

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 1 di 9	Riservatezza: Pubblico

INFORMATION SECURITY POLICY

<i>Redazione</i>	Responsabile SGSI
<i>Convalida</i>	Comitato SGSI
<i>Approvazione</i>	Direzione Generale

<i>Rev.</i>	<i>Data</i>	<i>Descrizione</i>
01	03/04/2026	Prima emissione

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 2 di 9	Riservatezza: Pubblico

Indice

Sommario

1. SCOPO E CAMPO DI APPLICAZIONE	3
Regolamenti, contratti e legislazioni	4
2. RUOLI E RESPONSABILITÀ PER LA SICUREZZA INFORMAZIONI	4
3. POLITICHE DI GESTIONE DEL RISCHIO	5
4. POLITICHE DI SEPARAZIONE DEI COMPITI	5
5. LINEA GUIDA: SICUREZZA NEI COMPORTAMENTI DEL PERSONALE	5
6. Affermazione dell'impegno per soddisfare i requisiti relativi a ISMS.....	5
7. Contatti con le Autorità e con i gruppi di interesse speciali	5
8. Gestione sicurezza nel project management	6
9. CLASSIFICAZIONE E PROTEZIONE DELLE INFORMAZIONI.....	6
10. LINEA GUIDA: CONTROLLO ACCESSI LOGICI	7
11. LINEA GUIDA: GESTIONE DEI SISTEMI ICT	7
12. LINEA GUIDA: SVILUPPO E MANUTENZIONE SOFTWARE	7
13. LINEA GUIDA: GESTIONE DEGLI INCIDENTI DI SICUREZZA, BC e DR	7
14. LINEA GUIDA: GESTIONE DEGLI INCIDENTI DI SICUREZZA	8
15. LINEA GUIDA: GESTIONE DELLA BUSINESS CONTINUITY	8
16. LINEA GUIDA: GESTIONE DEI FORNITORI	8
17. LINEA GUIDA: COMPLIANCE E AUDIT.....	8
18. PIANO DOCUMENTALE PER COMPLIANCE ISO27001	9
19. COMUNICAZIONE ALLE PARTI INTERESSATE E STAKEHOLDERS.....	9

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 3 di 9	Riservatezza: Pubblico

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento di Policy per la Sicurezza delle Informazioni è stato predisposto nel rispetto dei requisiti della Norma ISO/IEC 27001:2022 e rappresenta il quadro di riferimento dei principi, delle linee guida e delle regole che devono essere adottate per la sicurezza delle informazioni di SIA S.p.A.

I principi, le linee guida e le regole sono di natura generale, sono dedicate ai vari aspetti della sicurezza delle informazioni e sono articolate secondo la struttura suggerita dall'Annex A della Norma ISO 27001 e dagli standard e best practices ad essa correlati.

Finalità specifiche del presente documento sono:

- Definire le politiche generali e assicurare il miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni di SIA S.P.A., inteso come obiettivo fondamentale dei sistemi di gestione che il Management e tutti i dipendenti devono contribuire a raggiungere, attraverso l'effettuazione di una previa analisi del rischio, costantemente monitorata e aggiornata. Nel prosieguo del documento si potrà fare riferimento al sistema indifferentemente con gli acronimi SGSI o ISMS
- Stabilire la normativa generale e i principi base per il corretto trattamento e tutela delle informazioni e dei beni informatici, dell'Azienda e dei Clienti;
- Soddisfare i requisiti di sicurezza richiesti dalle parti interessate e stakeholders, tra cui clienti, fornitori, enti di certificazione.
- Adempiere agli obblighi imposti dalle leggi in tema di sicurezza delle informazioni e rispettare i requisiti normativi, contrattuali e legali;
- Fornire una base comune di linee guida e regole per lo sviluppo e l'attuazione delle procedure operative per la gestione della sicurezza delle informazioni;
- Definire ruoli e responsabilità, generali e specifiche, per tutti gli aspetti legati alla sicurezza delle informazioni e dei beni informatici, dell'Azienda e dei Clienti;
- Assicurare il miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni di SIA S.P.A., inteso come obiettivo fondamentale dei sistemi di gestione che il Management e tutti i dipendenti devono contribuire a raggiungere.
- proteggere le informazioni dall'accesso non autorizzato o dall'uso improprio;
- garantire la riservatezza delle informazioni;
- mantenere l'integrità delle informazioni;
- recepire, implementare, monitorare costantemente e aggiornare i principi fondamentali della cybersecurity (identify, protect, detect, respond e recover);
- mantenere la disponibilità delle informazioni e dei sistemi informativi per l'erogazione dei servizi;
- mantenere i processi di pianificazione e attuazione della continuità operativa;
- mantenere la sicurezza fisica, logica, ambientale e delle comunicazioni.
- Definire un regolamento IT security policy da condividere con il personale

La Information Security Policy è destinata ai dipendenti SIA S.P.A. ed a tutti gli stakeholders interessati (clienti, fornitori e altre terze parti). L'ambito di applicazione della Information Security Policy coincide con il perimetro del Sistema di Gestione per la Sicurezza Informazioni (SGSI) implementato sul contesto dell'Organizzazione.

