:

- Siano adeguatamente protetti da accessi logici tramite l'utilizzo di credenziali di accesso forti (as es.password complesse)
- *Prevedano per impostazione predefinita la cifratura dei dati at rest (es. Bitlocker);*
- siano sempre custoditi, soprattutto in situazioni di transito in luoghi pubblici;
- non siano collocati in ambienti non idonei (ad es. locali polverosi, in prossimità di forti campi magnetici, in presenza di umidità, ecc.) e/o in ambienti privi di un adeguato livello di sicurezza;
- non espongano le informazioni ad ulteriori minacce derivanti *dall'eventuale* utilizzo *extra lavorativo dei dispositivi*.

Il fornitore dovrà avvisare tempestivamente la *Committente* di eventuali interruzioni di rapporti con le proprie risorse coinvolte nei servizi affidati dalla *Committente*, al fine di consentire alla scrivente di eliminare le credenziali in uso.
Il fornitore dovrà garantire che le informazioni gestite dalle risorsa al momento dell'interruzione del rapporto siano state preventivamente archiviate e che la risorsa non ne trattenga alcuna copia.

Il Fornitore è tenuto a mantenere strettamente riservate e a non divulgare, comunicare o rendere disponibili a terzi, senza preventiva autorizzazione scritta della Committente, tutte le informazioni, i dati e la documentazione conosciuti o acquisiti in qualunque forma nell'ambito del rapporto (incluse informazioni tecniche, commerciali, organizzative, economiche, prezzi, know-how, credenziali e procedure), impegnandosi a utilizzarli esclusivamente per l'esecuzione delle prestazioni e nei limiti necessari, adottando misure organizzative e tecniche adeguate a prevenire accessi non autorizzati, perdita o diffusione indebita; tale obbligo si estende a dipendenti, consulenti e subfornitori, che dovranno essere vincolati da obblighi non meno restrittivi.

Nelle attività di dismissione degli strumenti utilizzati per la gestione delle informazioni legate ai servizi affidati dalla *Committente*, il Fornitore garantisce che tali operazioni siano effettuate in modo sicuro e controllato, al fine di rendere irrecuperabili tali informazioni.
Il fornitore deve garantire la riservatezza, integrità e disponibilità delle informazioni legate ai servizi affidati dalla *Committente* tramite l'uso di opportuni strumenti di sicurezza quali ad esempio antimalware, firewall, meccanismi di cifratura, ecc. *adeguati al rischio.*
Infine, per tutte le attività di sviluppo software, è fatto obbligo al fornitore di:

- prevedere una separazione effettiva dei ruoli operativi, per le attività di sviluppo e test delle soluzioni applicative;
- utilizzare e dare evidenza di metodologie universalmente accettate e riconosciute (es. OWASP) per lo sviluppo sicuro del codice.

- garantire che i requisiti di sicurezza richiesti siano implementati, operati e mantenuti ed i livelli di servizio della fornitura siano quelli concordati.

La *Committente* potrà effettuare delle verifiche ispettive nei confronti dei fornitori, incentrate sulla compliance verso le politiche per la sicurezza delle informazioni.
La *Committente* incoraggia tutti i Fornitori a diffondere le regole sopra enunciate anche attraverso un'adeguata attività di formazione dei dipendenti della propria base fornitori.

10. Sicurezza della catena di fornitura

Il Fornitore deve valutare, monitorare e gestire i rischi cyber lungo la propria catena di fornitura, includendo nei contratti con sub-fornitori requisiti minimi di sicurezza, diritti di audit, obblighi di notifica incidenti e di continuità del servizio non meno rigorosi rispetto a quelli previsti nel presente documento.

11. Gestione e notifica degli incidenti

Il Fornitore è tenuto a:

1. *disporre di una procedura di incident management (rilevazione, contenimento, eradicazione, ripristino, lessons learned);*
2. *notificare alla Società all'indirizzo nis2@tinextainnovationhub.com senza indebiti ritardi ogni incidente significativo che impatti o possa impattare i servizi/ dati della Società;*
3. *assicurare la tracciabilità (log, catena di custodia) e la conservazione delle evidenze.*

12. Utilizzo di strumenti di AI

Il Fornitore nell'ambito dell'esecuzione delle attività e dei servizi previsti, qualora applicabile agli stessi, potrà utilizzare strumenti basati su tecnologie di Intelligenza Artificiale (IA), utilizzati esclusivamente a fini strumentali e di supporto alla propria prestazione, senza alcuna prevalenza sul giudizio e sulla supervisione umana, che devono restare centrali e insostituibili nel processo decisionale del Fornitore.
A tali fini, il Fornitore garantisce che:

