PIS 009

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI NEI RAPPORTI CON I FORNITORI

EMESSO	02/08/2019	AHANONU Chidi			
APPROVATO DALLA DIREZIONE	02/08/2019	ROATI Gianfranco			
CLASSIFICAZIONE DOCUMENTO		☒	PUBBLICA	☐	CONFIDENZIALE
		☐	USO INTERNO	☐	RISTRETTO

INDICE DELLE REVISIONI

REVISIONI	DATA EMESSIONE	PRINCIPALI MODIFICHE
00	02/08/2019	Prima Emissione
01	10/09/2019	Paragrafo 3.2
02	07/10/2019	Paragrafo 3.3

SOMMARIO

1 RIFERIMENTI NORMATIVI

- ISO 27001
- GDP regolamento (UE) n. 2016/679

2 SCOPO DEL DOCUMENTO

Al fine di mitigare i rischi associati all'accesso agli asset di INSIS S.p.a. da parte dei propri fornitori, è stata predisposta la presente politica che definisce i requisiti di sicurezza delle informazioni.

3 POLITICA

3.1 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Insis implementa e mantiene un Sistema di Gestione delle Informazioni sicuro seguendo i requisiti specificati nella Norma UNI CEI EN ISO/IEC 27001:2017, così da garantire:

1. Riservatezza - informazioni accessibili solamente ai soggetti e/o ai processi debitamente autorizzati;
2. Integrità - salvaguardia della consistenza dell'informazione da modifiche non autorizzate;
3. Disponibilità - garanzia che i processi e strumenti per la gestione dei dati siano sicuri e testati;
4. Autenticità - provenienza affidabile dell'informazione;
5. Privacy - garanzia di protezione e controllo dei dati personali.

La mancanza di adeguati livelli di sicurezza delle informazioni può comportare il danneggiamento dell'attività di INSIS, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica, finanziaria e di immagine dell'azienda e della filiera sottostante.

L'impegno della direzione Insis, che si richiede applicazione anche da parte dei fornitori, si attua tramite la definizione di una struttura organizzativa adeguata a:

- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento della Sicurezza delle Informazioni;
- controllare che la politica per la Sicurezza delle Informazioni sia integrata in tutti i processi aziendali e che le procedure ed i controlli siano sviluppati coerentemente ed efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni;
- attivare programmi per diffondere la consapevolezza e la cultura sulla sicurezza delle informazioni.
- Gli obiettivi generali di INSIS S.p.a., che i fornitori di Insis dovranno a loro volta perseguire, sono quindi:
- garantire i migliori standard, ottimizzando e razionando i processi e gli strumenti aziendali;
- garantire l'efficacia delle procedure e controlli per la Sicurezza delle Informazioni;
- garantire la soddisfazione di Insis in relazione alla quantità delle informazioni.

Il fornitore deve assicurare che tutto il personale deve operare per il raggiungimento degli obiettivi di sicurezza nella gestione delle informazioni e deve impiegare le tecnologie più adeguate a garantire il rispetto della presente politica.

3.2 REQUISITI DI SICUREZZA DELLE INFORMAZIONI PER I FORNITORI

Il fornitore si impegna ad osservare le linee guida della precedente Politica per la Sicurezza delle Informazioni

Lo scambio disegni o altri documenti richiamati in Oda deve avvenire:

- Per i documenti sorgente (disegni, specifiche etc.), documenti confidenziali o protetti da IPR, su FTP di Insis o tramite e-mail come allegati in cartelle criptate con password; in entrambi i casi, sarà cura di Insis fornire, attraverso canali differenti, riferimenti e credenziali alla persona indicata in NDA (o comunque autorizzata allo scambio di dati)
- Via e-mail per tutti gli altri documenti quali cronoprogrammi, informazioni non riservate etc.

Le persone che potranno ricevere informazioni da Insis, ad eccezione quelle pubbliche, sono quelle indicate nell'NDA se sottoscritto tra le parti o diversamente autorizzate da entrambi le parti

Il fornitore si impegna ad attuare soluzioni per la protezione da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate

In caso di necessità di accesso agli asset di Insis da parte del fornitore, lo stesso dovrà essere preventivamente autorizzato e informato delle modalità di utilizzo degli stessi, cui dovrà attenersi scrupolosamente e sarà soggetti ai controlli previsti dalle politiche Insis

Per i fornitori associati ai servizi e ai prodotti della filiera di fornitura per l'ICT, il fornitore si impegna a rispettare i requisiti Insis per affrontare i rischi relativi alla sicurezza delle informazioni, richiedendo preventivamente ad Insis la copia delle Politiche e Procedure Applicabili.

