Società di riferimento	**APPLIED**
Perimetro di validità	Aziende gruppo Applied
Ambito documento	ISMS COMPL
Codificazione	APPL-COMPL-PL-003
Nome esteso documento	APPL-COMPL-PL-003-Vulnerability Disclosure Policy-v01
Documento	Vulnerability Disclosure Policy
Versione	1 del 14/07/2026
Lingua	Italiano
Approvatore	Comitato Direttivo
Autore	Cyber Security & Compliance Manager
Data di approvazione	14/07/2026
Data Classification	Pubblico

STORIA DELLE REVISIONI

Versione	Data	Autore	Note
0.1	14/07/2026	Cyber Security & Compliance Manager	Creazione del documento
0.1	14/07/2026	Comitato Direttivo	Approvazione del documento

1. Scopo

Applied riconosce l'importanza della collaborazione con clienti, partner, ricercatori di sicurezza e altri soggetti qualificati al fine di migliorare continuamente il livello di sicurezza dei propri prodotti con elementi digitali.

La presente Vulnerability Disclosure Policy (VDP) definisce le modalità attraverso cui eventuali vulnerabilità di sicurezza possono essere segnalate ad Applied e descrive i principi adottati per la loro valutazione, gestione e risoluzione.

La Policy ha l'obiettivo di:

- favorire la tempestiva identificazione delle vulnerabilità;
- promuovere una divulgazione coordinata e responsabile delle vulnerabilità (Coordinated Vulnerability Disclosure - CVD);
- supportare un processo strutturato di gestione delle segnalazioni;
- ridurre i rischi derivanti dall'eventuale sfruttamento delle vulnerabilità;
- contribuire alla conformità ai requisiti applicabili, incluso il Regolamento (UE) 2024/2847 (Cyber Resilience Act).

2. Ambito di applicazione

La presente Policy si applica alle segnalazioni di vulnerabilità riguardanti i prodotti con elementi digitali sviluppati e commercializzati da Applied S.r.l.

Qualora Applied riceva segnalazioni relative a prodotti con elementi digitali sviluppati da produttori terzi e distribuiti dalla Società, tali segnalazioni saranno gestite nel rispetto dei ruoli e delle responsabilità previsti dal Regolamento (UE) 2024/2847 e, ove necessario, condivise con il produttore competente.

La presente Policy non costituisce autorizzazione allo svolgimento di attività di penetration testing, scansioni automatiche o altre attività invasive sui sistemi e sulle infrastrutture di Applied S.r.l.

3. Principi di Responsible Vulnerability Disclosure

Applied promuove un approccio di Responsible Vulnerability Disclosure, incoraggiando la segnalazione tempestiva e responsabile delle vulnerabilità individuate.

I soggetti che effettuano una segnalazione sono invitati ad agire in buona fede e a:

- fornire informazioni accurate e sufficienti per consentire l'analisi della vulnerabilità;
- limitare le attività di verifica allo stretto necessario per dimostrare l'esistenza della vulnerabilità;
- evitare qualsiasi azione che possa compromettere la disponibilità, l'integrità o la riservatezza dei sistemi o dei dati;
- evitare l'accesso intenzionale a dati personali o informazioni riservate;
- mantenere riservate le informazioni tecniche relative alla vulnerabilità fino al completamento delle attività di gestione da parte di Applied o fino a diverso accordo tra le parti.

4. Modalità di segnalazione

Le vulnerabilità devono essere segnalate attraverso il seguente canale dedicato: **cybersecurity@applied.it**

Al fine di consentire una valutazione efficace, la segnalazione dovrebbe includere, ove disponibili:

- descrizione della vulnerabilità;
- prodotto interessato;
- versione del prodotto o del componente coinvolto;
- descrizione dell'impatto potenziale;
- passaggi necessari per riprodurre il problema;
- log, screenshot o altra documentazione tecnica di supporto;
- recapito del segnalante.

Le segnalazioni incomplete potranno richiedere ulteriori informazioni prima di poter essere valutate.

5. Processo di gestione delle vulnerabilità

Applied gestisce le segnalazioni ricevute attraverso un processo documentato di Vulnerability Management.

Ogni segnalazione viene:

- registrata e presa in carico;
- sottoposta a verifica tecnica;
- analizzata per determinarne validità, impatto e livello di rischio;
- classificata secondo criteri di severità appropriati;
- gestita mediante attività correttive o misure di mitigazione;

- monitorata fino alla conclusione del processo.