A tal fine l'Azienda ha definito l'ambito o portata del sistema ISO27001 con l'individuazione del seguente scope: **“Sviluppo, gestione ed erogazione di piattaforme applicative software e di servizi IT per il settore assicurativo”**.

In particolare, l'SGSI copre i seguenti aspetti:

- Gestione dell'infrastruttura IT ASPSIA

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 4 di 9	Riservatezza: Pubblico

- Gestione dell'infrastruttura IT ASPSIANP/SIAASP/No-Prod
- Gestione dell'infrastruttura IT SIACORP/SIASPA.COM
- Gestione dell'infrastruttura IT DR & BC
- Direzione Tecnica & Business Development JMIL
- Progettazione per evoluzioni e personalizzazioni al software JMIL
- Sviluppo del software JMIL e Quality Assurance
- Assistenza Jmil
- Manutenzione dei rilasci del software JMIL e Quality Assurance

La rivisitazione del presente documento è prevista con cadenza almeno annuale e, comunque, in occasione di variazioni significative di elementi che hanno impatti sul SGSI e sulla sicurezza delle informazioni in azienda al fine di garantirne l'adeguatezza al contesto.

Regolamenti, contratti e legislazioni

Le policy di sicurezza e o relativi framework applicati alla gestione dei dati di SIA S.p.A. mantengono una costante conformità con le seguenti categorie di regolamenti e legislazioni:

- Regolamento UE 679 del 2016 e D.Lgs. 196/2003
- Altri provvedimenti e Linee guida inerenti la protezione dei dati, tra cui EDPB, ENISA Autorità Garante Privacy Italia (GPDP), Agenzia Nazionale Cybersecurity
- Contratti con i clienti e relativi SLA
- Leggi sul diritto d'autore
- Best practice e standard in materia di sviluppo degli applicativi software
- Regolamento UE DORA
- Direttiva NIS2
- Regolamento IA ACT

2. RUOLI E RESPONSABILITÀ PER LA SICUREZZA INFORMAZIONI

La Direzione Generale SIA S.P.A., in relazione alla struttura organizzativa aziendale e alle dimensioni interfunzionali della sicurezza delle informazioni, ha individuato i seguenti ruoli ed organi per la gestione del SGSI:

- Direzione generale
- Soggetto di riferimento per l'Alta Direzione Aziendale e Responsabile Sicurezza Informazioni (anche "Responsabile SGSI")
- CTO / IT Manager
- Gestione Risorse Umane

I soggetti sopra evidenziati si riuniscono in un Organo Direzionale del SGSI:

- Comitato Sicurezza Informazioni (anche "Comitato SGSI")

Sono previsti inoltre dei ruoli specifici nell'ambito di alcune procedure particolari, quali ad esempio l'Incident Response e la Business Continuity, per cui si rimanda alle rispettive politiche (vedi in particolare il documento **"Ruoli e Responsabilità"**).

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 5 di 9	Riservatezza: Pubblico

3. POLITICHE DI GESTIONE DEL RISCHIO

SIA S.P.A. ha implementato una politica di gestione del rischio dei sistemi informativi, definendo le modalità per l'identificazione, l'approvazione, l'implementazione e la verifica di modifiche a sistemi, applicazioni e infrastrutture IT che possano influire sulla sicurezza delle informazioni o sulla continuità operativa, secondo gli standard ISO27001:2022.

4. POLITICHE DI SEPARAZIONE DEI COMPITI

SIA S.P.A. 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 deve essere attuato quando opportuno, 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.

5. LINEA GUIDA: SICUREZZA NEI COMPORTAMENTI DEL PERSONALE

Tutti i dipendenti, nonché i collaboratori e le terze parti, sono responsabili della tutela delle informazioni SIA S.P.A. e della strumentazione informatica di SIA S.P.A. 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.

6. Affermazione dell'impegno per soddisfare i requisiti relativi a ISMS

L'azienda si è dotata di una *policy di management responsibility*, in applicazione del controllo: 5.4 - Management responsibilities (*Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization*), articolata in base ai seguenti punti.

