					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P39					Titolo del documento: **Politica di divulgazione coordinata delle vulnerabilità**							
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**

Nota legale (diritti d'autore e limitazioni d'uso)

(C) 2025 Clarysec LLC. All rights reserved.

Il presente documento è proprietà intellettuale di Clarysec LLC. Nessuna parte del presente documento può essere copiata, riutilizzata, distribuita o modificata per finalità commerciali o di implementazione senza previa autorizzazione scritta espressa.

L'uso non autorizzato è severamente vietato e può comportare azioni legali.

Per richieste di licenza, contattare: info@clarysec.com

Allineamento a standard e normative applicabili

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
GDPR UE	Art. 32(1)(d)	
NIS2 UE	Art. 21(2)(e)	
DORA UE	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Finalità

1.1 Stabilire un processo formale per la ricezione, la gestione e la divulgazione delle informazioni relative alle vulnerabilità che interessano i sistemi o i servizi dell'organizzazione, come richiesto dall'articolo 21(2)(e) della NIS2 in materia di trattamento e divulgazione delle vulnerabilità.

1.2 Promuovere la segnalazione responsabile delle vulnerabilità da parte di ricercatori di sicurezza esterni, partner e utenti (Coordinated Vulnerability Disclosure - CVD) e definire le modalità con cui l'organizzazione comunica alle parti interessate le informazioni relative alle vulnerabilità.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i sistemi informativi e di rete di proprietà dell'organizzazione o da essa gestiti, nonché a tutte le vulnerabilità identificate in tali sistemi.

2.2 Si applica ai team interni (sicurezza, IT, sviluppo) e a qualsiasi parte esterna che segnali vulnerabilità (ad es. ricercatori, clienti, fornitori). Disciplina inoltre le comunicazioni con i fornitori di prodotti o i prestatori di servizi qualora i loro componenti siano coinvolti nella vulnerabilità.

3. Obiettivi

3.1 Individuare e risolvere tempestivamente le vulnerabilità di sicurezza, facendo leva sia su valutazioni interne sia su segnalazioni esterne.

3.2 Fornire indicazioni chiare ai segnalanti esterni per trasmettere le informazioni sulle vulnerabilità in modo sicuro e lecito, e all'organizzazione per rispondere e porre rimedio in modo efficace.

3.3 Garantire l'allineamento ai requisiti NIS2 e alle buone pratiche di settore (ISO/IEC 29147 e ISO/IEC 30111) per la divulgazione coordinata delle vulnerabilità, migliorando il livello di sicurezza complessivo dell'ecosistema.

4. Ruoli e responsabilità

4.1 Team di risposta alle vulnerabilità (VRT): team designato, guidato dal Responsabile della sicurezza delle informazioni (CISO) o dal Responsabile della gestione delle vulnerabilità, che riceve ed effettua il triage delle segnalazioni di vulnerabilità, valuta rischio e impatto e coordina le azioni di rimedio e la divulgazione pubblica.

4.2 Team IT e di sviluppo: collaborano con il VRT per validare le vulnerabilità segnalate, sviluppare e testare patch o misure di mitigazione e distribuire le correzioni. Forniscono, se necessario, i dettagli tecnici per gli avvisi.

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

9. Monitoraggio e audit

9.1 Il VRT deve mantenere un registro della divulgazione delle vulnerabilità che tracci ciascuna segnalazione dal ricevimento alla chiusura. Tale registro deve essere riesaminato mensilmente per garantire il tempestivo avanzamento degli elementi aperti. Gli elementi scaduti devono essere oggetto di escalation.

9.2 La Funzione di Internal Audit/Compliance o un valutatore di sicurezza indipendente deve riesaminare annualmente l'efficacia del processo di trattamento delle vulnerabilità, verificando ad esempio che campioni di casi siano stati gestiti in conformità alla politica, con presa in carico, correzione e divulgazione tempestive. Deve inoltre verificare che il canale pubblico di divulgazione sia funzionante, ad esempio che e-mail di test siano ricevute e gestite.

9.3 Le metriche sulle vulnerabilità (volumi per gravità, tempi di rimedio, ecc.) devono essere consolidate trimestralmente e presentate al comitato di governance della cibersicurezza per supportare l'aggiornamento delle valutazioni del rischio.

10. Riesame e manutenzione

10.1 La presente politica deve essere riesaminata almeno annualmente. Inoltre, qualsiasi cambiamento significativo del nostro ambiente IT, ad es. l'avvio di un nuovo servizio esposto a Internet, o sviluppi normativi pertinenti, ad es. nuove normative UE sulla divulgazione delle vulnerabilità dei prodotti, attivano un riesame straordinario.

10.2 Gli aggiornamenti della politica devono incorporare il feedback dei segnalanti esterni e le lezioni apprese dalle analisi interne post-incidente. Le modifiche rilevanti devono essere approvate dal CISO, comunicate a tutti i dipendenti e pubblicate nel nostro repository online delle politiche di sicurezza per garantire trasparenza.

11. Politiche correlate e collegamenti

11.1 P01 – Politica per la sicurezza delle informazioni. Mandato della direzione per il trattamento e la divulgazione delle vulnerabilità.

11.2 P19 – Politica di gestione delle vulnerabilità e delle patch. Processo interno di rimedio collegato alla ricezione delle segnalazioni CVD.

11.3 P24 – Politica di sviluppo sicuro. Alimenta le correzioni e il rafforzamento del ciclo di vita di sviluppo sicuro (SDLC) a partire dalle problematiche segnalate.

11.4 P25 – Politica sui requisiti di sicurezza delle applicazioni. Garantisce che i prodotti dispongano di requisiti di sicurezza idonei alla divulgazione.

11.5 P30 – Politica di risposta agli incidenti (P30). Gestisce lo sfruttamento attivo delle vulnerabilità divulgate.

11.6 P31 – Politica per la raccolta delle evidenze e l'analisi forense. Preserva gli artefatti relativi alle vulnerabilità segnalate o sfruttate.

11.7 P26 – Politica di sicurezza dei fornitori e delle terze parti. Coordina le divulgazioni che coinvolgono componenti di fornitori.

11.8 P37 – Politica di conformità legale e regolatoria. Disciplina notifiche, formulazioni di safe harbor e pubblicazione.

12. Riferimenti

12.1 Direttiva NIS2 (UE 2022/2555), articolo 21(2), lettera (e) (sicurezza nello sviluppo e trattamento e divulgazione delle vulnerabilità)

12.2 Regolamento di esecuzione (UE) 2024/2690 della Commissione, allegato, sezione 6.10 (requisiti tecnici sui processi di trattamento e divulgazione delle vulnerabilità)

12.3 Linee guida tecniche ENISA sulle misure di gestione dei rischi di cibersicurezza – sezione sul trattamento e sulla divulgazione delle vulnerabilità

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (controllo A.5.7 sulle informazioni sulle minacce e sulla divulgazione delle vulnerabilità; controllo A.8.28 sullo sviluppo sicuro)

12.5 ISO/IEC 29147:2018 (linee guida per la divulgazione delle vulnerabilità) e ISO/IEC 30111:2019 (linee guida per i processi di trattamento delle vulnerabilità)