1. *i sistemi di IA sono conformi alle disposizioni di legge e regolamentari applicabili (Regolamento UE 2024/1689 e L. 132/2025), e rispettano i principi di trasparenza, sicurezza, equità, non discriminazione e tutela dei diritti fondamentali;*
2. *l'impiego dei sistemi di IA è sempre soggetto a supervisione, verifica e controllo da parte di professionisti qualificati, con rimessione della decisione finale al personale umano del Fornitore;*
3. *Il personale autorizzato all'impiego dei sistemi di intelligenza artificiale è stato previamente sottoposto a specifici programmi di formazione tecnico-operativa e di aggiornamento normativo, al fine di garantirne un utilizzo conforme ai requisiti di sicurezza e alle disposizioni applicabili;*
4. *le operazioni svolte con supporto dell'IA sono integralmente tracciabili, documentate e accessibili per eventuali verifiche ex post, a garanzia del principio di responsabilità professionale;*
5. *i dati della Committente sono trattati in conformità alla normativa vigente in materia di protezione dei dati di natura personale (Reg. UE 2016/679, D.lgs. 196/2003 e s.m.i.).*

In particolare, il Fornitore garantisce che i dati e le informazioni della Committente saranno segregati, non saranno utilizzati per l'addestramento, il miglioramento o l'ottimizzazione dei sistemi di IA impiegati, né saranno condivisi con soggetti terzi.

13. Rispetto delle norme di legge

Al fine di evitare ricadute di natura legale, economica e di immagine per la *Committente*, Il fornitore è tenuto al rispetto della legislazione vigente in ambito protezione dei dati personali, nonché delle diverse norme che disciplinano la relazione lavorativa tra le parti.

Secondo specifiche esigenze, contrattualmente sono definite le:

- normative cui le terze parti devono attenersi;
- modalità di svolgimento delle eventuali verifiche, al fine di assicurare il rispetto delle normative;
- conseguenze in seguito al riscontro di eventuali non conformità.

14. Baseline di Sicurezza per Fornitori Tecnologici

I fornitori individuati nel precedente Capitolo 4 devono rispettare requisiti minimi di sicurezza delle informazioni, coerenti con la Direttiva (UE) 2022/2555 (NIS2) e con gli standard internazionali ISO/IEC 27001 e ISO/IEC 27701. I requisiti sono riportati nei paragrafi seguenti.

Matrice di applicabilità

La seguente matrice indica l'applicabilità generale dei controlliper ciascun tier.

Dominio	***T1 – Critico***	***T2 – Non critico***
GV – Governance & Policy	*Obbligatorio*	*Minimo*
IAM – Identità e Accessi	*Obbligatorio*	*Minimo (per accessi logici)*
AM – Asset Management & Cifratura	*Obbligatorio*	*Non necessario*
EP – Endpoint & Dispositivi Mobili	*Obbligatorio*	*Non necessario*
VM – Vulnerability Management & Patch	*Obbligatorio*	*Non necessario*
NW – Sicurezza di Rete	*Obbligatorio*	*Non necessario*
LM – Logging & Monitoring	*Obbligatorio*	*Non necessario*
IR – Incident Management & Notifiche	*Obbligatorio*	*Non necessario*
BC – Business Continuity & Backup	*Obbligatorio*	*Non necessario*
AS – Application Security / SDLC	*Obbligatorio*	*Non necessario*
CL – Cloud & SaaS Security	*Obbligatorio*	*Minimo*
DP – Protezione Dati & Crittografia	*Obbligatorio*	*Non necessario*
PH – Sicurezza Fisica & Dismissione	*Obbligatorio*	*Obbligatorio*
SR – Supplier Management & Flow-down	*Obbligatorio*	*Non necessario*
AW – Awareness & Formazione	*Obbligatorio*	*Minimo*
AU – Compliance & Audit	*Obbligatorio*	*Minimo*

GV – Governance & Policy

ID	***Requisito***	***Applicabilità (T1/T2)***
GV1	*Policy di sicurezza fornitori approvata e riesame annuale*	*T1/T2*
GV2	*Nomina referente sicurezza/contatto CSIRT per il fornitore*	*T1*
GV3	*Registro fornitori e sub-fornitori che trattano dati/sistemi della Società*	*T1/T2*
GV4	*Accettazione obblighi contrattuali di sicurezza, di riservatezza, audit e flow-down*	*T1/T2*

IAM – Identità e Accessi

ID	***Requisito***	***Applicabilità (T1/T2)***
IAM1	*Account nominativi; divieto account condivisi per accessi alla Società*	*T1/T2*
IAM2	*MFA obbligatoria su tutti gli accessi a sistemi/servizi della Società*	*T1/T2*
IAM3	*Principio del minimo privilegio e approvazione accessi*	*T1*
IAM4	*Revoca accessi entro 24h dalla cessazione/trasferimento risorsa*	*T1/T2*
IAM5	*Riesame periodico degli accessi amministrativi*	*T1*

AM – Asset Management & Cifratura

ID	*Requisito*	*Applicabilità (T1/T2)*
AM1	*Inventario asset che trattano dati/sistemi della Società*	*T1*
AM2	*Classificazione dati e indicazione requisiti di protezione*	*T1*
AM3	*Cifratura dati a riposo su dispositivi e storage*	*T1*
AM4	*Cifratura in transito per dati della Società*	*T1*
AM5	*Supporti rimovibili vietati salvo eccezioni autorizzate e cifrate*	*T1*

