INFORMATION SECURITY POLICY
PUBLIC DOMAIN

Redazione	Responsabile SGSI
Convalida	Comitato SGSI
Approvazione	Direzione Generale
Data emissione	30/11/2021

Indice

1. SCOPO E CAMPO DI APPLICAZIONE 3
2. RUOLI E RESPONSABILITÀ PER LA SICUREZZA INFORMAZIONI 3
3. SICUREZZA NEI COMPORTAMENTI DEL PERSONALE 3
4. GESTIONE E PROTEZIONE DEGLI ASSET 4
5. SICUREZZA FISICA 4
6. CONTROLLO ACCESSI LOGICI 4
7. GESTIONE DEI SISTEMI ICT 5
8. SVILUPPO E MANUTENZIONE SOFTWARE 5
9. GESTIONE DEGLI INCIDENTI DI SICUREZZA 6
10. GESTIONE DELLA BUSINESS CONTINUITY 6
11. GESTIONE DEI FORNITORI 7
12. COMPLIANCE E AUDIT 7

1. SCOPO E CAMPO DI APPLICAZIONE

Lo scopo del presente documento è quello di comunicare agli Stakeholders di Corvallis S.r.l. (nel seguito CORVALLIS), i principi generali, le linee guida e le responsabilità relative alla sicurezza delle informazioni in CORVALLIS, in coerenza con i requisiti della Norma ISO/IEC 27001:2013 e con la Information Security Policy aziendale.

2. RUOLI E RESPONSABILITÀ PER LA SICUREZZA INFORMAZIONI

La Direzione Generale di CORVALLIS ha individuato per la gestione del SGSI (Sistema Gestione Sicurezza Informazioni) i seguenti principali ruoli: Comitato SGSI, Responsabile SGSI, Risk Owner SGSI, Compliance Manager nonché IT Risk Manager. I compiti e le responsabilità delle suddette figure, sono riportati nell'ambito della documentazione del SGSI. Al riguardo si sottolinea che il "Comitato SGSI", anche a tutela degli Stakeholders, convalida l'integrità dei processi e della documentazione del SGSI, i risultati degli audit e delle valutazioni periodiche dei rischi, i piani di formazione relativi alla sicurezza delle informazioni.

CORVALLIS applica il principio della "separazione dei compiti" (segregation of duties), ove appropriato, per ridurre il rischio di negligenze o di un uso improprio dei sistemi. Tale principio è attuato tenendo conto delle specificità della situazione aziendale, in modo da ridurre le possibilità per una persona di effettuare modifiche non autorizzate o di utilizzare irregolarmente dati e/o servizi aziendali.

3. SICUREZZA NEI COMPORTAMENTI DEL PERSONALE

Tutti i dipendenti, nonché i collaboratori e le terze parti, sono responsabili della tutela delle informazioni di CORVALLIS e della strumentazione informatica della Società ad essi affidata. I dipendenti, i collaboratori e le terze parti devono applicare le policies, le regole e le procedure aziendali in tema di sicurezza delle informazioni, per quanto di rispettiva competenza. CORVALLIS assicura l'opportuna formazione dei dipendenti per garantire l'acquisizione delle necessarie competenze per mantenere la sicurezza del patrimonio aziendale (beni e informazioni) nell'esercizio delle mansioni ad essi affidate. La violazione delle regole aziendali in materia di sicurezza delle informazioni può comportare azioni disciplinari in carico al dipendente che le ha commesse. In fase di cessazione del rapporto di lavoro, ai dipendenti, collaboratori, terze parti che cessano la loro attività in CORVALLIS, sono revocati prontamente tutti gli accessi logici ai dispositivi in dotazione, ai server, ai software applicativi e sono tenuti alla restituzione dei dispositivi in dotazione. Tutti i soggetti che entrano in possesso di dati ed informazioni di CORVALLIS e del suo business sono tenuti a mantenere la massima riservatezza, come richiesto dalle policies, regole e procedure aziendali. L'utilizzo dei dispositivi informatici in dotazione ai dipendenti, ai collaboratori ed il trattamento dei dati e delle informazioni in essi contenuti, è inteso per soli scopi lavorativi. Ai fini della sicurezza delle informazioni aziendali, tutti i dipendenti e collaboratori di CORVALLIS adottano una modalità di "scrivania sgombra" (la cosiddetta "clean desk"), per ridurre il rischio di accessi non autorizzati. CORVALLIS può applicare il teleworking/smart working per lo svolgimento dell'attività lavorativa da remoto. In tali casi gli accessi da ubicazioni differenti dalle sedi aziendali sono protetti tramite connessione sicura (VPN), e avvengono nel rispetto dei requisiti di autenticazione di accesso e di protezione delle informazioni gestite, indicate nel "*Manuale di Sicurezza e Protezione dei Dati*" di CORVALLIS.