Le attività svolte e le decisioni adottate sono documentate secondo i processi interni applicabili.

Qualora una vulnerabilità risulti già nota, già risolta o duplicata rispetto a precedenti segnalazioni, Applied potrà chiudere la segnalazione dandone comunicazione al segnalante.

6. Valutazione e trattamento delle vulnerabilità

La valutazione della vulnerabilità tiene conto, tra gli altri elementi, di:

- probabilità di sfruttamento;
- impatto sulla sicurezza del prodotto;
- disponibilità di misure di mitigazione;
- presenza di condizioni che aumentino il rischio;
- dipendenze da componenti o fornitori terzi.

In funzione della valutazione effettuata, Applied potrà adottare una o più delle seguenti misure:

- correzioni software;
- aggiornamenti di sicurezza;
- misure di mitigazione temporanee;
- comunicazioni agli utilizzatori;
- altre misure tecniche o organizzative ritenute appropriate.

7. Divulgazione coordinata

Applied favorisce un processo di Coordinated Vulnerability Disclosure (CVD).

Al fine di proteggere gli utilizzatori dei prodotti e ridurre il rischio di sfruttamento della vulnerabilità, il segnalante è invitato a non divulgare pubblicamente informazioni tecniche relative alla vulnerabilità prima che Applied abbia avuto il tempo ragionevolmente necessario per:

- verificare la segnalazione;
- valutare il rischio associato;
- adottare eventuali misure correttive o di mitigazione;
- informare, ove necessario, gli utilizzatori interessati.

Applied collaborerà, ove possibile, con il segnalante per concordare tempi e modalità dell'eventuale divulgazione pubblica della vulnerabilità.

8. Tempi di gestione

Salvo circostanze eccezionali, Applied si impegna a:

- confermare la ricezione della segnalazione entro 5 giorni lavorativi;
- effettuare una prima valutazione entro 10 giorni lavorativi;
- mantenere aggiornato il segnalante sullo stato della gestione in caso di sviluppi significativi.

I tempi di analisi e risoluzione possono variare in funzione della complessità tecnica della vulnerabilità, della sua gravità e dell'eventuale coinvolgimento di soggetti terzi.

9. Segnalazioni relative a prodotti di terze parti

Nel caso in cui una segnalazione riguardi prodotti con elementi digitali sviluppati da terzi e distribuiti da Applied, la Società procederà alla valutazione della segnalazione nell'ambito del proprio ruolo nella catena di fornitura.

Ove necessario, Applied collaborerà con il produttore interessato condividendo le informazioni strettamente necessarie alla gestione della vulnerabilità, nel rispetto della normativa applicabile e degli eventuali obblighi contrattuali.

10. Attività non consentite

La presente Policy non autorizza lo svolgimento di attività che possano compromettere la sicurezza, la disponibilità o il corretto funzionamento dei prodotti, dei sistemi o delle infrastrutture di Applied.

Il segnalante è invitato a limitare le proprie attività a quanto strettamente necessario per individuare e documentare la vulnerabilità, evitando qualsiasi comportamento che possa arrecare danni ai sistemi, ai dati o agli utilizzatori.

11. Riservatezza e protezione dei dati personali

Applied S.r.l. tratta le informazioni ricevute nell'ambito delle segnalazioni di vulnerabilità nel rispetto dei principi di riservatezza e le utilizza esclusivamente per le finalità connesse alla valutazione, gestione e risoluzione delle vulnerabilità segnalate.

I dati personali eventualmente comunicati nell'ambito della segnalazione sono trattati in conformità al Regolamento (UE) 2016/679 (GDPR) e alla normativa applicabile.

12. Contatti

Le segnalazioni di vulnerabilità di sicurezza devono essere trasmesse al team Cybersecurity di Applied utilizzando il seguente indirizzo di posta elettronica dedicato: **cybersecurity@applied.it**

13. Aggiornamento della Policy

La presente Policy è riesaminata periodicamente e aggiornata, ove necessario, per garantirne l'allineamento alla normativa applicabile, all'evoluzione tecnologica e ai processi interni di Applied S.r.l.

La versione vigente della Policy è resa disponibile attraverso i canali di comunicazione ufficiali della Società.