DAB PUMPS S.p.A.

POLITICA DI COORDINATED VULNERABILITY DISCLOSURE
(CVD POLICY)

Titolo documento	**Politica di Coordinated Vulnerability Disclosure (CVD)**
Codice documento	DAB-IOT-SEC-002
Versione	1.0 — DRAFT FOR REVIEW
Data emissione	Luglio 2026
Classificazione	PUBBLICA — Disponibile su internofpumps.com
Proprietario	DAB PUMPS
Referente CSIRT-IOT	Nominato su piattaforma ACN — Agenzia per la Cybersicurezza Nazionale
Applicabilità	Tutti i prodotti DAB Pumps con elementi digitali e connettività IoT attiva soggetti al CRA
Riferimento normativo	CRA Artt. 13, 14 — Regolamento UE 2024/2847 | EN 40000-1-3 (PRE-2, PRE-4, PRE-5)
Collegamento	Procedura di Triage, Escalation e Notifica — DAB-IOT-SEC-001 v1.2 (documento interno)

Registro delle revisioni

Versione	Data	Autore	Descrizione modifica
1.0	Luglio 2026	FLO / IoT & Smart Solutions Manager	Prima emissione — Draft for Review

1. PREMESSA E SCOPO

DAB Pumps S.p.A. è un produttore italiano di soluzioni di pompaggio con soluzioni digitali integrate. I propri prodotti con elementi digitali connessi (di seguito "prodotti IoT") rientrano nel perimetro di applicazione del Cyber Resilience Act — Regolamento UE 2024/2847 (CRA).

DAB Pumps riconosce l'importanza della ricerca indipendente sulla sicurezza informatica e il valore della collaborazione con la comunità dei ricercatori, degli utenti e degli esperti di sicurezza per identificare e risolvere vulnerabilità nei propri prodotti prima che possano essere sfruttate in modo malevolo.

La presente Politica di Coordinated Vulnerability Disclosure (CVD) definisce:

- le modalità con cui DAB Pumps riceve segnalazioni di vulnerabilità da parte di ricercatori, utenti e soggetti terzi;
- gli impegni che DAB Pumps assume nei confronti di chi segnala una vulnerabilità (tempi di risposta, comunicazione, riconoscimento);
- il processo interno di gestione della vulnerabilità segnalata, incluso il periodo di embargo e le modalità di divulgazione pubblica;
- i canali di comunicazione disponibili e le informazioni di contatto.

La presente policy è pubblicata su internofpumps.com ed è accessibile pubblicamente. È allineata alla Procedura interna di Triage, Escalation e Notifica (DAB-IOT-SEC-001) e ai requisiti del CRA Art. 14, della norma EN 40000-1-3 e degli standard ISO/IEC 29147 e ISO/IEC 30111.

2. AMBITO DI APPLICAZIONE

La presente policy si applica a tutte le vulnerabilità di sicurezza informatica identificate nei prodotti DAB Pumps con elementi digitali e connettività IoT attiva, soggetti al Cyber Resilience Act, inclusi:

- Tutti i prodotti della gamma connessa DAB con architettura IOT
- Infrastruttura digitale associata: cloud H2D DAB, App mobile H2D

Sono esclusi dall'ambito i prodotti DAB privi di connettività di rete diretta o indiretta, o non soggetti al CRA.

Definizione di vulnerabilità (CRA Art. 2)
Ai sensi del CRA, per vulnerabilità si intende una debolezza, suscettibilità o difetto di un prodotto
con elementi digitali che può essere sfruttata da una minaccia informatica.
Una vulnerabilità attivamente sfruttata è una vulnerabilità per la quale esiste evidenza affidabile
che un attore malevolo l'abbia sfruttata in un sistema senza il permesso del proprietario.

3. COME SEGNALARE UNA VULNERABILITÀ

3.1 Canali di segnalazione

DAB Pumps mette a disposizione i seguenti canali per la ricezione di segnalazioni di vulnerabilità:

Canale	**Dettagli**
Form web dedicato	Form 'Security Breach Notification' disponibile su internofpumps.com, canale principale, trasmissione protetta via HTTPS
Email dedicata	dab.consumer.cybersecurity@dabpumps.com per comunicazioni dirette o segnalazioni che richiedono allegati tecnici
Comunicazioni riservate	Per segnalazioni che richiedono particolare riservatezza tecnica, è possibile richiedere via email un canale di comunicazione alternativo. DAB Pumps valuterà la modalità più adeguata caso per caso.