4. GESTIONE E PROTEZIONE DEGLI ASSET

Al fine di garantire il livello adeguato di protezione delle informazioni, gli asset CORVALLIS sono inventariati con l'indicazione di specifiche informazioni a seconda della tipologia di asset.

Classificazione delle informazioni

CORVALLIS adotta la classificazione delle informazioni, soprattutto dei documenti sia elettronici che cartacei, presenti in Azienda in base alla loro criticità. Il trattamento di tali informazioni deve avvenire in coerenza con le modalità definite per ciascuno nell'ambito del SGSI. I livelli di classificazione adottati in CORVALLIS sono: *Riservato*, *Confidenziale*, *Interno*, *Pubblico*. I documenti presenti in Azienda, ma non prodotti internamente, devono essere comunque classificati. Il livello di classificazione previsto per informazioni riferibili a Clienti e Fornitori è "confidenziale".

Supporti di memorizzazione e dispositivi mobili

È definito un processo per la gestione, l'assegnazione, la sostituzione e la distruzione dei desktop, dei notebook, dei dispositivi di memorizzazione removibili, degli smartphone e di ogni dispositivo che possa contenere dati al fine di evitare l'uso improprio degli stessi e l'eventuale divulgazione non autorizzata di informazioni. I dispositivi sono custoditi dagli assegnatari con la massima diligenza per evitare la perdita di informazioni.

Trasferimento e condivisione di informazioni con Aziende terze

CORVALLIS ha definito le regole per la condivisione con Aziende terze di documenti contenenti informazioni aziendali. Tali regole tengono in considerazione la criticità delle informazioni di business oggetto di condivisione. Tutti i documenti condivisi con Aziende terze devono essere classificati, a seconda dei casi, *Riservato* o *Confidenziale*, indicando il nome dell'Azienda con la quale è condivisa la documentazione in oggetto e le disposizioni di protezione messe in campo secondo le indicazioni riportate nel SGSI.

5. SICUREZZA FISICA

Sono individuate ed applicate specifiche ed adeguate misure per garantire la sicurezza fisica, tra cui il controllo fisico degli accessi, sistemi antintrusione e videosorveglianza, sistemi antincendio, e infrastrutture di supporto (UPS, generatori di corrente) per la continuità elettrica. L'individuazione delle misure da applicare è basata sulla valutazione della criticità delle risorse da proteggere. È assicurata la corretta e periodica manutenzione degli impianti per garantire il loro funzionamento ottimale ed il rispetto delle prescrizioni di legge.

6. CONTROLLO ACCESSI LOGICI

Sono applicate procedure per controllare la distribuzione dei diritti di accesso ai dispositivi, ai server, ai software e per la gestione degli account utente, in tutte le fasi: dalla creazione dell'account utente, alla sua modifica, aggiornamento, eliminazione. I diritti di accesso sono definiti in base al ruolo ed alle mansioni svolte dall'utente ed in base alle effettive necessità lavorative (criterio del "need to know"), nel rispetto del Provvedimento del Garante della Privacy sugli Amministratori di Sistema. La metodologia utilizzata da CORVALLIS per l'autenticazione di ciascun utente è commisurata alla criticità dei dati contenuti nei sistemi, in base a cui deve essere valutata l'opportunità di utilizzo di metodi di autenticazione più vincolanti (strong authentication). Di norma viene utilizzata la combinazione di user-id

e password. Come criterio generale deve essere garantita la robustezza delle password mediante il rispetto di criteri di complessità e la sua scadenza periodica.

7. GESTIONE DEI SISTEMI ICT

Al fine di garantire la gestione in sicurezza di tutti i sistemi e infrastrutture ICT aziendali, sono adeguatamente documentate le procedure operative e sono chiaramente definite le responsabilità, secondo quanto previsto nel SGSI, relative a installazione del software nei server e nei desktop/notebook, pianificazione e adeguamento della capacità delle risorse ICT, gestione delle vulnerabilità tecniche e relative patch, backup dei sistemi, raccolta e protezione dei log, gestione delle comunicazioni elettroniche e cartacee, trasmissione dei dati, crittografia, etc.

