Politica del Sistema di Gestione per la Sicurezza delle Informazioni

File	IMS.ORG.Politica Sicurezza Informazioni.000.docx
Name	Politica per la Sicurezza delle Informazioni
Ver	000
Date	02/07/2025
Written by	IMS / valerio.passerini
Controlled by	BD / marco.canepa

Indice

1. Tabella Revisioni

Rev	Data	Written by	Controlled by	Description
000	02/07/2025	IMS/ valerio.passerini	BD/ marco.canepa	Prima emissione (include versione Web, coerente con la politica estesa, senza riferimenti troppo operativi o sensibili, sintetica e leggibile dalle parti interessate

2. Politica per la Sicurezza delle Informazioni
(in conformità alla norma ISO/IEC 27001:2022)

1. Finalità e impegno della Direzione

La Direzione di Blue Star Software S.r.l. (detta anche BSS) riconosce che la sicurezza delle informazioni costituisce un fattore strategico e abilitante per il perseguimento degli obiettivi aziendali e per la tutela del proprio patrimonio informativo, dei clienti e delle parti interessate assicurando costantemente i tre requisiti fondamentali:

- Riservatezza: le informazioni sono accessibili solo a chi è debitamente autorizzato.
- Integrità: la completezza e l'accuratezza delle informazioni e dei metodi di elaborazione sono salvaguardate.
- Disponibilità: gli utenti autorizzati hanno accesso alle informazioni e agli asset associati quando richiesto.

Con la presente Politica, Blue Star Software S.r.l. definisce i principi, gli obiettivi e gli impegni per l'implementazione, il mantenimento e il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), in conformità alla norma ISO/IEC 27001:2022.

2. Campo di applicazione del SGSI e Asset

Il SGSI si applica ai processi, alle risorse e agli asset coinvolti nello sviluppo software e nella gestione dei Data Center, inclusi i servizi erogati, le infrastrutture, i sistemi informativi e le informazioni trattate da BSS, sia internamente sia presso fornitori qualificati.

3. Asset e risorse da proteggere

BSS si impegna a proteggere tutte le risorse direttamente e indirettamente impattate dai propri processi aziendali e censite nell'Asset Inventory aziendale vigente, classificati nelle seguenti macro-categorie:

Le principali categorie di asset includono:

- Patrimonio Informativo: dati, documenti tecnici e informazioni di business
- Asset Logici: codice sorgente, software applicativo, licenze e database
- Asset Fisici: Hardware, apparati dell'infrastruttura di rete e strutture Data Center
- Risorse Umane: competenze e know-how specialistico
- Servizi erogati: continuità operativa e livelli di servizio (SLA) contrattualizzati
- Facilities e servizi di terze parti e relativi livelli di servizio (SLA) contrattualizzati.

Ogni asset rilevante è associato a un responsabile formalmente individuato.

4. Analisi e gestione del rischio

In conformità alla ISO/IEC 27001:2022, BSS conduce con cadenza almeno annuale l'analisi dei rischi per la sicurezza delle informazioni per identificare le minacce e le vulnerabilità che insistono sugli asset, considerando:

- gli obiettivi strategici aziendali;
- gli incidenti di sicurezza occorsi;
- le evoluzioni del contesto organizzativo, tecnologico e normativo;
- i cambiamenti nei processi di sviluppo software e di gestione del Data Center.

I rischi identificati sono valutati, trattati e monitorati secondo criteri di accettabilità documentati, e sono pianificati i controlli necessari per mitigarli.

5. Classificazione delle informazioni

Le informazioni sono classificate in base al loro livello di criticità e al potenziale impatto su riservatezza, integrità e disponibilità.

Attualmente la classificazione prevede almeno le seguenti categorie:

- Pubbliche
- Riservate

La classificazione guida l'adozione di misure di protezione coerenti e proporzionate.

6. Sicurezza nella progettazione e nello sviluppo software

In linea con il core business aziendale, BSS integra la sicurezza nei processi di progettazione e in ogni fase del ciclo di vita dello sviluppo (SDLC) adottando controlli e strumenti definiti nel SGSI per garantire:

- integrità del codice e delle soluzioni;
- riservatezza delle informazioni trattate;
- disponibilità dei sistemi e dei servizi.

7. Protezione dei dati personali

Si applicano i principi di:

- Privacy by Design e by Default: protezione dei dati integrata sin dalla concezione del software.
- Minimizzazione dei dati: trattamento dei soli dati strettamente necessari alle finalità previste.
- Sicurezza del codice: adozione di standard e strumenti atti a prevenire vulnerabilità logiche e sistemistiche.

Sono adottate misure tecniche e organizzative adeguate (es. pseudonimizzazione), tenendo conto dello stato dell'arte, dei costi di attuazione e dei rischi per i diritti e le libertà delle persone fisiche.

8. Gestione del Data Center e Controllo degli accessi

L'accesso logico e fisico, alle informazioni, ai beni e alle risorse aziendali, è consentito esclusivamente secondo i seguenti principi:

- principio del minimo privilegio;
- principio della necessità di conoscenza, in funzione delle attività assegnate necessarie per le proprie mansioni.

L'Accesso fisico ai locali e al Data Center: è consentito esclusivamente al personale autorizzato.

Eventuali visitatori, fornitori o clienti possono accedere solo se accompagnati da personale autorizzato di BSS ed esclusivamente sotto la sua supervisione continua.

È severamente vietata la cessione di credenziali / badge di accesso.

9. Continuità operativa

BSS ha definito un Piano di Continuità Operativa per garantire il ripristino dei servizi e/o dei processi critici in tempi compatibili con le esigenze di business, con l'obiettivo comunque di minimizzare i tempi di inattività.

