D00 Politica Generale per la Sicurezza delle Informazioni

Ver.	Data	Descrizione	Redatto	Verificato
0100	30/04/2021	Prima emissione	Responsabile sicurezza delle informazioni	Direzione Generale
0101	30/03/2022	Aggiornamento	Responsabile sicurezza delle informazioni	Direzione Generale
0102	16/05/2022	Aggiornamento	Responsabile sicurezza delle informazioni	Direzione Generale

Sommario

1 INTRODUZIONE

1.1 Scopo

L'insieme di dati ed informazioni trattate da Opentech S.r.l., a prescindere dalla forma con cui esse siano elaborate, gestite o archiviate, determina il Patrimonio Informativo aziendale che costituisce un elemento competitivo di fondamentale importanza sia per guidare le scelte tattiche/strategiche che per supportare i processi operativi aziendali.

Opentech attribuisce quindi al patrimonio informativo un valore strategico e rivolge pertanto una grande attenzione alla Sicurezza delle Informazioni proprie e/o conferite ad essa da dipendenti, clienti, fornitori ed altri attori esterni ed in generale di tutti i beni informativi che appartengono al perimetro aziendale, nel pieno rispetto del quadro normativo vigente, di legge e di settore.
Su tali basi, Opentech ha deciso di realizzare un Sistema di Gestione per la Sicurezza delle Informazioni (di seguito "SGSI") definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento, in conformità ai requisiti delle norme internazionali UNI EN ISO/IEC 27001, UNI EN ISO/IEC 27017 e UNI EN ISO/IEC 27018.
Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da Opentech al fine di sviluppare un efficace e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

1.2 Applicabilità

La politica per la sicurezza delle informazioni di Opentech deve essere conosciuta, ed i principi in essa contenuti rispettati integralmente, da tutti coloro, personale interno, collaboratori, fornitori e tutte le terze parti, che a vario titolo entrano in contatto con le informazioni protette dal SGSI di Opentech.
La presente politica è distribuita mediante il sito internet aziendale, che ne mette a disposizione la versione approvata più aggiornata; di conseguenza, è responsabilità del lettore assicurarsi di ottenere la versione più aggiornata ed attuale del documento.

2 RIFERIMENTI NORMATIVI

Norme di legge

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- D.lgs. 231/2001, art.24-bis "Delitti informatici e trattamento illecito di dati";
- D.lgs. 169/99 "Attuazione direttiva 96/9/CE per tutela giuridica delle banche di dati";
- D.lgs. 259/2003 "Codice delle comunicazioni elettroniche";
- D.lgs. 196/2003 "Codice in materia di protezione dei dati personali";
- Provvedimento del Garante per la Protezione dei Dati Personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di Sistema" (Provvedimento del 27/11/2008);
- Legge 22 aprile 1941, n.633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio";
- Provvedimento del Garante per la Protezione dei Dati "Misure concernenti la videosorveglianza" (Provvedimento del 8/04/2010);
- Legge 23 dicembre 547/93 "Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica";
- Legge 18 marzo 48/2008 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23/11/2001, e norme di adeguamento dell'ordinamento interno" (Convenzione di Budapest).

Standard di riferimento

- ISO/IEC 27001:2013 "Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti";
- ISO/IEC 27000 "Tecnologie informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza dell'informazione – Descrizione e vocabolario".
- ISO/IEC 27002:2013 "Tecnologie informatiche – Tecniche di sicurezza – Code of practice for information - security controls."
- ISO/IEC 27017:2015 "Tecnologie informatiche – Tecniche di sicurezza – Code of practice for information security controls based on ISO/IEC 27002 for cloud services"
- ISO/IEC 27018:2019 – "Codice di condotta per la protezione delle PII (Personally Identifiable information) nei servizi di public cloud per i cloud provider"

3 OBIETTIVI DI SICUREZZA

La Sicurezza delle Informazioni ha come obiettivo primario la protezione dei dati e degli elementi del sistema informativo responsabile del loro trattamento e conservazione. In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere le seguenti proprietà delle stesse:

- Riservatezza: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione e conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- Integrità: garanzia che ogni dato aziendale sia realmente quello originariamente archiviato e sia stato modificato secondo le procedure. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere alterate da soggetti non autorizzati;
- Disponibilità: garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

La mancanza di adeguati livelli di sicurezza, in termini di Riservatezza, Disponibilità, Integrità, può comportare per la Società il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.

