					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P05S					Titolo del documento: **Politica di gestione delle modifiche**							
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**

Allineamento a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1, 8	
ISO/IEC 27002:2022	Controllo 8	
NIST SP 800-53 Rev. 5	CM-2 to CM-5, CM-11	
Direttiva UE NIS2	Articolo 21(2)(b)	
Regolamento UE DORA	Articoli 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Scopo

1.1 La presente politica garantisce che tutte le modifiche ai sistemi IT, alle configurazioni, alle applicazioni aziendali o ai servizi cloud siano pianificate, sottoposte a valutazione del rischio, testate e approvate prima dell'attuazione.

1.2 L'obiettivo è ridurre le interruzioni operative, i rischi per la sicurezza e le indisponibilità del servizio mediante un processo semplificato ma vincolante, applicabile anche alle piccole imprese con risorse limitate.

1.3 La presente politica supporta la certificazione ISO/IEC 27001:2022 formalizzando le modalità con cui le modifiche tecniche e operative sono gestite e documentate.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Dipendenti e responsabili di funzione che propongono o attuano modifiche

2.1.2 Fornitore di supporto IT esterno o fornitori di servizi IT esternalizzati che gestiscono sistemi o software

2.1.3 Direttore generale (GM), che detiene la responsabilità complessiva dell'approvazione delle modifiche

2.2 Essa copre le modifiche a:

2.2.1 Software (aggiornamenti, patch, nuove applicazioni)

2.2.2 Hardware (sostituzioni, upgrade)

2.2.3 Configurazioni di rete e firewall

2.2.4 Servizi cloud, autorizzazioni di accesso degli utenti o integrazioni con i fornitori

2.2.5 Processi aziendali critici che coinvolgono i sistemi informativi

2.3 Rientrano nell'ambito di applicazione della presente politica sia le modifiche pianificate sia quelle di emergenza.

3. Obiettivi

3.1 Garantire che tutte le modifiche ai sistemi IT e ai sistemi aziendali siano autorizzate, documentate e reversibili in caso di problemi.

3.2 Prevenire indisponibilità non pianificate, perdita di dati o incidenti di sicurezza causati da modifiche non controllate.

3.3 Definire procedure semplici e ripetibili per la richiesta, l'approvazione, il test e il rollback delle modifiche.

3.4 Mantenere un registro delle modifiche verificabile in sede di audit, a supporto della responsabilità operativa e della conformità normativa.

3.5 Consentire decisioni basate sul rischio per le modifiche significative o sensibili.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Detiene la responsabilità ultima per tutte le modifiche rilevanti.

4.1.2 Riesamina e approva le modifiche non ordinarie, critiche o ad alto rischio.

4.1.3 Riesamina il registro delle modifiche con cadenza trimestrale o a seguito di incidenti rilevanti.

4.2 Supporto IT o fornitore di supporto IT esternalizzato

4.2.1 Attua le modifiche, inclusi aggiornamenti di configurazione, applicazione delle patch e migrazioni di sistema.

4.2.2 Mantiene un registro delle modifiche di base con indicazione di date, tipologie di modifica, esiti e approvatori.

4.2.3 Esegue i test delle modifiche prima dell'attuazione e applica, ove necessario, le procedure di rollback.

4.2.4 Informa gli utenti interessati prima e dopo le modifiche rilevanti.

[... 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 Riesame annuale

9.1.1 La presente politica deve essere riesaminata annualmente dal Direttore generale (GM) o dal referente IT designato per garantirne l'allineamento ai sistemi, ai flussi di lavoro e ai requisiti normativi vigenti.

9.2 Riesami intermedi

9.2.1 I riesami devono inoltre essere attivati da:

9.2.1.1 Incidenti di sicurezza causati da una gestione inadeguata delle modifiche

9.2.1.2 Introduzione di nuovi sistemi IT

9.2.1.3 Modifiche a norme rilevanti quali ISO, NIS2 o DORA

9.3 Documentazione degli aggiornamenti

9.3.1 Le modifiche alla presente politica devono essere soggette a controllo di versione e approvate dal Direttore generale (GM). Ogni versione deve riportare la data, il riepilogo delle modifiche e l'approvatore.

9.4 Comunicazione della politica

9.4.1 Eventuali aggiornamenti devono essere comunicati a tutti i dipendenti e ai fornitori esterni interessati. La documentazione deve essere aggiornata in tutti i punti di riferimento pertinenti (ad es. portale del personale, unità condivise).

10. Politiche correlate e collegamenti

10.1 La presente politica è strettamente correlata alle seguenti politiche PMI:

10.1.1 P2S – Politica sui ruoli e le responsabilità di governance: definisce l'autorità di approvazione delle modifiche.

10.1.2 P4S – Politica di controllo degli accessi: garantisce che le modifiche agli accessi derivanti dai cambiamenti siano documentate e attuate correttamente.

10.1.3 P7S – Politica di onboarding e cessazione del personale: coordina le modifiche relative ai passaggi di ruolo e al provisioning degli accessi.

10.1.4 P15S – Politica di backup e ripristino: garantisce che le procedure di rollback e ripristino possano essere eseguite in caso di esito negativo di una modifica.

10.1.5 P30S – Politica di risposta agli incidenti: disciplina le modalità di trattamento delle modifiche non riuscite o non autorizzate come incidenti di sicurezza.

11. Norme e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 6.1 – La pianificazione basata sul rischio deve includere le attività di modifica.

11.1.2 Clausola 8.1 – I controlli operativi devono essere applicati in modo coerente alle attività connesse alle modifiche per garantire l'integrità del servizio.

11.2 ISO/IEC 27002

11.2.1 Controllo 8.32 – Fornisce indicazioni per processi sicuri di gestione delle modifiche, inclusi documentazione, test e approvazione.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Configurazione di baseline dei sistemi prima della modifica.

11.3.2 CM-3 – Controllo delle modifiche di configurazione.

11.3.3 CM-4 – Analisi dell'impatto sulla sicurezza.

11.3.4 CM-5 – Approvazione e documentazione delle modifiche.

11.3.5 CM-11 – Audit e monitoraggio delle modifiche.

11.4 Direttiva UE NIS2

11.4.1 Articolo 21(2)(b) – Richiede procedure formali per le misure di sicurezza tecniche e organizzative, inclusa la gestione delle modifiche.

11.5 Regolamento UE DORA

11.5.1 Articoli 6(9) e 8(4)(b) – Richiedono ai soggetti finanziari di mantenere processi di gestione delle modifiche e della configurazione per i sistemi ICT.

11.6 COBIT 2019

11.6.1 BAI06 – Gestire le modifiche: pone l'accento su pianificazione, valutazione del rischio e capacità di rollback.

11.6.2 DSS01 – Gestire le operazioni: garantisce l'integrità operativa durante transizioni e modifiche tecniche.