È prevista la conduzione di una rigorosa Business Impact Analysis (BIA) per determinare priorità, tempi e costi di ripristino dei servizi critici in caso di evento / disastro.

10. Cultura della sicurezza, Consapevolezza e formazione

La Direzione assicura che tutto il personale, i collaboratori e le parti interessate coinvolte nell'erogazione dei servizi:

- siano consapevoli delle responsabilità in materia di sicurezza delle informazioni;
- adottino comportamenti coerenti con la presente Politica ed il Codice di comportamento.

BSS garantisce programmi di formazione, informazione e addestramento periodici, adeguati al ruolo e alle responsabilità assegnate.

11. Rapporti con parti terze

La sicurezza delle informazioni è un criterio mandatorio nella selezione e gestione dei fornitori / partner, regolati in modo coerente ai requisiti del SGSI, attraverso accordi di riservatezza (NDA) e clausole di sicurezza specifiche, periodicamente riesaminate in funzione della valutazione dei rischi.

12. Conformità Legale e contrattuale

BSS opera nel pieno rispetto del quadro normativo vigente, con particolare riferimento al Regolamento UE 2016/679 (GDPR) ed al D.Lgs. 101/2018 per la protezione dei dati, alle normative sulla proprietà intellettuale.

Il SGSI è progettato per garantire il rispetto degli obblighi contrattuali assunti e provvedimenti delle Autorità competenti verso dipendenti (in accordo al CCNL), Clienti e Terze Parti.

13. Protezione delle informazioni

Le informazioni e gli asset sono protetti da perdita, distruzione, alterazione, accesso o divulgazione non autorizzata mediante misure tecniche e organizzative adeguate e proporzionate al loro valore e ai rischi identificati.

Le registrazioni rilevanti sono conservate e protette in conformità ai requisiti legali, normativi e di business.

14. Miglioramento continuo e sanzioni disciplinari

BSS conduce audit interni con cadenza almeno annuale ed un piano di monitoraggio basato su indicatori di prestazione (KPI) per verificare l'efficacia e l'adeguatezza del SGSI.

I risultati sono documentati e periodicamente riesaminati dal Responsabile del SGSI e dalla Direzione.

La presente Politica è soggetta a Riesame della Direzione con cadenza almeno annuale o in occasione di cambiamenti significativi nel contesto organizzativo, tecnologico o normativo.

Violazioni: la mancata osservanza dei principi enunciati nella presente Politica e nelle procedure correlate è considerata una violazione contrattuale e/o disciplinare; BSS perseguirà in modo proporzionato alla gravità dell'evento applicando sanzioni nel rispetto delle normative vigenti e del CCNL.

15. Gestione dei costi

La Direzione valuta i costi delle misure di sicurezza in rapporto ai rischi da mitigare, assicurando un equilibrio tra protezione delle informazioni e sostenibilità economica.

Politica per la Sicurezza delle Informazioni

(in conformità alla norma ISO/IEC 27001:2022 – versione Web)

Blue Star Software Srl (detta anche BSS) adotta un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme alla norma UNI CEI ISO/IEC 27001:2022, con l'obiettivo di garantire la protezione delle informazioni e degli asset aziendali a supporto delle attività di sviluppo software e gestione del Data Center.

Impegno della Direzione

La Direzione di Blue Star Software Srl si impegna a:

- proteggere la riservatezza, integrità e disponibilità delle informazioni;
- tutelare i dati dei clienti, delle parti interessate e dell'azienda;
- assicurare la continuità dei servizi e la resilienza operativa;
- rispettare i requisiti legali, normativi e contrattuali applicabili.

Ambito di applicazione

La Politica si applica:

- a tutti i processi aziendali inclusi nel campo di applicazione dello scopo del SGSI;
- al personale dipendente;
- ai collaboratori, consulenti, fornitori e partner;
- a tutte le parti terze che trattano informazioni o utilizzano asset di BSS

Asset e informazioni protette

BSS protegge tutte le informazioni e gli asset rilevanti, tra cui:

- dati, documenti e informazioni;
- infrastrutture fisiche e Data Center;
- sistemi informativi e software;
- servizi e prodotti di sviluppo software;
- competenze e risorse umane.

Gestione del rischio

L'azienda effettua periodicamente un'analisi dei rischi per identificare, valutare e trattare le minacce alla sicurezza delle informazioni, tenendo conto dell'evoluzione tecnologica, del contesto operativo e degli obiettivi di business.

Controllo degli accessi

L'accesso alle informazioni e agli asset è consentito esclusivamente a personale autorizzato, secondo i principi di necessità di conoscenza e minimo privilegio. Gli accessi fisici e logici sono monitorati e controllati.

Sicurezza nello sviluppo software

La sicurezza delle informazioni è integrata nel processo di progettazione e sviluppo software, al fine di garantire soluzioni affidabili, sicure e conformi ai requisiti di qualità e protezione dei dati.

Protezione dei dati personali

BSS tratta i dati personali nel rispetto del Regolamento UE 679/2016 (GDPR), applicando i principi di privacy by design e privacy by default, assicurando trasparenza, minimizzazione e adeguate misure di sicurezza.

Formazione e consapevolezza

L'azienda promuove la consapevolezza e la formazione continua del personale in materia di sicurezza delle informazioni e protezione dei dati.

Parti terze

I rapporti con fornitori e partner sono regolati da accordi contrattuali e clausole di riservatezza che includono specifici requisiti di sicurezza delle informazioni.

Continuità operativa

BSS adotta misure di Business Continuity per garantire il ripristino dei servizi critici e limitare gli impatti derivanti da eventi imprevisti.

Miglioramento continuo

La Politica per la Sicurezza delle Informazioni è oggetto di riesame periodico ed è parte integrante del processo di miglioramento continuo del SGSI.