					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P03					Titolo del documento: **Politica di uso accettabile**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineata a norme e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 5	Definisce regole comportamentali e requisiti per la politica di uso accettabile
ISO/IEC 27002:2022	Controls 6.1, 6.2, 8.1, 8	Fornisce indirizzi in materia di responsabilità per la sicurezza delle informazioni, sensibilizzazione e governance di dispositivi e dati
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Controllo degli accessi e controlli di sensibilizzazione/comportamentali rilevanti per l'uso degli asset IT
GDPR UE	Articles 5(1)(f), 32; Recital 39	Impone riservatezza e integrità, richiede controlli tecnici e organizzativi e basi giuridiche per l'uso corretto
NIS2 UE	Article 21(2)(a–d)	Richiede politiche operative e formazione sull'uso sicuro
DORA UE	Article 5	Supporta la gestione del rischio ICT disciplinando il comportamento degli utenti
COBIT 2019	APO07, BAI05, DSS05, MEA01	Risorse umane, gestione del cambiamento, sicurezza gestita, monitoraggio della conformità e delle prestazioni

1. Scopo

1.1 La presente politica definisce gli usi accettabili e non accettabili dei sistemi informativi, delle risorse informatiche, degli strumenti di comunicazione e delle pratiche di trattamento dei dati dell'organizzazione.

1.2 Essa assicura che tutti gli utenti comprendano le proprie responsabilità nell'uso degli asset IT aziendali e che le loro azioni supportino la riservatezza, l'integrità, la disponibilità (CIA) e il trattamento lecito delle informazioni.

1.3 La politica soddisfa il requisito della ISO/IEC 27001:2022, clausola 5.10, stabilendo regole comportamentali per l'uso dei sistemi e applicando misure di sicurezza tecniche e procedurali per ridurre al minimo il rischio di uso improprio, negligenza o abuso.

1.4 La politica supporta inoltre le attività di indagine e di applicazione, incluse la risposta agli incidenti e le misure disciplinari in caso di violazioni.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le persone fisiche e giuridiche alle quali è concesso l'accesso ai sistemi informativi e agli asset dell'organizzazione, inclusi, a titolo esemplificativo e non esaustivo:

2.1.1 dipendenti, collaboratori esterni, consulenti, tirocinanti e lavoratori somministrati

2.1.2 fornitori terzi con accesso ai sistemi o con ruoli amministrativi delegati

2.1.3 ospiti o partner che utilizzano infrastrutture informatiche di proprietà dell'organizzazione o da essa autorizzate

2.2 L'ambito di applicazione comprende tutti gli asset tecnologici e i dati dell'organizzazione, inclusi:

2.2.1 workstation, laptop, dispositivi mobili e server

2.2.2 infrastrutture di rete e servizi ospitati nel cloud

2.2.3 posta elettronica, messaggistica, archiviazione file, piattaforme di collaborazione e VPN

2.2.4 dati a riposo, in transito o in corso di trattamento, indipendentemente dal formato o dalla posizione

2.2.5 qualsiasi dispositivo personale utilizzato nell'ambito di accordi BYOD (Bring Your Own Device) che si connetta ai sistemi dell'organizzazione

2.3 La presente politica si applica in tutti gli ambienti di lavoro, inclusi:

2.3.1 uffici aziendali e siti produttivi

2.3.2 sedi di lavoro da remoto o assetti ibridi

2.3.3 attività sul campo o sedi gestite da terze parti

2.4 Tutti gli utenti sono tenuti a prendere visione della presente politica e a rispettarla quale condizione per accedere ai sistemi aziendali o trattare dati aziendali.

3. Obiettivi

3.1 Definire e applicare regole per l'uso accettabile delle risorse IT dell'organizzazione.

3.2 Prevenire accessi non autorizzati, perdita di dati o danni derivanti da uso negligente o malevolo.

3.3 Proteggere reti, asset e dati aziendali dalle minacce introdotte dal comportamento degli utenti.

3.4 Supportare gli obblighi legali e contrattuali dimostrando un'adeguata diligenza nella governance delle risorse IT.

3.5 Assicurare coerenza e chiarezza nell'applicazione delle azioni disciplinari e dei processi di gestione delle eccezioni.