8. SVILUPPO E MANUTENZIONE SOFTWARE

I processi di sviluppo e manutenzione del software applicativo sono opportunamente regolamentati, documentati e gestiti, al fine di garantire che il software rispetti i requisiti di qualità e sicurezza necessari.

Change Management applicativo

Le modalità e le responsabilità di gestione delle attività che riguardano lo sviluppo e la manutenzione del software, sono descritte in specifiche procedure aziendali secondo le diverse fasi della metodologia SDLC (System Development Life Cycle), dalla definizione dei requisiti funzionali e di sicurezza delle applicazioni, alla progettazione, sviluppo e test del software, al rilascio in produzione e al change management delle applicazioni, nel rispetto del principio di "separazione dei compiti e delle responsabilità".

Nel caso di servizi di sviluppo/manutenzione software affidati a terzi, sono utilizzate le stesse modalità di gestione dello sviluppo/manutenzione ed applicati requisiti di sicurezza del software analogamente a quanto fatto per gli sviluppi interni; sono, inoltre, definiti i criteri di accettazione del software.

Requisiti di sicurezza

I requisiti relativi allo sviluppo software e alle modifiche ai sistemi sono definiti già nelle fasi iniziali dei progetti e documentati, secondo quanto definito nel SGSI.

Gestione della configurazione

È gestita la conservazione ed il "versioning" del software per tenere traccia del livello di aggiornamento dei sistemi e delle applicazioni. Le precedenti versioni del software sono conservate come misura preventiva in caso di malfunzionamento della nuova versione.

Protezione del codice sorgente e degli ambienti di sviluppo.

Il codice sorgente dei programmi è conservato e protetto da accessi non autorizzati e perdite accidentali. L'accesso al codice sorgente e agli ambienti di sviluppo è limitato alle sole persone incaricate delle modifiche alle applicazioni, secondo il principio del "need to know".

Dati di test

I dati di test sono protetti qualora essi siano copie complete o parziali dei dati di produzione o nel caso di dati critici relativi al business e a trattamenti di dati personali. Per tale ragione l'accesso agli ambienti di sviluppo è controllato e limitato, in particolare se essi sono accessibili da terze parti.

Change Management infrastrutturali

Sono definite le modalità e le responsabilità di gestione dei progetti infrastrutturali, ovvero le attività progettuali che rispondono alle specifiche esigenze aziendali di implementazione di nuove infrastrutture IT o di modifica significativa delle infrastrutture esistenti.

Al fine di garantire che la sicurezza delle informazioni e la protezione dei dati personali sia parte integrante dei progetti IT, sono raccolti, già in fase di progettazione, anche i requisiti di sicurezza dell'infrastruttura da realizzare o modificare, valutati i rischi di sicurezza del progetto e individuate le contromisure adeguate a ridurre i rischi evidenziati.

9. Gestione degli Incidenti di Sicurezza

Gli incidenti sono gestiti tempestivamente e appropriatamente, al fine di minimizzare danni ulteriori e di ripristinare al più presto e in modo ottimale le normali condizioni operative. In particolare, sono individuati gli incidenti di sicurezza che possono mettere a repentaglio la riservatezza, l'integrità e la disponibilità delle informazioni. Per questo è definito, documentato ed adottato un processo aziendale per la gestione degli incidenti che prevede la classificazione degli incidenti in base alla loro priorità, la loro registrazione, opportune modalità di gestione in relazione alla classificazione, l'individuazione dei responsabili della risoluzione, l'analisi delle problematiche segnalate, l'uso di uno strumento per la tracciatura degli incidenti, la predisposizione di opportuna reportistica, il riesame periodico degli incidenti principali. Tutti i dipendenti, i collaboratori e le terze parti sono tenuti a segnalare gli incidenti relativi alla sicurezza delle informazioni di CORVALLIS tramite i canali e gli strumenti adottati in Azienda. Qualora l'incidente riguardi i dati personali degli interessati di cui CORVALLIS è Titolare del Trattamento oppure Responsabile esterno del Trattamento, viene attivato, ove necessario, rispettivamente il processo di notifica di violazione dati personali al Garante Privacy oppure la comunicazione al Cliente Titolare dei dati coinvolti nella violazione.

10. Gestione della Business Continuity

CORVALLIS adotta strategie e piani per la continuità operativa dei servizi erogati e della sicurezza delle informazioni che tengano conto dei servizi aziendali valutati critici per il business, dei requisiti minimi di ripristino, dei principali scenari di incidenti derivati dalle best practices internazionali, degli impatti dei suddetti scenari sull'Azienda e dei conseguenti livelli di rischio.

