Politica per la Sicurezza delle Informazioni per i Fornitori

Rev B

CENTRIC

Politica per la Sicurezza delle Informazioni per i Fornitori

SCOPO

Lo scopo del presente documento è quello di definire i requisiti di sicurezza delle informazioni nei rapporti con i Fornitori al fine di mitigare i rischi associati all'accesso agli asset di IT CENTRIC da parte di soggetti esterni.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

IT CENTRIC S.p.A. implementa e mantiene un Sistema di Gestione per la sicurezza delle Informazioni in accordo ai requisiti specificati nella norma ISO/IEC 27001, nel Regolamento UE 2016/679 e nelle disposizioni nazionali ed europee in materia di cybersecurity, in modo da garantire:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. **Controllo**: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità**: garantire una provenienza affidabile dell'informazione;
6. **Privacy**: garantire la protezione ed il controllo dei dati personali.

La mancanza di adeguati livelli di sicurezza delle informazioni può comportare il danneggiamento dell'attività di IT CENTRIC, 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.
La Direzione di IT CENTRIC è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con l'azienda nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati.

Per questi motivi la Direzione di IT CENTRIC promuove tutte le azioni necessarie affinché i processi e le attività siano orientati al raggiungimento dei seguenti obiettivi:

- Identificare le esigenze di sicurezza tramite l'analisi dei rischi al fine di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo;
- Attuare le azioni necessarie per mitigare i rischi individuati e le misure di sicurezza più idonee;
- Garantire la massima sicurezza delle informazioni dei clienti, in termini di riservatezza, disponibilità e integrità;
- Dare continuità operativa ai servizi critici anche a seguito di gravi incidenti;
- Tutelare i diritti e gli interessi di tutti coloro che interagiscono con l'azienda (clienti, dipendenti, collaboratori, terze parti, ecc.);
- Salvaguardare gli interessi degli investitori e dei partners;
- Garantire un livello di servizio eccellente.

I Fornitori devono assicurare che tutto il personale operari per il raggiungimento dei suindicati obiettivi di sicurezza nella gestione delle informazioni e impieghino le tecnologie più adeguate a garantire il rispetto della presente politica.

REQUISITI DI SICUREZZA PER LA TRASMISSIONE DELLE INFORMAZIONI

Lo scambio di documenti e informazioni tra IT CENTRIC e il Fornitore deve avvenire in modo controllato e sicuro in accordo al sistema di classificazione ed etichettatura adottato dall'azienda e al quale il Fornitore deve adeguarsi. Tale sistema prevede in particolare i seguenti livelli di classificazione delle informazioni:

1. di dominio pubblico (non necessitano di alcuna etichettatura)
2. ad uso interno
3. riservato (o confidenziale)
4. strettamente riservato

Nel caso si debbano discutere o scambiare informazioni confidenziali tra IT CENTRIC e il Fornitore, o tra un Fornitore e terzi, le parti devono prima assicurarsi di aver sottoscritto un Accordo di riservatezza o di non divulgazione.

Per le informazioni digitalizzate la trasmissione deve avvenire in modo cifrato attraverso FTPS, posta elettronica o PEC con utilizzo del protocollo TLS; nel corpo del messaggio di posta elettronica deve essere presente un'intestazione standardizzata in cui si avverte della confidenzialità/riservatezza del messaggio; gli allegati di posta elettronica possono essere cifrati con password per assicurare maggiore protezione alle Informazioni Riservate ritenute più critiche (es. dati personali particolari o giudiziari).

Le informazioni riservate che sono comunicate in forma verbale devono essere considerate tali nel momento in cui il soggetto che le comunica le indicherà come "riservate" all'altra parte.

Il fornitore si impegna ad attuare soluzioni per la protezione delle informazioni da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate. In caso di necessità di accesso agli asset di IT CENTRIC da parte del Fornitore, lo stesso dovrà essere preventivamente autorizzato e informato delle modalità di utilizzo degli stessi, cui dovrà attenersi scrupolosamente e sarà soggetto ai controlli previsti dalle politiche di sicurezza di IT CENTRIC.

Per i Fornitori associati ai servizi e ai prodotti della filiera di fornitura per l'ICT, il Fornitore deve impegnarsi a rispettare i requisiti di IT CENTRIC per affrontare i rischi relativi alla sicurezza delle informazioni, richiedendo preventivamente a IT CENTRIC la copia delle policy applicabili.

MONITORAGGIO E RIESAME DEI SERVIZI EROGATI DAL FORNITORE

Al fine di assicurare il controllo su tutti gli aspetti di sicurezza relativi alle informazioni critiche o alle strutture di elaborazione delle informazioni, IT CENTRIC monitora i livelli di prestazione del servizio erogato e ricevuto dal Fornitore al fine di verificare il rispetto degli accordi. Potranno essere condotti audit ai propri Fornitori, congiuntamente al riesame dei rapporti di fornitura.

GESTIONE DEGLI ACCESSI ALLA RETE ED AI SERVIZI DI RETE

Qualora il servizio richiesto al Fornitore richieda di operare all'interno della rete IT CENTRIC, 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 IT CENTRIC:

- Il Fornitore dovrà comunicare il nominativo degli operatori che saranno preventivamente approvati da IT CENTRIC per operare sulla rete;

- Agli stessi verrà assegnata una credenziale di autenticazione composta da userID e password da modificare al primo accesso.

CONTROLLO DEI LOG

L'utente (operatore del Fornitore) è soggetto al controllo dei Log da parte del personale ICT di IT CENTRIC.

GESTIONE PASSWORD

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

Le password devono essere lunghe almeno otto caratteri, non devono contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente, devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole, non devono essere uguale alle precedenti.

La password deve essere obbligatoriamente modificata ogni sei mesi ; nel caso di trattamento di dati personali particolari e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi.

La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno o all'esterno 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 dallo stesso messaggio di posta ricevuto, al fine di contrastare possibili frodi informatiche (es. phishing, furto di identità, ecc.).

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 personale IT di IT CENTRIC.

Per la conservazione sicura delle credenziali di accesso si consiglia di evitare la memorizzazione su documenti cartacei o in file conservati all'interno della postazione di lavoro.

ACCESSI FISICI

IT CENTRIC ha predisposto un sistema di controllo perimetrale per l'accesso alla sede, agli uffici e ai locali in cui si trattano informazioni. L'accesso è consentito solo al personale autorizzato, per cui se il Fornitore ha necessità di accedere agli uffici o ai locali della sede di IT CENTRIC deve disporre di autorizzazione specifica e rispettare le misure di sicurezza fisica ed ambientale applicate.

COMUNICAZIONE EVENTI DI SICUREZZA

Ogni segnalazione di vulnerabilità, eventi ed incidenti di sicurezza rilevati nel corso delle attività svolte dal Fornitore deve essere comunicata in modo formale anche per il tramite della posta elettronica al referente del contratto di IT CENTRIC per la successiva gestione e risoluzione della problematica.

SANZIONI

Il mancato o il ritardato adempimento di quanto previsto dalla presente politica aziendale e/o dal contratto stipulato tra le parti, che dovesse provocare dei danni di natura economica, finanziaria e di immagine alla IT CENTRIC e alla filiera sottostante, comporterà il conseguente obbligo di risarcimento in favore di IT CENTRIC, oltre alle eventuali sanzioni amministrative pecuniarie e/o penali previste dal Regolamento GDPR 2016/679 e/o dalla normativa vigente.