					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P29					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**

Allineata a standard e normative

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Rilevante ai fini della pianificazione e del controllo operativi sicuri dei dati e degli ambienti di test
ISO/IEC 27002:2022	Controlli 8.28–8.29	Copre la protezione dei dati di test e la sicurezza degli ambienti di test
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Riguarda il testing e la valutazione da parte degli sviluppatori, la protezione dei dati a riposo e l'integrità delle informazioni
GDPR UE	Articoli 5, 25, 32	Copre la minimizzazione dei dati, la protezione dei dati fin dalla progettazione e la sicurezza del trattamento nei contesti di test
NIS2 UE	Articolo 21(2)(e), (h)	Riguarda pratiche sicure di sviluppo e test
DORA UE	Articolo 9	Riguarda i sistemi ICT, i protocolli e la sicurezza dei dati di test
COBIT 2019	DSS05, BAI07	Riguarda la gestione dei servizi di sicurezza e l'accettazione/la transizione dei cambiamenti

1. Finalità

1.1. La presente politica definisce i requisiti obbligatori per la gestione degli ambienti di test e dei dati di test, al fine di garantire sicurezza, riservatezza e integrità operativa lungo l'intero ciclo di vita dello sviluppo e del testing del software.

1.2. Mira a prevenire accessi non autorizzati, perdite di dati e contaminazione dei sistemi di produzione derivanti da una gestione impropria degli ambienti di test o dall'uso di dati reali nelle attività di test.

1.3. La politica impone la gestione sicura dei dati utilizzati per il testing, l'hardening dell'infrastruttura di test e il controllo degli accessi basato sui ruoli (RBAC), in conformità agli obblighi normativi e contrattuali applicabili.

2. Ambito di applicazione

2.1. La presente politica si applica a tutti gli ambienti di test, ai dati, agli strumenti e ai processi utilizzati per il testing di software, sistemi, applicazioni e infrastrutture nell'intera organizzazione.

2.2. Comprende:

2.2.1. Ambienti di test predisposti on-premise, nel cloud o tramite piattaforme di terze parti

2.2.2. Dati di test utilizzati in test funzionali, prestazionali, di regressione e di sicurezza

2.2.3. Attività di test manuali, basate su script o automatizzate (ad es. pipeline CI/CD)

2.2.4. Tutto il personale coinvolto nelle attività di test, inclusi team interni, fornitori e collaboratori esterni

2.3. La politica si applica indipendentemente dalla criticità del sistema, dal tipo di applicazione o dal fatto che lo sviluppo sia interno o esternalizzato.

3. Obiettivi

3.1. Prevenire l'uso, negli ambienti di test, di dati in esercizio, dati sensibili o dati soggetti a regolamentazione (ad es. dati personali identificabili, dati dei titolari di carta), salvo che siano anonimizzati o specificamente approvati.

3.2. Garantire una completa segregazione di rete e degli accessi tra ambienti di test e ambienti di produzione, al fine di evitare accessi non autorizzati ai dati o contaminazione dei sistemi.

3.3. Richiedere cifratura, mascheramento dei dati o generazione di dati sintetici quando, ai fini del test, sono necessari dati rappresentativi.

3.4. Ridurre la probabilità di non conformità, esposizione dei dati dei clienti o interruzioni operative derivanti da dati o ambienti di test non sicuri.

3.5. Allineare la gestione dei dati di test agli standard di settore (ISO, NIST, COBIT) e alle normative quali GDPR, NIS2 e DORA.

4. Ruoli e responsabilità

4.1. Responsabile della sicurezza delle informazioni (CISO)

4.1.1. È il titolare della politica e assicura l'attuazione delle misure tecniche e organizzative di sicurezza per i dati e gli ambienti di test.

4.1.2. Approva l'uso di dati reali o sensibili nelle attività di test sulla base di un'adeguata giustificazione e di controlli compensativi.

4.2. Responsabili QA/Test

4.2.1. Coordinano la pianificazione dei test e garantiscono che tutte le attività di test rispettino i requisiti della presente politica.

4.2.2. Convalidano l'adeguata segregazione, gli accessi e la predisposizione dei dati per ciascuna fase di test.

[... 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. La presente politica deve essere riesaminata annualmente e aggiornata, se necessario, per riflettere:

9.1.1. Modifiche dei requisiti normativi (ad es. GDPR, DORA, NIS2)

9.1.2. L'adozione di nuovi strumenti di test, piattaforme o pipeline di automazione

9.1.3. Le risultanze dell'audit interno o le raccomandazioni successive agli incidenti

9.1.4. L'estensione dei processi di sviluppo o QA che modifichino la gestione dei dati di test o l'utilizzo degli ambienti