3.6 Promuovere una cultura dell'uso etico, sicuro e responsabile delle risorse informatiche digitali e fisiche.

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Approva la Politica di uso accettabile (AUP) e ne assicura l'allineamento agli obiettivi aziendali, ai requisiti normativi e ai valori dell'organizzazione.

4.1.2 Alloca le risorse necessarie per l'applicazione della politica, la formazione, il monitoraggio e il riesame della politica.

4.1.3 Riesamina lo stato di conformità e le misure disciplinari associate alle violazioni della politica nell'ambito della governance del SGSI.

4.2 Team IT e Sicurezza delle informazioni

4.2.1 Attuano i controlli tecnici per applicare la presente politica, inclusi:

4.2.2 filtraggio dei contenuti, protezione antimalware, strumenti di sicurezza degli endpoint e monitoraggio della rete

4.2.3 configurazioni di sicurezza della posta elettronica e soluzioni di prevenzione della perdita di dati (DLP)

4.2.4 liste di blocco e liste di autorizzazione per software, hardware e siti web

4.2.5 Mantengono un inventario del software, dei dispositivi e dei servizi approvati e vietati.

4.2.6 Indagano sulle sospette violazioni della politica di uso accettabile, raccolgono evidenze forensi e supportano, ove appropriato, azioni disciplinari o legali.

4.2.7 Collaborano con Risorse Umane e Legale in materia di gestione dell'incidente, escalation e obblighi di segnalazione.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 Trigger e frequenza del riesame

9.1.1 La presente politica deve essere riesaminata:

9.1.1.1 almeno annualmente

9.1.1.2 a seguito di qualsiasi cambiamento significativo della tecnologia o dell'infrastruttura

9.1.1.3 dopo incidenti o risultanze di audit che evidenzino lacune nell'applicazione della politica

9.1.1.4 in risposta a modifiche della normativa o dei contratti applicabili

9.2 Titolare e approvazione

9.2.1 Il Responsabile della sicurezza delle informazioni (CISO) o il Responsabile del SGSI designato è responsabile del processo di riesame.

9.2.2 Gli aggiornamenti devono essere approvati dalla Direzione aziendale e comunicati a tutta l'organizzazione.

9.2.3 La presa d'atto dei termini aggiornati deve essere nuovamente acquisita in caso di riemissione della politica.

9.3 Gestione documentale

9.3.1 La politica deve includere i seguenti metadati e dettagli di versionamento:

9.3.1.1 titolo, ID e livello di classificazione

9.3.1.2 proprietario della politica e responsabile del documento

9.3.1.3 cronologia delle modifiche e motivazioni degli aggiornamenti

9.3.1.4 date di riesame e data del successivo aggiornamento pianificato

9.3.1.5 riferimenti alla distribuzione e al registro delle prese d'atto

9.3.2 La copia master deve essere conservata nel repository documentale del SGSI sotto controllo di versione.

10. Politiche correlate e collegamenti

10.1 La presente politica deve essere interpretata congiuntamente alle seguenti:

10.1.1 P1 – Politica per la sicurezza delle informazioni: definisce le aspettative comportamentali di base e l'impegno della direzione aziendale rispetto all'uso accettabile.

10.1.2 P4 – Politica di controllo degli accessi: definisce autorizzazioni e diritti associati all'accesso di utenti, sistemi e dati, applicando direttamente i limiti dell'uso accettabile.

10.1.3 P6 – Politica di gestione del rischio: affronta i rischi connessi al comportamento e supporta le attività di monitoraggio e trattamento associate alle minacce derivanti dagli utenti.

10.1.4 P7 – Politica di onboarding e cessazione del personale: assicura che i termini di uso accettabile siano confermati all'ingresso e revocati all'uscita.

10.1.5 P9 – Politica di lavoro da remoto: estende le disposizioni sull'uso accettabile agli ambienti di lavoro da remoto e ibridi.

