POLITICA

SICUREZZA DELLE INFORMAZIONI

ORGANIZZAZIONE Stiip S.r.l.	**CODICE DOCUMENTO** POL-SGSI-01
REVISIONE 1.0	**CLASSIFICAZIONE** Pubblica
APPROVATA IL 03/10/2026	**ULTIMO RIESAME** 2/10/2026
APPROVAZIONE Organi di amministrazione e direttivi *Simone Lo Iacono* Firma elettronica 03/10/2026 alle 00:07 SHA-256 5d379dd80352... **FIRMA**	

INDICE

1. SCOPO E APPROCCIO	1
2. AMBITO DI APPLICAZIONE	1
3. CONTESTO E REQUISITI APPLICABILI	1
4. IMPEGNI DEGLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI	2
5. OBIETTIVI	3
6. PRINCIPI	3
7. ORGANIZZAZIONE, RUOLI E RESPONSABILITÀ	4
8. POLITICHE SPECIFICHE PER TEMATICA	5
9. ECCEZIONI E DEROGHE	6
10. INFORMAZIONI DOCUMENTATE E CONSERVAZIONE	6
11. MONITORAGGIO DELL'ATTUAZIONE	7
12. COMUNICAZIONE E PRESA D'ATTO	7
13. RIESAME E AGGIORNAMENTO	7
REGISTRO DELLE REVISIONI	9

1. Scopo e approccio

La presente politica definisce l'approccio di Stiip S.r.l. alla gestione della sicurezza delle informazioni e dei sistemi informativi e di rete. È il documento di vertice del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI): stabilisce obiettivi, principi e responsabilità dai quali discendono le politiche specifiche, le procedure, i piani e i controlli. In caso di contrasto con un documento subordinato prevale la presente politica.

Per **sicurezza delle informazioni** si intende la protezione della riservatezza (confidentiality), dell'integrità (integrity) e della disponibilità (availability) delle informazioni e dei sistemi che le trattano, unitamente all'autenticità e alla tracciabilità delle operazioni compiute su di essi, qualunque sia la forma delle informazioni e il supporto sul quale sono conservate, trasmesse o comunicate.

La politica è adeguata alla strategia e agli obiettivi di business della Società e complementare ad essi: Stiip progetta e gestisce sistemi informativi per conto di terzi, e la sicurezza delle proprie informazioni e di quelle dei clienti è parte di ciò che vende.

2. Ambito di applicazione

La politica si applica a tutta l'organizzazione: a ogni sede, a ogni linea di attività e di servizio, a tutto il personale a qualunque titolo operante per la Società e, per le parti pertinenti, ai fornitori e alle altre parti esterne che accedono ai sistemi informativi e di rete o che trattano informazioni per conto della Società. Non sono previste esclusioni.

3. Contesto e requisiti applicabili

La politica tiene conto della strategia e dei requisiti di business della Società, dei requisiti legali, regolamentari e contrattuali applicabili e dei rischi e delle minacce per la sicurezza delle informazioni attuali e prevedibili.

La Società è qualificata come **soggetto importante** ai sensi del decreto legislativo 4 settembre 2024, n. 138, ed è iscritta nell'elenco dei soggetti NIS tenuto dall'Agenzia per la Cybersicurezza Nazionale; in quanto fornitore di servizi gestiti e di servizi di cloud computing è inoltre destinataria diretta del regolamento di esecuzione (UE) 2024/2690. Dove i requisiti applicabili divergono, la Società adotta il più stringente.

Il sistema di gestione adotta come riferimento:

- UNI CEI EN ISO/IEC 27001:2022 e ISO/IEC 27002:2022;
- ISO/IEC 27017:2015 e ISO/IEC 27018:2019, per i servizi cloud e per i dati personali trattati in cloud.

I requisiti legali, regolamentari e contrattuali applicabili alla Società in materia di sicurezza delle informazioni, e le modalità con cui la Società vi dà attuazione, sono identificati, documentati e mantenuti aggiornati nel **registro dei requisiti legali e contrattuali**, tenuto nell'ambito della politica su conformità e audit di sicurezza. Il contesto dell'organizzazione, le parti interessate e i loro requisiti sono determinati e documentati nell'analisi del contesto e nel campo di applicazione del SGSI.

4. Impegni degli organi di amministrazione e direttivi

Gli organi di amministrazione e direttivi approvano la presente politica e assumono i seguenti impegni.

- **Conformità**: soddisfare i requisiti applicabili in materia di sicurezza delle informazioni, di origine legale, regolamentare e contrattuale, e quelli derivanti dalle parti interessate.
- **Miglioramento continuo**: assicurare il miglioramento continuo del SGSI e della sicurezza dei sistemi informativi e di rete.

- **Risorse**: fornire le risorse adeguate all'attuazione della politica, ivi compresi personale, risorse finanziarie, processi, strumenti e tecnologie.
- **Governo**: approvare le modalità di attuazione delle misure di gestione dei rischi, sovrintendere alla loro attuazione e rispondere delle violazioni, ai sensi dell'articolo 23 del decreto legislativo n. 138/2024.