9.2. Il CISO è responsabile dell'avvio del riesame in collaborazione con:

9.2.1. Responsabili QA/Test

9.2.2. Responsabili DevOps e Infrastruttura

9.2.3. Team di sviluppo applicativo

9.2.4. Responsabile della protezione dei dati (DPO) e consulente legale

9.3. Tutte le revisioni devono essere:

9.3.1. Sottoposte a controllo di versione e conservate nel repository documentale centrale

9.3.2. Comunicate al personale interessato tramite canali formali (ad es. notifiche del SGSI, briefing di team)

9.3.3. Collegate agli aggiornamenti dei relativi standard tecnici, controlli e procedure operative

9.4. Riesami intermedi attivati da eventi specifici devono essere effettuati immediatamente a seguito di qualsiasi:

9.4.1. Perdita di dati o violazione che coinvolga ambienti di test

9.4.2. Non conformità rilevata in audit relativa alla gestione dei dati di test

9.4.3. Modifica significativa degli obblighi legali o dell'architettura IT

10. Politiche correlate e collegamenti

10.1. La presente politica è strettamente integrata con le seguenti politiche, al fine di garantire una gestione sicura e conforme dei dati e degli ambienti di test:

10.1.1. P1 – Politica per la sicurezza delle informazioni: stabilisce i principi generali di sicurezza che disciplinano la protezione dei dati di test e la gestione degli ambienti.

10.1.2. P5 – Politica di gestione dei cambiamenti: si applica alla creazione, all'aggiornamento e alla dismissione degli ambienti di test e delle pipeline di deployment.

10.1.3. P13 – Politica di classificazione ed etichettatura dei dati: guida la selezione dei dati di test e l'applicazione dei controlli in funzione della sensibilità.

10.1.4. P14 – Politica di conservazione e smaltimento dei dati: definisce i tempi di conservazione e i requisiti di smaltimento sicuro per i set di dati di test.

10.1.5. P15 – Politica di backup e ripristino: prescrive le pratiche di backup e la convalida del ripristino per gli ambienti di test.

10.1.6. P18 – Politica sui controlli crittografici: specifica gli standard obbligatori di cifratura per i dati a riposo e i dati in transito all'interno delle piattaforme di test.

10.1.7. P22 – Politica di registrazione e monitoraggio: disciplina la visibilità e il rilevamento delle anomalie nelle attività degli ambienti di test.

10.1.8. P30 – Politica di risposta agli incidenti (P30): definisce l'escalation e le azioni di rimedio per violazioni o incidenti che coinvolgano sistemi di test.

10.1.9. P33 – Politica di monitoraggio dell'audit e della conformità: consente la verifica della conformità alle politiche e il presidio continuo.

11. Standard e quadri di riferimento

11.1. La presente politica è allineata agli standard globali di cybersicurezza e ai quadri normativi che richiedono la gestione sicura dei dati di test e la protezione degli ambienti non di produzione.

11.2. ISO/IEC 27001:

11.2.1. Clausola 8.1 - Richiede pianificazione e controllo operativi sicuri dei dati e degli ambienti di test.

11.3. ISO/IEC 27002:2022 – Controlli 8.28–8.29:

11.3.1. Controllo dell'Allegato A 8.28 – Dati di test sicuri: richiede la protezione dei dati di test utilizzati nelle fasi di sviluppo e test mediante anonimizzazione, mascheramento dei dati o generazione di dati sintetici.

11.3.2. Controllo dell'Allegato A 8.29 – Protezione degli ambienti di test: richiede segregazione dalla produzione, controllo degli accessi e hardening dell'ambiente per i sistemi di test.

11.3.3. Tali controlli definiscono i requisiti per la gestione sicura dei dati utilizzati durante il testing e per la protezione dei sistemi non di produzione da uso improprio, compromissione o contaminazione.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Testing e valutazione degli sviluppatori: stabilisce aspettative per procedure di test sicure e ripetibili, con adeguati controlli sui dati.

11.4.2. SC-28 – Protezione delle informazioni a riposo: è coerente con la cifratura dei dati di test conservati in sistemi non di produzione.

11.4.3. SC-32 – Integrità delle informazioni: supporta la validazione dei dati, la prevenzione della corruzione e i controlli di input/output durante il testing.

11.5. GDPR UE (2016/679):

11.5.1. Articolo 5 – Minimizzazione dei dati: vieta l'uso non necessario di dati personali nelle attività di test.

11.5.2. Articolo 25 – protezione dei dati fin dalla progettazione: richiede che le tecniche di protezione dei dati siano applicate fin dall'inizio del ciclo di sviluppo e test.

11.5.3. Articolo 32 – Sicurezza del trattamento: impone misure di sicurezza per gli ambienti di test che trattano dati personali o sensibili.

11.6. Direttiva UE NIS2 (2022/2555):

11.6.1. Articolo 21(2)(e, h): richiede processi sicuri di sviluppo e testing del software, con enfasi sulla protezione contro accessi non autorizzati e perdite di dati.

11.7. DORA UE (2022/2554):

11.7.1. Articolo 9 – Sistemi e protocolli ICT: richiede che i processi di test supportino la resilienza e proteggano i dati operativi da compromissione o divulgazione non autorizzata.

11.8. COBIT 2019:

11.8.1. DSS05 – Gestire i servizi di sicurezza: supporta l'applicazione delle politiche di sicurezza in tutti gli ambienti, inclusi quelli non di produzione.

11.8.2. BAI07 – Gestire l'accettazione e la transizione dei cambiamenti: copre il processo formale di transizione dal testing alla produzione, inclusi i controlli su dati e ambienti.