10.2 Tali politiche correlate costituiscono un modello di difesa multilivello per la governance comportamentale, tecnica e contrattuale.

11. Norme e quadri di riferimento

11.1 La presente Politica di uso accettabile (AUP) è allineata a norme riconosciute a livello internazionale e a quadri giuridici di riferimento, al fine di assicurare controlli comportamentali applicabili, verificabili in sede di audit e basati sul rischio per tutti gli usi digitali e fisici dei sistemi informativi.

11.2 ISO/IEC 27001:2022

11.2.1 Clausola 5.10 – Uso accettabile delle informazioni e degli altri asset associati: la presente politica soddisfa direttamente il requisito di definire, comunicare e applicare regole che disciplinano l'uso appropriato delle risorse IT.

11.2.2 Allegato A Controllo 6.1 – Responsabilità per la sicurezza delle informazioni: assegna responsabilità chiare in materia di comportamento degli utenti e supervisione della conformità.

11.2.3 Allegato A Controllo 6.2 – Consapevolezza, istruzione e formazione sulla sicurezza delle informazioni: i processi di formazione integrata e presa d'atto della politica fanno parte dell'applicazione della politica di uso accettabile.

11.2.4 Allegato A Controllo 8.1 – Dispositivi endpoint degli utenti e 8.12 – Prevenzione della perdita di dati (DLP): affronta i comportamenti accettabili sui dispositivi degli utenti e disciplina le attività che potrebbero causare esposizione o perdita di dati.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (controllo degli accessi per dispositivi mobili) e AC-20 (uso di sistemi informativi esterni): la presente politica definisce obblighi e restrizioni per gli utenti relativamente a BYOD e accesso a sistemi di terze parti.

11.3.2 PL-4 (regole di comportamento): fornisce requisiti dettagliati di uso accettabile coerenti con la presente politica.

11.3.3 AT-2 (formazione di sensibilizzazione alla sicurezza): supportato tramite formazione degli utenti e presa d'atto documentata della politica.

11.3.4 AU-2 (eventi di audit) e AU-12 (generazione dell'audit): l'applicazione della politica si basa sul monitoraggio delle azioni degli utenti e sulla generazione di allerte in caso di violazioni.

11.4 GDPR UE (2016/679):

11.4.1 Articolo 5(1)(f): impone la sicurezza e l'integrità dei dati personali; la presente politica mitiga i rischi introdotti dal comportamento umano e dall'uso non autorizzato.

11.4.2 Articolo 32: richiede misure tecniche e organizzative, quali controlli comportamentali e restrizioni d'uso, per proteggere i dati personali.

11.4.3 Considerando 39: evidenzia la necessità di garantire che solo gli accessi necessari e l'uso lecito dei dati siano consentiti a soggetti autorizzati.

11.5 Direttiva UE NIS2 (2022/2555):

11.5.1 Articolo 21(2)(a–d): richiede politiche operative e formazione per l'uso sicuro dei sistemi, che la presente politica di uso accettabile attua definendo comportamenti, monitoraggio e processi di applicazione.

11.6 DORA UE (2022/2554):

11.6.1 Articolo 5: la presente politica supporta il quadro di riferimento per la gestione del rischio ICT definendo regole per l'interazione tra persone e sistemi e riducendo al minimo l'esposizione al rischio cyber derivante dal comportamento.

11.7 COBIT 2019:

11.7.1 APO07 Gestire le risorse umane: applica responsabilità e sensibilizzazione degli utenti lungo l'intero ciclo di vita del personale.

11.7.2 BAI05 – Managed Organizational Change: integra la governance dell'uso accettabile nei processi di cambiamento che incidono sul comportamento degli utenti.

11.7.3 DSS05: supporta il monitoraggio delle attività degli utenti, le allerte comportamentali e i meccanismi di risposta automatizzati.

11.7.4 MEA01 – Monitor, Evaluate, and Assess Performance and Conformance: la politica definisce metriche e meccanismi per convalidare la conformità degli utenti alle aspettative comportamentali.