Con la presente Politica generale Opentech intende formalizzare i seguenti obiettivi da realizzare nell'ambito della Sicurezza delle Informazioni:

- la salvaguardia delle informazioni e dei dati dell'organizzazione da accessi non autorizzati, da alterazioni non autorizzate e da danni accidentali o intenzionali che ne potrebbero compromettere l'accesso e l'impiego da parte dei soggetti autorizzati;
- la protezione dei sistemi e delle infrastrutture (informatiche e non) impiegate per il trattamento e la conservazione delle informazioni aziendali;
- l'aumento del livello di consapevolezza e di competenza sui temi di Sicurezza delle Informazioni nel personale interno ed esterno con cui l'organizzazione interagisce nell'ambito della conduzione dei propri processi e dell'erogazione dei servizi;
- il rispetto dei requisiti legali, regolamentari e contrattuali e degli standard in materia di Sicurezza delle Informazioni.

4 PRINCIPI GENERALI

Di seguito sono espressi i principi che determinano e sostengono la definizione ed attuazione del SGSI a garanzia della sicurezza delle informazioni.

Principio 1	Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione di soluzioni e servizi e ai dati ad essi collegati.
Principio 2	Tutte le informazioni essenziali relative ai prodotti di Opentech (ad es.: documenti tecnici e commerciali, codice sorgente, informazioni di configurazione, e-mail relative al servizio, informazioni fornite dai clienti delle soluzioni, ecc.) devono essere protette.
Principio 3	Tutte le informazioni da proteggere devono essere gestite secondo il livello di classificazione attribuito, nel rispetto delle relative procedure, lungo tutto il loro ciclo di vita.
Principio 4	La sicurezza delle informazioni costituisce un aspetto fondamentale nel successo di Opentech e per il conseguimento degli obiettivi di business.
Principio 5	Tutti coloro i quali entrano a vario titolo in contatto con le informazioni da proteggere hanno un ruolo diretto nel successo di tale protezione. È dunque responsabilità diretta ed esplicita di tali soggetti attenersi ai principi contenuti nella presente politica ed in tutte le politiche di sicurezza applicabili ad essa correlate e garantirne il rispetto.
Principio 6	La sicurezza delle informazioni viene progettata ed attuata in modo da essere parte integrante dei normali processi e comportamenti di business, e definita in modo da non pregiudicare l'adeguatezza degli stessi ai fini ed agli scopi dell'organizzazione.
Principio 7	Il conseguimento degli obiettivi di sicurezza viene governato mediante un approccio basato sul rischio, che prevede l'applicazione di un processo di gestione del rischio che tiene in considerazione il contesto dell'organizzazione, il campo di applicazione del SGSI, gli obiettivi dell'organizzazione.
Principio 8	L'organizzazione adotta un processo strutturato per la gestione degli incidenti di sicurezza delle informazioni mirato a contenerne gli impatti, ad individuarne le cause ed a favorirne la rimozione. Tutti i soggetti interessati dal SGSI sono tenuti alla segnalazione di circostanze anomale o sospette riguardo alle informazioni.

I principi generali adottati in Opentech, che determinano e sostengono la definizione ed attuazione del SGSI a garanzia della sicurezza delle informazioni, si applicano nei seguenti ambiti:

1. Organizzazione per la Sicurezza delle Informazioni: assicurare l'individuazione dei ruoli e l'attribuzione delle autorità e responsabilità per la Sicurezza delle Informazioni, nonché la costituzione di processi organizzativi in grado di garantire l'omogenea e corretta applicazione della presente Politica;
2. Gestione del rischio per la Sicurezza delle Informazioni: definire un processo per l'adozione di criteri e metodologie per la determinazione e la valutazione dei rischi per la Sicurezza delle Informazioni e per il relativo trattamento e riduzione ad un livello accettabile per l'organizzazione;
3. Classificazione e protezione delle informazioni e dei beni aziendali: proteggere le informazioni aziendali trattate e conservate all'interno ed all'esterno dell'organizzazione tramite l'adozione di misure di sicurezza adeguate al relativo livello di riservatezza;
4. Controllo degli accessi logici ai sistemi informativi: garantire la coerenza delle abilitazioni di accesso ai sistemi informativi ai principi del "need to know" (necessità di conoscere) e del privilegio minimo, garantendo al contempo il rispetto della segregazione dei ruoli;
5. Controllo degli accessi fisici alle sedi ed agli impianti: limitare l'accesso alle sedi ed agli impianti di elaborazione, trattamento e memorizzazione delle informazioni aziendali ai soli soggetti, mezzi e materiali autorizzati;
6. Sicurezza delle infrastrutture e sistemi IT, delle reti e delle dotazioni informatiche: garantire l'adozione di misure di sicurezza logiche, fisiche ed organizzative tali da consentire una sicura gestione dei sistemi informativi;
7. Gestione degli eventi critici: garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e gestiti attraverso sistemi di prevenzione, comunicazione e reazione, al fine di minimizzare l'impatto sul business;
8. Continuità Operativa: stabilire misure per la continuità operativa tali da consentire di fronteggiare, in caso di guasti, malfunzionamenti o eventi disastrosi, le situazioni che potrebbero impedire la normale operatività;
9. Gestione della Conformità: definire misure adeguate per assicurare la conformità alle leggi, ai regolamenti, alle normative interne e agli standard applicabili all'organizzazione.