Gli scenari di rischio considerati nel Business Continuity Plan (BCP) sviluppato da CORVALLIS sono i seguenti:

- indisponibilità dei servizi/sistemi IT (erogati da Corvallis e fornitori);
- indisponibilità della sede di lavoro;
- indisponibilità di personale essenziale;
- perdita di informazioni, dati cartacei, dotazioni specifiche;
- interruzione di forniture/servizi di terzi.

È costituito in CORVALLIS un Comitato di gestione della crisi di continuità operativa (di seguito, Comitato BCP) e un Team di Recovery che viene attivato dal Comitato BCP nei casi di crisi in cui è necessario attivare operativamente il BCP. Il Comitato BCP ha prevalentemente compiti di organizzazione, coordinamento e

comunicazione, mentre il Team di Recovery ha prevalentemente compiti di operatività tecnica nel periodo di crisi.

Il Recovery Team Leader assicura il coordinamento nella gestione della crisi di continuità operativa e la supervisione delle attività del Team di Recovery di CORVALLIS e del supporto operativo ai Fornitori IT per le attività necessarie per il ripristino dei servizi/sistemi IT nel sito di recovery e, successivamente, per il ritorno al sito primario. Inoltre, assicura il mantenimento del BCP ed il corretto svolgimento dei test periodici, informando la Direzione sui risultati conseguiti. È compito del Recovery Team Leader, in collaborazione con le Funzioni coinvolte, mantenere aggiornato l'elenco dei servizi critici e dei relativi obiettivi di ripristino.

11. GESTIONE DEI FORNITORI

Il livello di sicurezza garantito dalle terze parti (fornitori, outsourcers, partners, etc.) deve essere conforme al livello di sicurezza applicato da CORVALLIS, per evitare che i prodotti/servizi acquisiti dall'esterno costituiscano un elemento di debolezza per la sicurezza delle informazioni.

A tale scopo viene fatta preventivamente una valutazione dei rischi delle terze parti e, quindi, sono definite e inserite nel contratto le responsabilità, le condizioni specifiche, i requisiti di sicurezza e gli SLA (coerenti con le valutazioni di rischio) che le terze parti sono tenute a rispettare.

Le terze parti sono tenute a garantire, in particolare, il rispetto delle policy e procedure di CORVALLIS relative alla sicurezza delle informazioni e alla privacy, l'ottemperanza alla normativa relativa alla proprietà intellettuale, la segnalazione tempestiva di eventuali incidenti che riguardano trattamenti di dati personali o interruzioni di servizi critici che possano pregiudicare la continuità operativa di CORVALLIS. La terza parte deve garantire anche il rispetto delle condizioni pattuite (ad esempio, reportistica, definizione KPI, monitoraggio degli indicatori, etc.) e dei tempi di consegna della documentazione di reporting, e che siano da loro applicate analoghe misure di sicurezza delle informazioni verso i sub-fornitori, in modo da garantire che gli standard di sicurezza richiesti da CORVALLIS siano applicati da tutte le parti coinvolte nella catena di fornitura.

12. COMPLIANCE E AUDIT

CORVALLIS opera nel rispetto delle leggi nazionali e internazionali applicabili ai settori di mercato per i quali opera, dei regolamenti interni, delle normative volontarie adottate (ad esempio, ISO 9001, ISO 27001, etc.), dei contratti con le controparti esterne. Inoltre, CORVALLIS garantisce l'adeguata disponibilità di documentazione e di risorse per consentire le eventuali attività degli Auditor interni ed esterni (Enti certificatori).

<u>Compliance con requisiti legali e contrattuali</u>

I principali riferimenti normativi cogenti corrispondono a:

- Regolamento Europeo n. 2016/679 in materia di protezione dei dati personali (GDPR);
- D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e ss.mm.ii., per le parti ancora in vigore;
- D.Lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio";
- D.Lgs. 81/2008 "Testo Unico sulla Sicurezza sul Lavoro" e ss.mm.ii.;

- D.Lgs. 231/2001 “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica” e ss.mm.ii;
- Legge sulla Proprietà Intellettuale.

Verifiche della sicurezza delle informazioni

CORVALLIS pianifica controlli periodici indipendenti (audit) per verificare il rispetto ed il corretto recepimento della presente policy e delle procedure del SGSI.