IPAS S.p.A. • C.so LOMBARDIA, 36 (AUT. PESCARITO)
10099 SAN MAURO T.SE
Tel. 011.2734567/8/9/0 r.a. – 011.2235858 r.a.
Telefax 011.2735764
E-mail: ipas@ipas.it
Cap. Soc. € 5.000.000 int vers.
Reg. Impr. Torino Cod. Fisc. e P. IVA 02495130011
R.E.A. 561871

GRUPPO IPAS®

Quality management system ISO 9001
• Customer focus
• Customer satisfaction
• Continuous improvement
• System/process effectiveness
ID 15 100 2010866

Occupational safety management ISO 45001
• Hazard detection
• Risk assessment
• Control measures
• Involvement of employees
ID 15 118 20152

Politica del SGSI

Titolo	Politica del SGSI			
Versione	1.0#1		N. pag.	6
Proprietario	IPAS S.p.A.			
Autore	Antonio D'Addio		Data	12/05/2025
Criteri per il controllo del documento	Idoneità	Adeguatezza		
Riesame:	L. Scarabosio (Auditor)	L. Scarabosio (Auditor)	Data	23/07/2025
Approvazione:	B. Naddei (Presidente)	B. Naddei (Presidente)	Data	23/07/2025
Classificazione	PUBBLICO			

Sommario

1 INTRODUZIONE

1.1 SCOPO

La presente politica definisce l'impegno di IPAS S.p.A. nella protezione delle informazioni, siano esse proprie, dei clienti, dei partner o di altri stakeholders, garantendone riservatezza, integrità e disponibilità, in conformità alla norma UNI CEI EN ISO/IEC 27001:2024.

IPAS considera la Sicurezza delle Informazioni un aspetto primario per la protezione del proprio business e dei propri clienti. La reputazione aziendale si basa sulla corretta gestione degli asset fisici, informativi e del personale: per preservarla è quindi fondamentale un modello della sicurezza che miri a proteggere i processi e le informazioni da un'ampia gamma di minacce e a minimizzarne l'impatto sulla continuità operativa.

Tale politica si applica a tutte le forme di informazione, non solo a quella digitale. Pertanto, anche alla documentazione cartacea gestita dall'azienda.

1.2 OBIETTIVI

Gli obiettivi del Sistema di Gestione della Sicurezza dell'Informazione di IPAS sono:

- Garantire una protezione dell'informazione adeguata in termini di riservatezza, integrità e disponibilità;
- Garantire la continuità operativa anche in caso di eventi critici;
- Proteggere l'interesse dei clienti, dei dipendenti e delle terze parti;
- Assicurare la conformità alle leggi e ai regolamenti applicabili in materia di trattamento e protezione dell'informazione;
- Assicurare un modello strutturale alla protezione dell'informazione e alla gestione dei rischi correlati;
- Rispondere in modo efficace alle crescenti minacce ai sistemi informativi nello spazio cibernetico.

Questi obiettivi costituiscono il fondamento per la creazione, l'implementazione, il funzionamento, il monitoraggio, la revisione, la manutenzione e il miglioramento continuo di un efficace sistema di gestione della sicurezza delle informazioni, realizzato in conformità alla norma UNI EN ISO/IEC 27001:2024.

1.3 AMBITO DI APPLICAZIONE

Questa politica si applica a tutti i processi, le persone, le tecnologie e i servizi gestiti da IPAS S.p.A. nell'ambito delle attività di:

- Strategia e consulenza rivolte alla comunicazione esterna;
- Produzione e diffusione di contenuti pubblicitari destinati agli spazi di impianti propri, o affittati da terzi, sul territorio italiano, secondo le richieste dei clienti;
- Gestione dei clienti, dei fornitori, dei partner esterni (agenti) e dei dipendenti attraverso i programmi e le procedure del proprio gestionale IBM Power i (AS400);
- Gestione degli impianti dedicati all'arredo urbano e alle campagne affissionali, nel contesto di contratti attivi e in corso d'opera nonché della posa in opera e fino all'eventuale rimozione;
- Gestione di impianti digitali (DOOH) e delle campagne pubblicitarie montate sui relativi palinsesti.

1.4 INFORMAZIONI PROTETTE

Le informazioni protette dal SGSI possono essere riassunte come segue (in accordo con quanto definito nell'analisi del contesto).