5. Obiettivi

La Società persegue i seguenti obiettivi di sicurezza delle informazioni:

- garantire la disponibilità e la continuità dei servizi erogati ai clienti;
- proteggere la riservatezza e l'integrità delle informazioni proprie e dei clienti;
- prevenire, rilevare tempestivamente e gestire gli incidenti, riducendone impatto e tempi di ripristino;
- assicurare la conformità agli obblighi applicabili, compresi quelli di notifica;
- mantenere la consapevolezza e la competenza del personale;
- governare il rischio della catena di approvvigionamento.

Gli obiettivi sono declinati in traguardi misurabili, assegnati a ruoli responsabili e riesaminati secondo il capitolo 13.

6. Principi

Ogni attività relativa alla sicurezza delle informazioni è guidata dai principi seguenti.

- **Approccio basato sul rischio**: l'intensità delle misure è proporzionata al rischio valutato, alle dimensioni della Società e all'esposizione dei servizi.
- **Necessità di conoscere e minimo privilegio** (need to know, least privilege): l'accesso è concesso nella misura minima necessaria ai compiti assegnati.
- **Separazione dei compiti** (segregation of duties): le funzioni e le aree di responsabilità in conflitto sono separate; dove la dimensione organizzativa non lo consenta si adottano controlli compensativi.

- **Sicurezza fin dalla progettazione** (security by design): i requisiti di sicurezza sono definiti nella progettazione di servizi, sistemi e modifiche, non aggiunti dopo.
- **Difesa in profondità** (defence in depth): la protezione è affidata a più livelli indipendenti di prevenzione, rilevamento e risposta.
- **Documentazione e tracciabilità**: decisioni, deroghe, valutazioni e incidenti sono registrati e conservati.
- **Responsabilità individuale** (accountability): chiunque acceda ai sistemi della Società risponde del rispetto della presente politica e delle politiche specifiche.

7. Organizzazione, ruoli e responsabilità

Gli organi di amministrazione e direttivi hanno la responsabilità ultima della sicurezza delle informazioni: approvano la presente politica e le politiche specifiche, ne sovrintendono l'attuazione e rispondono delle violazioni.

La Società istituisce un'**organizzazione per la sicurezza informatica**: le responsabilità e i poteri in materia di sicurezza delle informazioni sono attribuiti a ruoli definiti, approvati dagli organi di amministrazione e direttivi e resi noti alle articolazioni competenti. Almeno una persona riferisce direttamente agli organi di amministrazione e direttivi sulle questioni di sicurezza delle informazioni. L'organizzazione comprende il punto di contatto con l'Agenzia per la Cybersicurezza Nazionale e il suo sostituto, e il referente CSIRT.

Chiunque acceda ai sistemi informativi e di rete della Società — personale, collaboratori e terzi — è tenuto ad applicare la presente politica, le politiche specifiche e le procedure. Il mancato rispetto è gestito secondo la politica sull'affidabilità delle risorse umane e, per le parti esterne, secondo il contratto.

L'individuazione dei ruoli, la definizione dei rispettivi compiti e poteri, i requisiti di competenza e l'elenco nominativo delle persone incaricate sono stabiliti dalla **politica su ruoli e responsabilità** e dai suoi allegati.

L'organizzazione per la sicurezza informatica e l'assegnazione dei ruoli sono riesaminate almeno ogni anno e comunque al verificarsi di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

8. Politiche specifiche per tematica

La presente politica è attuata dalle politiche specifiche per tematica (topic-specific policies) elencate di seguito. Ciascuna è documentata, approvata dagli organi di amministrazione e direttivi e resa nota alle articolazioni competenti secondo il principio della necessità di conoscere; ciascuna è allineata e complementare alla presente politica e non può derogarvi.

- gestione del rischio;
- ruoli e responsabilità;
- affidabilità delle risorse umane;
- conformità e audit di sicurezza;
- gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
- gestione degli asset;
- gestione delle vulnerabilità;
- continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche;
- gestione dell'autenticazione, delle identità digitali e del controllo accessi;
- sicurezza fisica;
- formazione del personale e consapevolezza;
- sicurezza dei dati;
- sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
- protezione delle reti e delle comunicazioni;
- monitoraggio degli eventi di sicurezza;
- risposta agli incidenti e ripristino;

- crittografia;
- test di sicurezza;
- account privilegiati e account di amministrazione dei sistemi;
- supporti di memorizzazione rimovibili;
- classificazione e trattamento delle informazioni;
- uso accettabile delle risorse e dei dispositivi degli utenti finali.

I primi sedici ambiti attuano la misura GV.PO-01 delle misure di sicurezza di base per i soggetti importanti; i quattro successivi sono richiesti in forma autonoma dal regolamento di esecuzione (UE) 2024/2690; gli ultimi due completano le politiche specifiche raccomandate dal controllo 5.1 della ISO/IEC 27002.

