# Standard di Sicurezza Informatica per i Fornitori

## Sezione A – tutti i fornitori

TUTTI i fornitori sono tenuti a rispettare gli standard di sicurezza informatica dettagliati di seguito.

1. I fornitori devono poter dimostrare una cultura di consapevolezza in materia di standard di sicurezza informatica all'interno delle proprie aziende, ivi incluso a titolo esemplificativo e non esaustivo quanto segue:
    I. prova di adesione a standard di sicurezza informatica riconosciuti (ad es., quelli specificati in Cyber Essentials);
    II. formazione dei dipendenti in materia di standard di sicurezza informatica, incluso un programma di costante miglioramento;
    III. backup efficaci; politiche di risposta agli incidenti; piani di disaster recovery ecc.

2. Phishing e malware sono spesso originati da fornitori compromessi. Pertanto, i fornitori sono tenuti a dimostrare l'utilizzo di validi sistemi di sicurezza informatica, ivi incluso quanto segue:
    I. un sistema di posta elettronica con autenticazione a più fattori (MFA) o altre misure di protezione, ad es. DMARC;
    II. processi in essere per garantire un'attiva e tempestiva notifica nel caso in cui il fornitore rilevi una compromissione dei suoi sistemi o episodi di Phishing.

3. In caso di compromissione da Phishing o malware, originati dal fornitore e rilevati da INEOS Inovyn, dovrà avvenire un chiaro percorso di riassegnazione per il fornitore.

4. La frode finanziaria viene tentata spesso attraverso e-mail intercettate che chiedono al destinatario di modificare le credenziali bancarie. La politica anti-frodi di INEOS Inovyn prevede che i fornitori dispongano di processi chiari attraverso i quali notificare a INEOS Inovyn le modifiche legittime, con nominativi di contatto da poter impiegare per controlli indipendenti al fine di verificarne la validità.

5. I fornitori con dati archiviati riconducibili a INEOS Inovyn devono assicurare che tale archiviazione sia conforme ai requisiti di Protezione legale dei dati relativi al Paese, inclusi:
    I. Conformità al Regolamento Generale sulla Protezione dei Dati (GDPR) o regolamento equivalente;
    II. I dati INEOS Inovyn archiviati su dispositivi portatili, come laptop, adottino una crittografia completa del disco.

6. Tutti i metodi impiegati per il trasferimento software o dati nell'ambito del lavoro dei fornitori devono impiegare metodi di sicurezza adeguati, quali ad esempio:
    I. un sito sicuro SharePoint ospitato da INEOS Inovyn

II. un sito sicuro di trasferimento file messo a disposizione dal fornitore e certificato da INEOS Inovyn.

7. I dispositivi portatili di trasferimento dati quali chiavette e pen drive USB devono essere impiegati solo nel caso in cui non siano disponibili altri mezzi pratici, e devono comunque essere conformi alle politiche INEOS Inovyn e ai controlli al momento dell'uso.

## Sezione B –fornitori di sistemi e risorse che lavorano sui sistemi INEOS Inovyn

In aggiunta alla Sezione A, TUTTI i fornitori di sistemi, attrezzature e risorse che lavorano su sistemi INEOS Inovyn dovranno assicurarsi di soddisfare anche i seguenti requisiti.

8. I sistemi forniti e le attrezzature rimarchiate devono utilizzare piattaforme supportate dal venditore con un'aspettativa di vita utile di almeno 5 anni. Ciò include:
   I. Sistemi operativi (SO);
   II. firmware;
   III. ricorso a eventuali applicazioni, componenti e browser web di terzi.

9. I sistemi forniti devono poter essere **aggiornati contro vulnerabilità future**, ad es.:
   I. applicazione di patch di sistema operativo periodiche;
   II. applicazione di versioni aggiornate del sistema operativo;
   III. il fornitore deve dichiarare i processi di verifica e approvazione delle patch, ad es. durata della fase di qualifica del fornitore, disposizioni speciali per patch particolarmente critiche.

10. I sistemi forniti devono garantire la protezione informatica, includendo misure quali:
    I. protezione anti-virus di base;
    II. protezione mediante whitelisting per applicazioni;
    III. protezione malware avanzata;
    IV. protezione della rete mediante dispositivi firewall;
    V. il fornitore non deve essere stato identificato dal governo come intrinsecamente poco sicuro dal punto di vista informatico, e di conseguenza sottoposto a restrizioni.

11. Se a un fornitore viene consentito l'accesso da remoto ai sistemi INEOS Inovyn, tutti gli accessi devono essere eseguiti esclusivamente per scopi leciti, e solo ai sistemi preposti alle finalità del supporto, accordi sul livello del servizio (SLA), ecc:
    I. i. tutte le suddette operazioni devono essere concordate con INEOS Inovyn prima di avere luogo, e devono essere oggetto di regolare verifica (almeno annuale).

12. In caso di concessione di accesso da remoto a una qualsiasi delle parti dei sistemi INEOS Inovyn, potrebbero essere richiesti requisiti aggiuntivi, quali:
    I. i. solo nominativi individuali, che implichino eventuali controlli di referenze, riscontri di formazione, nominativi concordati di sostituti, ecc;
    II. un'autenticazione a due fattori posseduto da INEOS Inovyn.

13. Laddove a essere forniti a INEOS Inovyn fossero risorse e non sistemi, si richiede che tutte le risorse possano operare seguendo le linee guida di INEOS Inovyn per la sicurezza informatica, sia quando sono operative sui nostri siti che quando operano altrove ma per conto di INEOS Inovyn. Tali guide vengono abitualmente comunicate nell'ambito del processo di orientamento di INEOS Inovyn.

FINE DOCUMENTO

V1. Agosto 2020