Parte interessata	Informazioni protette dal SGSI		
	Dati personali	Contratti	Documentazione dei processi aziendali
Soci/azionisti	Dati anagrafici soci, amministratori	Resoconto economici	Verbali CDA, accordi riservati
Dipendenti/collaboratori	Dati su selezione e reclutamento Dati anagrafici dipendenti e collaboratori Login, pwd, log, e-mail, permessi, dati sensibili Sorgenti grafici, patrimonio immagini impianti	Dati elaborazione presenza/paghe Regolamento aziendale Credenziali accessi ai sistemi tramite VPN	Documentazione aziendale ISO Informative privacy
Clienti	Dati anagrafici Dati fiscali	Dati contratti clienti /fatturazione /recupero crediti /rinnovi	n.a.
Fornitori	Dati anagrafici fornitori Mail	Dati contratti fornitori /fatturazione Credenziali accessi ai sistemi tramite VPN	n.a.
Enti Regolatori	n.a.	n.a.	Requisiti normativi e relativi aggiornamenti
Pubblica Amministrazione (o privati)	Dati anagrafici Dati dei referenti Ente che rilascia la Concessione Dati del privato con cui si stipula la Concesione	Stipula della Concessione	n.a.
Agenti di vendita	Dati anagrafici Dati fiscali	Dati degli ordini e tipologia (Nuovo, Re.Di., annulla e sostituisce, rinnovo)	n.a.

1.5 PRINCIPI GUIDA

- Leadership e impegno: La Direzione assume la responsabilità dell'efficace attuazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).
- Approccio basato sul rischio: Tutte le attività sono valutate in base al rischio informatico.
- Formazione e consapevolezza: Tutto il personale è formato e sensibilizzato sul tema della sicurezza.
- Controllo degli accessi: Le informazioni sono accessibili solo a personale autorizzato in base al principio del "minimo privilegio".
- Gestione dei fornitori: I partner e fornitori sono selezionati e monitorati anche in base a requisiti di sicurezza informativa.

1.6 RESPONSABILITÀ

Tutti i collaboratori e consulenti di IPAS S.p.A. hanno il dovere di rispettare questa politica e segnalare eventuali vulnerabilità o incidenti alla funzione preposta (RCED).

1.7 MIGLIORAMENTO CONTINUO

IPAS S.p.A. si impegna a riesaminare periodicamente la presente politica e il SGSI nel suo complesso, al fine di garantirne l'adeguatezza rispetto all'evoluzione del contesto normativo, tecnologico e operativo.

1.8 COMUNICAZIONE

La politica è comunicata internamente tramite i canali aziendali ufficiali (intranet, e-mail, formazione) ed è resa disponibile agli stakeholder esterni, se richiesto.

1.9 VALIDITÀ E RIESAME

La presente politica è riesaminata almeno annualmente o in caso di modifiche significative ai rischi o ai processi aziendali.

2 LIVELLI DI CLASSIFICAZIONE DEI DOCUMENTI

Sebbene la ISO 27001 non prescriva una tassonomia specifica, è prassi comune adottare una classificazione a più livelli, che può includere:

1. Pubblico: Informazioni destinate alla diffusione senza restrizioni, come comunicati stampa o materiali promozionali.
2. Ad uso interno (o anche solamente "Interno"): Informazioni non destinate al pubblico, ma che non richiedono particolari misure di sicurezza.
3. Riservato: Informazioni che, se divulgate, potrebbero causare danni all'organizzazione, come dati degli ordini / contratti o dati dei clienti.
4. Strettamente riservato: Informazioni altamente sensibili, la cui divulgazione non autorizzata potrebbe avere gravi conseguenze, come dettagli finanziari o piani strategici.

2.1 IMPLEMENTAZIONE DELLA CLASSIFICAZIONE

Per implementare efficacemente un sistema di classificazione dei documenti, è consigliabile:

- Definire criteri chiari: Stabilire linee guida per determinare il livello di classificazione appropriato per ciascun tipo di informazione.
- Etichettare i documenti: Applicare marcature visibili (fisiche o digitali) che indicano il livello di classificazione.
- Controllare gli accessi: Limitare l'accesso alle informazioni in base al principio del "minimo privilegio", assicurando che solo il personale autorizzato possa accedere a determinati livelli di informazioni.
- Formare il personale: Educare i dipendenti sull'importanza della classificazione delle informazioni e sulle procedure da seguire.
- Monitorare e rivedere: Effettuare audit periodici per garantire la conformità alle politiche di classificazione e apportare modifiche se necessario.

Implementare una politica di classificazione dei documenti conforme alla ISO 27001 aiuta a proteggere le informazioni sensibili, ridurre i rischi associati alla divulgazione non autorizzata e garantire la fiducia dei clienti e dei partner commerciali.

Antonio D'Addio

Firmato digitalmente da Antonio D'Addio
DN: cn=Antonio D'Addio, c=IT, o=Ipas S.p.A., ou=CED, email=responsabileit@ipas.it
Data: 2025.07.28 15:08:56 +02'00'