Per maggiori info vedi il documento **procedura management review**.

7. Contatti con le Autorità e con i gruppi di interesse speciali

L'Azienda ha definito una serie di contatti con tutte le principali autorità rilevanti in termini di garanzia di sicurezza del ISMS o comunque rilevanti in base alle normative o ai gruppi speciali di interesse ad essa applicabili.

In particolare è stato definito il seguente prospetto.

Vedi anche i documenti/procedure in base alle rispettive policies (es. incident response).

Autorità/Enti	Soggetto referente o punto di contatto	Metodi di comunicazione
Ente di Certificazione ISMS	Responsabile ISMS	Contatti comunicati dall'Ente
Autorità Garante protezione dati	Consulente GDPR	Portale Garante o PEC
ACN/NIS 2	CSIRT	Contatti comunicati dall'autorità (vedi portale)
Autorità di Controllo DORA	Amm. Del.	Enti previsti dal Regolamento

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 6 di 9	Riservatezza: Pubblico

Polizia postale	Amm. Del.	Riferimenti pubblici e portale dedicato commissariatodips.it/
Altre autorità di P.S. (es. Comando locale Carabinieri)	Amm. Del.	Comando di Bassano del Grappa
VV.FF	Amm. Del.	Riferimenti pubblici (112)
Istituto vigilanza	Amm. Del.	Tel.
Gruppo di interesse	Soggetto referente o punto di contatto	Metodi di comunicazione
ASSO SOFTWARE	Amm. Del.to	Contatti predefiniti
FEDERPRIVACY	Consulente GDPR	Contatti predefiniti
CLUSIT	Consulente GDPR	Contatti predefiniti
ACN	Amm. Del.	Contatti predefiniti
IVASS	Amm. Del.	Contatti predefiniti
SHARE	Amm. Del.	Contatti predefiniti

8. Gestione sicurezza nel project management

Poiché l'Azienda ha nella sua mission lo sviluppo di software, adotta metodologie proprie per la protezione delle informazioni coinvolte negli stessi. Tali metodologie contemplano la piattaforma proprietaria di change/project management "SIA PROCAST", e opportune "access control policy" per le documentazioni sulle cartelle di rete. In relazione ai contenuti e alle sostanze dei progetti (in particolare codice sorgente di programmazione) vengono adottate le seguenti metodologie:

- Adozione di metodologie di quality assurance
- Altri standard di sviluppo sicuro del codice

Vedi a riguardo il documento della policy per la sicurezza nei processi di project management.

9. CLASSIFICAZIONE E PROTEZIONE DELLE INFORMAZIONI

SIA S.P.A. 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 dei livelli riportati in questa policy.

I livelli di classificazione adottati in SIA S.P.A. sono i seguenti:

- Riservato/Confidenziale SIA S.P.A.
- Interno/Business Use SIA S.P.A.
- Pubblico

L'azienda ha definito una "Information & Classification policy" a cui si rinvia per maggiori dettagli.

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 7 di 9	Riservatezza: Pubblico

10.LINEA GUIDA: 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*).

I diritti di accesso di tipo Amministrativo sono limitati il più possibile e controllati nel rispetto delle normative vigenti (Provvedimento del Garante della Privacy sugli Amministratori di Sistema).

Le utenze e i profili di accesso sono periodicamente controllati per verificarne l'adeguatezza nel tempo e sanare situazioni non conformi.

Per maggiori dettagli si rinvia al documento "Access Control Policy".

11.LINEA GUIDA: GESTIONE DEI SISTEMI ICT

Al fine di garantire la gestione in sicurezza di tutti i sistemi e infrastrutture ICT aziendali, è necessario che siano adeguatamente documentate le procedure operative e che siano chiaramente definite le responsabilità in merito a:

- Installazione del software nei server e nei desktop/notebook;
- 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;
- Uso di sistemi di Crittografia.

Per maggiori dettagli si rinvia ai documenti relativi alle Procedure IT.

12.LINEA GUIDA: SVILUPPO E MANUTENZIONE SOFTWARE

I processi di sviluppo e manutenzione del software applicativo devono essere opportunamente regolamentati, documentati e gestiti, non solo nell'intento di perseguire la massima qualità di servizio, efficacia ed efficienza operativa, ma anche nell'ottica di garantire che il software rispetti i requisiti di sicurezza necessari. Le **'Linee guida sullo sviluppo di software sicuro'**, sono il documento *master* per tutti coloro che si occupano di sviluppo; il documento è diffuso e consultabile nel sistema documentale intero (vedi documento **Procedura Secure Development Policy**).