Per la realizzazione degli obiettivi nell'ambito della Sicurezza delle Informazioni, Opentech ha definito e si impegna a mantenere aggiornate nel tempo norme e procedure con riferimento agli ambiti di gestione sopra illustrati; tali norme e procedure, congiuntamente alla presente Politica generale, costituiscono l'insieme di regole che guidano l'implementazione dei meccanismi di protezione per le diverse tipologie di informazioni e beni aziendali.

6 IMPEGNO DELLA DIREZIONE

La Direzione è pienamente coinvolta nel rispetto e nell'attuazione dei principi richiamati nella presente politica, assicurando e verificando che sia resa operativa e diffusa a tutto il personale.
In particolare, la Direzione si impegna a:

- comunicare la presente Politica a tutti i dipendenti e diffonderla a tutti i soggetti esterni, poiché chiunque intrattenga rapporti di lavoro o collabori a diverso titolo con l'azienda è chiamato a garantire il rispetto dei requisiti di sicurezza qui contenuti;
- coinvolgere e responsabilizzare il personale nelle attività previste dalla presente Politica;
- promuovere tutte le iniziative necessarie al fine di garantire la piena implementazione della presente Politica e il raggiungimento degli obiettivi dell'azienda per la sicurezza delle informazioni;
- definire obiettivi e strategie operative coerenti con gli elementi descritti nella seguente Politica.

7 POLITICA PER L'UTILIZZO DI SERVIZI CLOUD

In considerazione dei seguenti aspetti:

- le informazioni archiviate nell'ambiente di cloud computing possono essere soggette all'accesso e alla gestione da parte del fornitore di servizi cloud;
- le risorse possono essere mantenute nell'ambiente di cloud computing, ad esempio programmi applicativi;
- i processi possono essere eseguiti su un servizio cloud virtualizzato multi-tenant;
- gli utenti del servizio cloud e il contesto in cui utilizzano il servizio cloud;
- gli amministratori del servizio cloud del cliente del servizio cloud che hanno accesso privilegiato;
- le posizioni geografiche dell'organizzazione del fornitore di servizi cloud e i paesi in cui il fornitore di servizi cloud può archiviare i dati dei clienti del servizio cloud (anche temporaneamente).

Opentech richiede una particolare attenzione nell'adozione di servizi cloud; in particolare

1. Si considera necessaria una conoscenza dettagliata delle caratteristiche dei servizi utilizzati, con particolare riferimento ai requisiti di sicurezza, ai livelli di servizio garantiti, agli elementi contrattuali.

2. Si richiede un livello di sicurezza coerente con il livello di rischio del Processo e delle Informazioni presenti.
3. Si applica una revisione periodica ed un monitoraggio dei requisiti garantiti ed applicati dai servizi cloud, con la possibilità di auditare i fornitori e i servizi utilizzati.

8 POLITICA PER L'EROGAZIONE DI SERVIZI SAAS

In considerazione dei seguenti aspetti:

- i requisiti di base di sicurezza delle informazioni applicabili alla progettazione e all'attuazione del servizio cloud;
- rischi da insider autorizzati;
- isolamento clienti multi-tenancy e servizi cloud (compresa la virtualizzazione);
- accesso agli asset dei clienti del servizio cloud da parte del personale del fornitore del servizio cloud;
- procedure di controllo degli accessi, ad es. autenticazione forte per l'accesso amministrativo ai servizi cloud;
- comunicazioni ai clienti del servizio cloud durante la gestione del cambiamento; – sicurezza della virtualizzazione;
- accesso e protezione dei dati dei clienti del servizio cloud;
- gestione del ciclo di vita degli account dei clienti del servizio cloud;
- comunicazione delle violazioni e linee guida per la condivisione delle informazioni a supporto delle indagini e della scientifica.

Opentech ha predisposto un documento di Condizioni Generali per i servizi SaaS attraverso il quale certifica e comunica ai propri clienti i livelli di servizio e le misure applicate per i servizi erogati.