3.2 Informazioni utili da includere nella segnalazione

Per consentire a DAB Pumps di valutare e riprodurre la vulnerabilità nel modo più rapido ed efficace possibile, si raccomanda di includere nella segnalazione le seguenti informazioni (non tutte obbligatorie):

1. Prodotto interessato: nome del prodotto, versione firmware/software, numero di serie se disponibile e ricevuta di acquisto
2. Descrizione della vulnerabilità: tipo di vulnerabilità (es. autenticazione debole, data breach), componente interessato (firmware, cloud, app mobile, comunicazione wireless)
3. Condizioni di riproducibilità: passi necessari per riprodurre il problema, ambiente di test utilizzato
4. Impatto potenziale: valutazione soggettiva dell'impatto (es. accesso non autorizzato, modifica parametri, denial of service)
5. Proof of Concept: se disponibile e se il segnalante ritiene opportuno condividerlo in modo riservato
6. Dati di contatto del segnalante: nome, cognome, email per le comunicazioni di aggiornamento della segnalazione stessa

DAB Pumps si riserva di richiedere informazioni aggiuntive al segnalante qualora quelle fornite non siano sufficienti per completare l'analisi tecnica.

3.3 Cosa NON rientra nell'ambito di questa policy

Non sono oggetto della presente CVD policy:

- Vulnerabilità in prodotti o infrastrutture di terze parti non gestite da DAB Pumps (es. fornitori di componenti, app store, reti dei clienti)
- Segnalazioni di bug funzionali non correlati alla sicurezza informatica, per questi utilizzare i canali di assistenza tecnica ordinari
- Richieste di informazioni commerciali o tecniche non relative a vulnerabilità di sicurezza

4. IMPEGNI DI DAB PUMPS VERSO IL SEGNALANTE

DAB Pumps si impegna a gestire ogni segnalazione in modo professionale, riservato e trasparente, secondo i seguenti impegni:

4.1 Tempi di risposta

Impegno	Tempistica
Acknowledgement — conferma di ricezione con tracking ID univoco (VUL-AAAA-NNN)	Entro 5 giorni lavorativi dalla ricezione della segnalazione
Aggiornamento sull'esito del triage iniziale	Entro 15 giorni lavorativi dalla ricezione
Comunicazione della decisione di remediation	Entro 30 giorni dalla ricezione (salvo complessità eccezionali documentate)
Notifica del rilascio della patch o misura correttiva	Al momento del rilascio, nel rispetto del periodo di embargo
Comunicazione finale di chiusura del caso	Entro 30 giorni dal rilascio della patch

4.2 Riservatezza

- DAB Pumps tratterà con adeguate misure di riservatezza le informazioni tecniche contenute nella segnalazione e ne limiterà la condivisione ai soggetti che abbiano necessità di conoscerle per analizzare, gestire e correggere la vulnerabilità (a titolo esemplificativo fornitori, consulenti e società del gruppo vincolati da obblighi di riservatezza) nonché alle autorità competenti quando previsto dalla legge. Ove ragionevolmente possibile, DAB Pumps informerà preventivamente il segnalante delle comunicazioni a terzi non imposte dalla legge.

- Le informazioni raccolte saranno utilizzate esclusivamente per l'analisi e la risoluzione della vulnerabilità segnalata
- Il nome e i dati di contatto del segnalante saranno trattati nel rispetto del Regolamento UE 2016/679 (GDPR)

4.3 Riconoscimento pubblico

- DAB Pumps è disponibile a riconoscere pubblicamente il contributo del segnalante nel comunicato relativo alla vulnerabilità risolta (es. security advisory, release notes), previo consenso esplicito del segnalante
- Il segnalante può scegliere di essere menzionato con il proprio nome reale, con uno pseudonimo, o di rimanere anonimo
- DAB Pumps non offre attualmente un programma di bug bounty con compensazione economica

4.4 Aggiornamenti continui

DAB Pumps si impegna a mantenere una comunicazione attiva con il segnalante durante l'intero processo di gestione della vulnerabilità, fornendo aggiornamenti sullo stato di avanzamento e avvisando tempestivamente in caso di ritardi rispetto alle tempistiche indicate.