Lo sviluppo, il riesame e l'approvazione di ciascuna politica specifica sono assegnati a personale dotato di adeguato livello di autorità e di competenza tecnica; l'approvazione compete in ogni caso agli organi di amministrazione e direttivi.

9. Eccezioni e deroghe

Ogni scostamento dalla presente politica o dalle politiche specifiche costituisce deroga e deve essere autorizzato preventivamente, motivato, limitato nel tempo e registrato. Le deroghe che impediscono l'attuazione di un requisito di legge sono approvate dagli organi di amministrazione e direttivi. Ogni deroga confluisce nel piano di trattamento dei rischi con le misure compensative adottate e il rischio residuo accettato, ed è riesaminata alla scadenza.

10. Informazioni documentate e conservazione

Le informazioni documentate del SGSI sono create, approvate, distribuite, controllate nelle versioni, protette, conservate e dismesse secondo la procedura per la gestione delle informazioni documentate. Sono conservate almeno le classi seguenti, per i periodi indicati:

- **politiche** — la presente politica e le politiche specifiche: 10 anni dalla sostituzione;
- **piani** — gestione e trattamento dei rischi, vulnerabilità, continuità, ripristino, crisi, formazione, adeguamento, obiettivi: 10 anni dalla sostituzione;
- **procedure e istruzioni operative** — i documenti che attuano le politiche specifiche: 10 anni dalla sostituzione;
- **registri e inventari** — sistemi rilevanti, asset, fornitori, personale con ruoli di sicurezza, formazione, deroghe: versione corrente e 3 anni;
- **evidenze e registrazioni** — incidenti e notifiche, verbali di riesame, esiti di audit: 10 anni; per i log, il termine fissato dalla politica sul monitoraggio degli eventi di sicurezza.

L'elenco puntuale dei documenti in vigore, con proprietario, versione e stato, è mantenuto nel registro delle informazioni documentate.

11. Monitoraggio dell'attuazione

L'attuazione della presente politica e il livello di maturità della sicurezza dei sistemi informativi e di rete sono monitorati mediante indicatori e misure relativi almeno alla copertura della formazione, agli esiti delle valutazioni dei rischi, ai tempi di rilevazione e di risposta agli incidenti, all'avanzamento del piano di adeguamento e agli esiti degli audit. Gli indicatori, le soglie e la periodicità della rilevazione sono definiti dalla politica su conformità e audit di sicurezza; gli esiti sono portati al riesame di cui al capitolo 13.

12. Comunicazione e presa d'atto

La politica è comunicata a tutto il personale e, per quanto pertinente, alle parti interessate esterne, con modalità adeguate, accessibili e comprensibili per i destinatari. Il personale ne prende atto formalmente, con riscontro registrato; le parti esterne rilevanti ne prendono atto attraverso i contratti o documenti equivalenti. La politica è resa disponibile come informazione documentata alle parti interessate che ne hanno titolo;

nella distribuzione all'esterno si evita di divulgare informazioni riservate. La formazione e la consapevolezza sono disciplinate dalla politica specifica in materia.

13. Riesame e aggiornamento

La presente politica e le politiche specifiche sono riesaminate dagli organi di amministrazione e direttivi **almeno una volta all'anno** e comunque al verificarsi di evoluzioni del contesto normativo, incidenti significativi, variazioni organizzative o cambiamenti significativi delle operazioni, mutamenti dell'esposizione alle minacce e ai relativi rischi, evoluzioni della strategia aziendale o dell'ambiente tecnologico, o di lezioni apprese da eventi e incidenti.

Il riesame tiene conto degli esiti dei riesami di direzione e degli audit e verifica la conformità delle politiche alla normativa in materia di sicurezza informatica. Quando una politica è modificata è verificata la coerenza delle politiche correlate. Ogni modifica della presente politica è approvata dagli organi di amministrazione e direttivi.

L'esito di ogni riesame è documentato; per la presente politica è registrato nel registro delle revisioni in calce, anche quando il riesame non comporta modifiche. Sulla base degli esiti è definito, attuato e approvato dagli organi di amministrazione un **piano di adeguamento**, sul cui avanzamento gli organi sono informati periodicamente.

Registro delle revisioni

Il registro documenta ogni emissione e ogni riesame del presente documento, comprese le verifiche periodiche che non hanno comportato modifiche. La data indicata è quella di approvazione da parte degli organi di amministrazione e direttivi.

REVISIONE	DATA	DESCRIZIONE DELLA MODIFICA
1.0	2/10/2026	Prima emissione

Nella stesura di questo documento sono stati impiegati strumenti di intelligenza artificiale. L'impostazione, le scelte di merito e la verifica finale del contenuto restano opera umana: l'intelligenza artificiale ha avuto funzione di supporto alla redazione, non decisionale.