					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P29S					Titolo del documento: **Politica sui dati di test e sugli ambienti di test**							
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 standard e normative

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1, 8	
ISO/IEC 27002:2022	Controlli 8.28–8.29	
NIST SP 800-53 Rev.5	SA-11, SA-12, SC-32	
GDPR UE	Articoli 5(1)(c), 25, 32	
NIS2 UE	Articolo 21(2)(e), (h)	
DORA UE	Articolo 9	
COBIT 2019	BAI07, DSS	

1. Finalità

1.1 La presente politica definisce le modalità di gestione dei dati di test e degli ambienti di test al fine di prevenire esposizioni accidentali, violazioni dei dati o interruzioni operative durante le attività di test.

1.2 Essa garantisce che i dati reali dei clienti non siano utilizzati impropriamente durante i test software o di sistema e che gli ambienti di test siano separati dai sistemi di produzione sia sul piano logico sia su quello tecnico.

1.3 La politica è definita per supportare le PMI nel soddisfacimento dei requisiti di certificazione ISO/IEC 27001 e della normativa applicabile in materia di protezione dei dati, mantenendo al contempo un impianto pratico e attuabile anche nelle organizzazioni prive di un team IT dedicato.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutti gli ambienti di test (ad es. server di staging, sistemi sandbox, ambienti di prova di sviluppo)

2.1.2 tutti i dati di test, creati manualmente, generati o derivati da dati dei sistemi in esercizio

2.1.3 tutto il personale coinvolto nelle attività di test, inclusi dipendenti, collaboratori esterni, freelance e fornitori IT

2.1.4 qualsiasi attività di test che possa avere impatto su piattaforme rivolte ai clienti, sistemi aziendali interni o servizi di terze parti

2.2 La politica copre sia gli ambienti tecnici sia i processi utilizzati a supporto di:

2.2.1 sviluppo di siti web, applicazioni e strumenti

2.2.2 aggiornamenti di sistema, test di configurazione e test di integrazione

2.2.3 test funzionali o di sicurezza, automatizzati e manuali

3. Obiettivi

3.1 Prevenire l'utilizzo nei test di dati reali e identificabili dei clienti, salvo che siano anonimizzati ed espressamente approvati.

3.2 Mantenere una rigorosa separazione tra sistemi di test e sistemi di produzione per evitare esposizioni indesiderate di dati o interferenze operative.

3.3 Proteggere i sistemi e i dati di test da accessi non autorizzati, divulgazioni accidentali o riutilizzo tra ambienti in assenza di controlli adeguati.

3.4 Rispettare la normativa applicabile in materia di protezione dei dati (ad es. GDPR, NIS2), assicurando che tutti i dati di test siano trattati in modo lecito, corretto e sicuro.

3.5 Supportare la capacità dell'organizzazione di dimostrare la conformità in sede di audit esterni e di certificazione ISO/IEC 27001 mediante la documentazione delle pratiche di test e l'applicazione coerente delle misure di sicurezza.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Ha la responsabilità complessiva della protezione dei dati di test e della sicurezza dei sistemi di test.

4.1.2 Approva qualsiasi utilizzo di dati reali nei test previa verifica della presenza di misure di sicurezza adeguate (ad es. anonimizzazione o mascheramento dei dati).

4.1.3 Verifica che le attività di test siano correttamente documentate e conformi alla presente politica.

4.2 Responsabile di progetto

4.2.1 Coordina la progettazione e l'esecuzione dei processi di test.

4.2.2 Garantisce che tutti i membri del team comprendano e rispettino la presente politica.

4.2.3 Conferma che i sistemi di test siano configurati in modo sicuro prima dell'avvio delle attività di test.

4.2.4 Segnala al Direttore generale (GM) qualsiasi incidente che coinvolga ambienti di test o perdita di dati.

[... 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 Riesami pianificati

9.1.1 La presente politica deve essere riesaminata almeno una volta all'anno dal Direttore generale (GM). Il riesame garantisce che la politica rimanga aggiornata rispetto a:

9.1.1.1 modifiche agli strumenti, alle piattaforme o agli ambienti di sviluppo software

9.1.1.2 aggiornamenti degli obblighi normativi, inclusi quelli relativi alla protezione dei dati o alla resilienza digitale

9.1.1.3 esigenze di certificazione delle PMI e capacità di dimostrare la conformità in sede di audit ai sensi della ISO/IEC 27001

9.2 Eventi attivanti per il riesame intermedio

9.2.1 Devono essere effettuati riesami aggiuntivi a seguito di:

9.2.1.1 qualsiasi incidente che comporti esposizione di dati o compromissione negli ambienti di test

9.2.1.2 utilizzo di dati reali nei test, anche se anonimizzati

9.2.1.3 introduzione di nuovi metodi di test, sistemi o fornitori

9.2.1.4 aggiornamenti normativi che incidano sulle modalità di trattamento dei dati durante i test