3.3 MONITORAGGIO E RIESAME DEI SERVIZI EROGATI DAL FORNITORE

Al fine di avere una visibilità complessivamente sufficiente su tutti gli aspetti di sicurezza relativi alle informazioni critiche o alle strutture di elaborazione delle informazioni, Insis monitora i livelli di prestazione del servizio ricevuto al fine di verificare il rispetto degli accordi. Potranno essere condotti audit ai propri fornitori, congiuntamente al riesame dei rapporti di fornitura.

3.4 GESTIONE DEGLI ACCESSI ALLA RETE ED AI SERVIZI DI RETE

Qualora il servizio richiesto al fornitore richieda di operar all'interno della rete Insis, allo stesso verrà fornito l'accesso con le seguenti modalità e solo per i servizi ai quali sono stati specificatamente autorizzati dai singoli accordi con INSIS Spa:

- Il fornitore dovrà comunicare il nominativo degli operatori che saranno preventivamente approvati da Insis per operare sulla rete
- Agli stessi verrà comunicata una password verbalmente, che non dovrà essere modificata;
- Al momento della necessità di attivare il servizio, all'operatore autorizzato verrà abilitato da ICT Manager l'accesso alla VPN per l'accesso remoto alla rete aziendale, per un periodo definito.
- Al termine del periodo, ICT Manager disattiverà l'abilitazione VPN
- Le attivazioni e disattivazione degli accessi VPN, sono registrati dal responsabile ICT attraverso portali dedicati.

3.5 CONTROLLO DEI LOG

L'utente (operatore del fornitore) è soggetto al controllo dei Log da parte del personale ICT di Insis.

3.6 GESTIONE PASSWORD

Gli utenti si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso indicati all'interno di questo documento.

La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno dell'organizzazione.

Gli utenti devono prestare attenzione a fornire le proprie credenziali di accesso, rispondere ad e-mail sospette e/o cliccare sui link durante la navigazione web (o nella mail) al fine di contrastare possibili frodi informatiche (come il phishing, lo spear phishing, il furto di identità etc.).

Ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account.

Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà segnalarlo a CED Insis.

Per la conservazione sicura delle credenziali di accesso è consigliabile evitare di memorizzarle su documenti cartacei o file conservati all'interno della postazione di lavoro.

3.7 ACCESSI FISICI

L'azienda ha predisposto un sistema di controllo perimetrale, con varchi di accesso attraverso l'utilizzo di badge per proteggere le aree che contengono informazioni critiche e strutture di elaborazione.

Al fine di proteggere e limitare l'accesso ad aree che contengono informazioni critiche l'azienda ha predisposto vari sistemi anti-intrusione, il cui layout sono ad uso esclusivo della proprietà.

Da bordo strada, l'accesso può avvenire attraverso:

- nr. 2 cancelli (cerchi rossi) che si aprono esclusivamente attraverso badge di riconoscimento,
- nr. 1 cancelletto pedonale (freccia blu), che si apre dalla reception.

Superato questo primo varco, l'intero plesso strutturale consta di 7 accessi di cui:

- nr. 5 Porte carrabili (frecce verdi) posti in prossimità dell'area di stoccaggio materiali. Queste porte rimangono sono chiuse e non vengono aperte se non per casi eccezionali;
- nr. 1 Porta carrabile (frecce arancione) usata per attività di carico scarico. L'area di carico-scarico è nettamente separata dall'area di "elaborazione delle informazioni";

- nr. 1 portone ingresso, dotato di sistema doppio varco. L'accesso avviene attraverso badge di riconoscimento.

3.7.1 Consegna del badge

Al personale autorizzato da Insis ad accedere alle proprie strutture, viene consegnato in reception un badge di accesso. Il badge è contraddistinto da logo, dicitura "Visitatore" ed è di proprietà di Insis S.p.A.

Lo stesso deve essere esposto durante la permanenza in struttura e riconsegnato all'uscita e non deve essere ceduto a terzi (nemmeno temporaneamente). In caso di smarrimento deve tempestivamente segnalarlo alla Reception, che attiverà le procedure di segnalazione dell'evento al RSGSI.

3.8 SANZIONI

Il mancato od il ritardato adempimento di quanto previsto dalla presente politica aziendale e/o dal contratto stipulato tra le parti, che dovessero provocare dei danni, comporteranno il conseguente obbligo di risarcimento dei danni in favore di Insis spa oltre alle eventuali sanzioni amministrative pecuniarie e/o penali previste dal GDPR 2016/679 e/o dalla normativa vigente