EP – Endpoint & Dispositivi Mobili

ID	***Requisito***	***Applicabilità (T1/T2)***
EP1	*Gestione MDM/EMM per dispositivi mobili e laptop*	*T1*
EP2	*Cifratura disco completa su endpoint*	*T1*
EP3	*EDR/antimalware con monitoraggio attivo*	*T1*
EP4	*Patch OS/applicazioni con SLO definiti*	*T1*
EP5	*Blocco schermo automatico e timeout sessione*	*T1*

VM – Vulnerability Management & Patch

ID	***Requisito***	***Applicabilità (T1/T2)***
VM1	*Scansioni di vulnerabilità periodiche su asset esposti/critici*	*T1*
VM2	*Remediation SLO per vulnerabilità*	*T1*
VM3	*Pen-test annuale per sistemi esposti su Internet*	*T1*
VM4	*Gestione disclosure e vulnerabilità zero-day*	*T1*

NW – Sicurezza di Rete

ID	*Requisito*	*Applicabilità (T1/T2)*
NW1	*Accessi remoti tramite VPN sicura o zero-trust*	*T1*
NW2	*Segregazione reti e ambienti (dev/test/prod)*	*T1*
NW3	*Firewall/filtri in ingresso e uscita con regole minime*	*T1*
NW4	*Disabilitazione protocolli insicuri/legacy*	*T1*

LM – Logging & Monitoring

ID	***Requisito***	***Applicabilità (T1/T2)***
LM1	*Raccolta centralizzata dei log di sicurezza*	*T1*

LM2	*Sincronizzazione oraria (NTP) su sistemi critici*	*T1*
LM3	*Monitoraggio eventi chiave (autenticazioni, privilegi, cambi config)*	*T1*
LM4	*Protezione integrità dei log*	*T1*

IR – Incident Management & Notifiche

ID	***Requisito***	***Applicabilità (T1/T2)***
IR1	*Procedura di gestione incidenti allineata a NIS2/ACN*	*T1*
IR2	*Notifica incidenti significativi alla Società*	*T1/T2*
IR3	*Conservazione evidenze e tracciabilità (chain of custody)*	*T1*

BC – Business Continuity & Backup

ID	***Requisito***	***Applicabilità (T1/T2)***
BC1	*Piani BC/DR per servizi erogati alla Società*	*T1*
BC2	*Strategia di backup 3-2-1 (o equivalente) con test di ripristino*	*T1*
BC3	*Definizione RTO/RPO per servizi critici*	*T1*

AS – Application Security / SDLC

ID	***Requisito***	***Applicabilità (T1/T2)***
AS1	*Adozione di pratiche OWASP e code review per software sviluppato*	*T1*
AS2	*SAST/DAST su applicazioni critiche*	*T1*
AS3	*Gestione dipendenze e SBOM*	*T1*
AS4	*Segregazione ambienti dev/test/prod*	*T1*

CL – Cloud & SaaS Security

ID	***Requisito***	***Applicabilità (T1/T2)***
CL1	*Definizione responsabilità condivise (shared responsibility) e hardening (es. CIS Benchmarks)*	*T1*
CL2	*Logging/monitoring a livello tenant e servizi gestiti*	*T1*
CL3	*Protezione dati a riposo e in transito per servizi cloud*	*T1/T2*

DP – Protezione Dati & Crittografia

ID	***Requisito***	***Applicabilità (T1/T2)***
DP1	*Crittografia dei dati della Società (at-rest/in-transit)*	*T1*
DP2	*Gestione chiavi/secret management*	*T1*
DP3	*Minimizzazione e segregazione dati*	*T1*
DP4	*DLP o controlli equivalenti per dati ad alta sensibilità*	*T1*

PH – Sicurezza Fisica & Dismissione

ID	*Requisito (shall)*	*Applicabilità (T1/T2)*
PH1	*Controllo accessi fisici ad aree/sistemi della Società*	*T1/T2*
PH2	*Protezione siti/armadi (lock, CCTV, ambienti idonei)*	*T1*
PH3	*Dismissione sicura e cancellazione certificata dei supporti*	*T1/T2*

SR – Supplier Management & Flow-down

ID	***Requisito***	***Applicabilità (T1/T2)***
SR3	*Autorizzazione preventiva per subappalto di attività critiche*	*T1*

AW – Awareness & Formazione

ID	***Requisito***	***Applicabilità (T1/T2)***
AW1	*Formazione annuale su igiene cyber, phishing, gestione incidenti*	*T1/T2*
AW2	*Formazione specifica per amministratori e personale con privilegi*	*T1*

AU – Compliance & Audit

AU3	*Gestione non conformità e piani di rimedio*	*T1*