9.3 Gestione delle modifiche e comunicazione

9.3.1 Il Direttore generale (GM) è responsabile di:

9.3.1.1 aggiornare la presente politica e documentare ogni modifica nella cronologia delle versioni

9.3.1.2 comunicare gli aggiornamenti al personale, agli sviluppatori e ai fornitori di servizi interessati

9.3.1.3 confermare che tutto il personale coinvolto nei test comprenda e applichi le regole più recenti

9.3.1.4 mantenere accessibile l'ultima versione della politica ai fini del riesame e degli audit

9.4 Audit e documentazione

9.4.1 Le registrazioni di tutti i riesami della politica, delle approvazioni all'uso di dati reali e delle relative giustificazioni di eccezione devono essere:

9.4.1.1 conservate in modo sicuro ai fini di audit

9.4.1.2 rese disponibili su richiesta durante audit interni o audit di terze parti

9.4.1.3 riesaminate annualmente per assicurarne la coerenza con le pratiche di test

10. Politiche correlate e collegamenti

10.1 La presente politica deve essere applicata in coordinamento con le seguenti politiche SME al fine di mantenere sicurezza e conformità durante le attività di test:

10.1.1 P2S – Politica sui ruoli e sulle responsabilità di governance: definisce chi è responsabile della supervisione delle attività di sviluppo, test e segregazione dei sistemi.

10.1.2 P4S – Politica di controllo degli accessi: disciplina l'assegnazione, la gestione e la revoca delle credenziali di accesso ai sistemi di test.

10.1.3 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: garantisce che il personale comprenda i rischi relativi ai dati di test, le corrette pratiche di gestione sicura e l'adeguata separazione degli ambienti.

10.1.4 P13S – Politica di classificazione ed etichettatura dei dati: supporta la chiara classificazione dei dati di test e orienta le strategie di anonimizzazione o mascheramento dei dati.

10.1.5 P17S – Politica di protezione dei dati e privacy: si allinea agli obblighi del GDPR, comprese le misure di sicurezza relative al trattamento e alla conservazione dei dati personali, anche negli ambienti di test.

10.1.6 P24S – Politica di sviluppo sicuro: definisce le aspettative generali di sicurezza per i team di sviluppo, incluso l'uso sicuro dei dati durante le fasi di test.

10.1.7 P30S – Politica di risposta agli incidenti: definisce le modalità di risposta a qualsiasi violazione o problematica rilevata in un ambiente di test o causata da una gestione impropria dei dati di test.

10.2 Tali politiche costituiscono un quadro di riferimento unitario per la sicurezza a supporto dell'integrità dei test, della minimizzazione dei dati e del pieno allineamento alla ISO/IEC 27001 nelle attività di sviluppo e garanzia della qualità (QA).

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 6.1 – Richiede azioni di valutazione e trattamento del rischio, inclusi i rischi connessi ai test.

11.1.2 Clausola 8.1 – Richiede la pianificazione e il controllo dei processi operativi, inclusa la predisposizione degli ambienti dei sistemi di test.

11.2 ISO/IEC 27002

11.2.1 Controllo 8.28 – Richiede alle organizzazioni di proteggere i dati di test e di garantire che non contengano dati sensibili o dati reali di produzione.

11.2.2 Controllo 8.29 – Richiede una chiara separazione tra ambienti di sviluppo, test e produzione.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Copre i requisiti di controllo relativi allo sviluppo e ai test.

11.3.2 SA-12 – Riguarda i rischi di test nella catena di fornitura e le valutazioni di sicurezza.

11.3.3 SC-32 – Richiede la separazione degli ambienti e misure di protezione per la riservatezza e l'integrità dei dati di test.

11.4 Regolamento generale sulla protezione dei dati dell'UE (GDPR)

11.4.1 Articolo 5(1)(c) – Richiede la minimizzazione dei dati, incluso l'utilizzo nei test dei soli dati necessari.

11.4.2 Articolo 25 – Richiede la protezione dei dati fin dalla progettazione, che comprende anche i controlli sugli ambienti di test.

11.4.3 Articolo 32 – Richiede il trattamento sicuro dei dati personali in tutti i sistemi, inclusi gli ambienti non di produzione.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(e, h) – Richiede sviluppo sicuro e test dei sistemi, in particolare quando i servizi digitali sono esposti al rischio informatico.

11.6 Regolamento UE DORA (2022/2554)

11.6.1 Articolo 9 – Sottolinea l'importanza della resilienza operativa digitale, inclusi i test sicuri dei sistemi ICT da parte delle PMI del settore finanziario.

11.7 COBIT 2019

11.7.1 BAI07 – Gestire l'accettazione del cambiamento e la transizione: include controlli di test per convalidare i nuovi sistemi e la gestione dei dati.

11.7.2 DSS05 – Gestire i servizi di sicurezza: richiede pratiche di test e sviluppo che prevengano l'uso improprio o l'esposizione dei dati aziendali.