calzavara

SMART SOLUTIONS BEYOND INFRASTRUCTURE

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI		POL SGSI-001	
REV	**01**	**DATA**	21/08/2025

REDAZIONE **SGSI**	**CONTROLLO** **IT**	**APPROVAZIONE** Direzione generale
R.SGSI	IT Manager	CEO

CLASSIFICAZIONE		
☒ **PUBBLICO**	☐ **INTERNO**	☐ **RISERVATO**

	LISTA DI DISTRIBUZIONE
Nome	**Ruolo**
Le persone con accesso al documento sono descritte nella cartella SharePoint che lo contiene	
Responsabili di funzione	Tutti i Dirigenti e i Responsabili di Funzione sono tenuti a rispettare la presente procedura, e a farla rispettare dai propri Collaboratori

STORICO REVISIONI

VERSIONE	DATA	AUTORE	SOMMARIO CAMBIAMENTI
00	30/09/2024	R.SGSI	Prima stesura
01	21/08/2025	R.SGSI	Revisione per integrazione di Stas srl

Sommario

1. Introduzione

Calzavara opera sui mercati nazionali ed internazionali nel settore delle infrastrutture per le telecomunicazioni. Specializzata nella produzione di strutture per telecomunicazioni. I clienti sono principalmente tower company, mobile network operators e grandi aziende.

Calzavara (con la sua BU Beeup) e la controllata Stas si occupano di soluzioni ingegneristiche per la sicurezza, come la videosorveglianza, controllo accessi, rilevazione incendi ecc. I clienti sono prevalentemente enti pubblici, ma anche privati, stadi, aeroporti e altre infrastrutture critiche.

Calzavara inoltre progetta e produce impianti di segnalazione ostacolo al volo. I clienti appartengono ai diversi settori industriali tra i quali Oil & Gas, Building & Construction, Telecomunication e Brodcasting, distribuzione di Energia, eliporti ed aviosuperfici.

Data la natura delle proprie attività, Calzavara e Stas, considerano la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo e di quello dei propri clienti ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.

Entrambe le aziende pongono particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione e sviluppo e manutenzione dei propri servizi e prodotti, che devono essere ritenuti un bene primario dell'azienda.

Consapevoli del fatto che i progetti realizzati per i clienti possono comportare l'affidamento di dati e informazioni critiche, le organizzazioni operano secondo normative di sicurezza internazionalmente riconosciute.

Per questo motivo Calzavara e Stas intendono adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza e la disponibilità sia del patrimonio informativo interno che di quello a lei affidato dai propri Clienti.

Su tali basi Calzavara e Stas hanno deciso di implementare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità alle indicazioni della norma internazionale ISO/IEC 27001:2022.

2. Obiettivi

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di Calzavara e Stas è di garantire un adeguato livello di sicurezza dei dati e delle informazioni, attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il Sistema di Gestione per la Sicurezza per le Informazioni di Calzavara e Stas definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

- RISERVATEZZA: l'informazione deve essere nota solo a chi dispone di opportuni privilegi;
- INTEGRITÀ: l'informazione deve essere modificabile solo ed esclusivamente da chi ne possiede i privilegi;

- DISPONIBILITÀ: l'informazione deve essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che dispongono dei relativi privilegi.

Inoltre, con la presente politica Calzavara e Stas intendono formalizzare i seguenti obiettivi strategici nell'ambito della sicurezza delle informazioni:

- preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità;
- rispondere pienamente alle indicazioni della normativa vigente e cogente;
- mantenere allineate le competenze alle evoluzioni tecnologiche e assicurare la comunicazione degli obiettivi e dei meccanismi di sicurezza a tutte le persone che lavorano per l'organizzazione.

3. Contenuto della politica

Il SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) si applica a:

- **Progettazione, esercizio e manutenzione dei sistemi informatici ad uso degli utenti interni**
- **Progettazione, test di accettazione, integrazione, installazione, esercizio e manutenzione di sistemi hardware e software**
- **Progettazione, test di accettazione, installazione e manutenzione di soluzioni di sicurezza integrata ad uso interno e dei clienti**
- **Gestione della sicurezza delle informazioni legate allo studio, progettazione, consulenza, costruzione, installazione, gestione, manutenzione di sistemi, impianti, componenti di infrastrutture nel settore degli impianti tecnologici, elettrici ed elettronici (Stas s.r.l.)**

Tutte le informazioni che vengono create o utilizzate dalle aziende sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile, e debbono essere prontamente disponibili per gli usi consentiti.

Con "utilizzo dell'informazione" si intende qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito di applicazione dell'SGSI, si prevede, in conformità alla norma ISO/IEC 27001:2022, che il Responsabile per la Sicurezza delle Informazioni svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi durante tale periodo e dei cambiamenti strategici, di business e tecnologici avvenuti; l'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate.

La Direzione condivide con il Responsabile della Sicurezza delle Informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella redazione della metodologia la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio.

In seguito dell'elaborazione dell'analisi dei rischi da parte del Responsabile per la Sicurezza delle Informazioni ed in base alla metodologia condivisa con la Direzione, la Direzione stessa valuta i risultati ottenuti accogliendo la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere che saranno classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti.

Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

4. Responsabilità

La responsabilità finale della sicurezza delle informazioni ricade sulla Direzione che a sua volta ha delegato i responsabili della divisione IT e dei responsabili di funzione coinvolti nel perimetro SGSI.

Tutto il personale che, a qualsiasi titolo, collabora con le aziende è responsabile dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

Viene istituito un comitato per la sicurezza delle informazioni che si riunirà con cadenza semestrale. Tale comitato è composto, in forma stabile, dalla Direzione e dal Responsabile della Sicurezza delle Informazioni. Vengono coinvolte a livello di comitato le competenze tecniche necessarie per la valutazione di aspetti specifici (es: Responsabile IT, ecc).

Il comitato ha il compito di fissare gli obiettivi, assicurare un indirizzamento chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di sicurezza. Promuove la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza, coerentemente con le politiche e le linee strategiche aziendali definite.

Il responsabile della sicurezza delle informazioni si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni ed in particolare di:

- emanare tutte le norme necessarie ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di Calzavara e Stas;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza per il personale;

- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni

Tutti i soggetti esterni che intrattengono rapporti con Calzavara e Stas devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

5. Applicabilità

La presente politica si applica indistintamente a tutti gli organi delle aziende. L'attuazione della presente politica è obbligatoria per tutto il personale Calzavara e Stas, così come per i collaboratori esterni, e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda. –

Calzavara e Stas consentono la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

6. Riesame – Impegno al miglioramento continuo del SGSI

La direzione Calzavara verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, garantendo l'adeguato supporto ed impegno per il suo continuo miglioramento, e che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

Questa politica è comunicata a tutto il personale attraverso lo strumento aziendale SharePoint on-line ove risiederà il repository accessibile con la documentazione necessaria