13.LINEA GUIDA: GESTIONE DEGLI INCIDENTI DI SICUREZZA, BC e DR

L'Incident Response (IR) e il Disaster Recovery (DR) sono due aspetti distinti della gestione della continuità aziendale, con obiettivi e scope differenti. L'IR si concentra sulla gestione di incidenti di sicurezza (es. attacchi informatici), miranti a contenerne l'impatto e a ripristinare la normalità operativa. Il DR, invece, riguarda la gestione di eventi catastrofici (es. guasti hardware, catastrofi naturali) che possono interrompere le operazioni IT, con l'obiettivo di ripristinare le infrastrutture e i sistemi.

Sulla scorta delle suesposte precisazioni, l'Azienda ha predisposto le seguenti linee guida per IR e BC/DR

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 8 di 9	Riservatezza: Pubblico

14. LINEA GUIDA: GESTIONE DEGLI INCIDENTI DI SICUREZZA

Gli incidenti devono essere 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, è necessario individuare gli incidenti di sicurezza che possono mettere a repentaglio la riservatezza, l'integrità e la disponibilità delle informazioni. Per questo deve essere definito, documentato ed adottato un processo per la gestione degli incidenti che preveda almeno:

- La classificazione degli incidenti in base alla loro priorità;
- La registrazione degli incidenti;
- Opportune modalità di gestione in relazione alla classificazione;
- L'individuazione dei responsabili della risoluzione degli incidenti;
- 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.

Per maggiori dettagli vedi documento **"Incident Response Procedure"**.

15. LINEA GUIDA: GESTIONE DELLA BUSINESS CONTINUITY

SIA S.P.A. deve adottare 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 incidentali derivati dalle best practices internazionali;
- Degli impatti dei suddetti scenari sull'azienda e dei conseguenti livelli di rischio.

Per maggiori dettagli vedi documento **"BC & DR"**.

16. LINEA GUIDA: GESTIONE DEI FORNITORI

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

Deve essere fatta preventivamente una valutazione dei rischi delle terze parti e, quindi, devono essere 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, in particolare nel caso di fornitori/outsourcers ICT.

Inoltre, le terze parti devono garantire a SIA S.P.A. 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 SIA S.P.A. siano applicati da tutte le parti coinvolte nella catena di fornitura.

Per maggiori dettagli vedi documenti **"Classificazione Fornitori, e procedura gestione Supply chain"**.

17. LINEA GUIDA: COMPLIANCE E AUDIT

SIA S.P.A. opera nel rispetto delle leggi nazionali e internazionali applicabili ai settori di mercato per i quali opera, dei regolamenti interni, delle normative volontarie adottate (es. ISO 27001, etc.), dei contratti con

	INFORMATION SECURITY POLICY	Codice: P-ISP-02 Rev. 1 del 03/04/2026
	Pag. 9 di 9	Riservatezza: Pubblico

le controparti esterne. Inoltre, SIA S.P.A. garantisce l'adeguata disponibilità di documentazione e di risorse per consentire le eventuali attività degli Auditor interni ed esterni.

Per il dettaglio, si veda la Procedura Gestionale ‘

I principali riferimenti normativi cogenti corrispondono a:

- Regolamento Europeo 2016/679 in materia di protezione dei dati personali;
- D.Lgs. 196/2003 “Codice in materia di protezione dei dati personali” e ss.mm.ii., per le parti ancora in vigore;
- 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.
- Direttiva NIS2
- Regolamento DORA
- Regolamento IA ACT

Per maggiori dettagli vedi documento **“Audit procedure o procedura di audit interno”**.

18. PIANO DOCUMENTALE PER COMPLIANCE ISO27001

L'Azienda ha predisposto un piano documentale per asseverare la compliance alla presente norma. Vedi documento “piano documentale”, allegato al presente.

19. COMUNICAZIONE ALLE PARTI INTERESSATE E STAKEHOLDERS

La presente politica è stata oggetto di comunicazione a tutte le parti interessate, individuate da SIA S.P.A., tra cui:

- Clienti (aziende del settore assicurativo)
- Dipendenti e collaboratori
- Fornitori IT e partner tecnologici
- Autorità e organismi di controllo
- Proprietà / Direzione aziendale
- Utenti finali del software ERP (Jmil).

Per ciascuna parte interessata sono stati individuate le rispettive esigenze e requisiti a cui deve rispondere l'implementazione dello standard ISO27001 da parte di SIA S.P.A.