5. PROCESSO DI GESTIONE DELLA VULNERABILITÀ

Le segnalazioni ricevute vengono gestite secondo la Procedura interna di Triage, Escalation e Notifica (DAB-IOT-SEC-001). Di seguito una sintesi del processo dal punto di vista del segnalante:

Fase	Attività DAB	Tempistica	Impegno verso il segnalante
Ricezione	Registrazione segnalazione nel registro vulnerabilità con ID univoco VUL-AAAA-NNN	Immediata	Acknowledgement al segnalante entro 5 giorni lavorativi dalla ricezione con conferma del tracking ID assegnato
Triage	Analisi tecnica preliminare: componente impattato, vettore di attacco, CVSS v3.1, verifica sfruttamento attivo	CRITICA/ALTA: entro 2-4h MEDIA/BASSA: entro 24-72h	Aggiornamento al segnalante sullo stato dell'analisi, se richiesto
Classificazione	Assegnazione severity definitiva e decisione GO/NO-GO escalation CRA Art. 14	Contestuale al triage	Comunicazione dell'esito della valutazione al segnalante
Remediation	Sviluppo patch o workaround; test di qualificazione	CRITICA: 24-48h ALTA: 72h MEDIA: 7 gg BASSA: 14 gg	Aggiornamento al segnalante sulla timeline di rilascio della fix, nel rispetto del periodo di embargo
Rilascio	Distribuzione OTA via cloud DAB; notifica agli utenti; comunicazione pubblica post-embargo	Secondo SLA e periodo di embargo	Notifica al segnalante del rilascio e ringraziamento; possibile menzione pubblica (con consenso del segnalante)
Chiusura	Chiusura record VUL-AAAA-NNN, lessons learned, aggiornamento analisi rischi	Entro 30 gg dal rilascio patch	Comunicazione finale di chiusura al segnalante

Il processo completo è descritto nella Procedura interna DAB-IOT-SEC-001, disponibile su richiesta alle autorità di vigilanza e agli enti di certificazione.

6. PERIODO DI EMBARGO

Il periodo di embargo è l'intervallo di tempo tra la ricezione di una segnalazione e la divulgazione pubblica dei dettagli tecnici della vulnerabilità. Il suo scopo è garantire a DAB Pumps il tempo necessario per sviluppare, testare e distribuire una patch prima che i dettagli tecnici siano resi pubblici, riducendo il rischio di sfruttamento sui dispositivi non ancora aggiornati.

Periodo di embargo — Parametri DAB Pumps

DURATA STANDARD: 30 giorni dalla conferma della vulnerabilità da parte di DAB Pumps.

ESTENSIONE: il periodo può essere esteso su base motivata e concordata con il segnalante, in caso di complessità tecnica della remediation, necessità di coordinamento con fornitori terzi, o necessità di aggiornare componenti hardware che richiedono tempi di produzione più lunghi.

RIDUZIONE: il periodo può essere ridotto o annullato se:
- La vulnerabilità è già pubblicamente nota o attivamente sfruttata
- Il rischio per gli utenti finali è tale da richiedere divulgazione immediata
- DAB Pumps e il segnalante concordano una divulgazione coordinata anticipata

NOTA: il periodo di embargo si applica esclusivamente alla divulgazione pubblica verso clienti, distributori e pubblico generale. NON si applica agli obblighi di notifica alle autorità (ACN/ENISA) previsti dal CRA Art. 14, che decorrono automaticamente dalla conoscenza dell'evento e non possono essere posticipati.

DAB Pumps si impegna a rispettare il periodo di embargo concordato e chiede al segnalante di fare altrettanto. Qualora il segnalante intenda procedere alla divulgazione pubblica prima della scadenza del periodo concordato, è richiesto un preavviso minimo di 7 giorni per consentire a DAB Pumps di accelerare la risposta.

7. OBBLIGHI DI NOTIFICA ALLE AUTORITÀ — CRA ART. 14

Indipendentemente dal processo di CVD e dal periodo di embargo, DAB Pumps è soggetta agli obblighi di notifica obbligatoria alle autorità competenti previsti dal CRA Art. 14, in vigore dall'11 settembre 2026. Tali obblighi hanno priorità assoluta e decorrono automaticamente dal momento della conoscenza dell'evento.

Obblighi di notifica CRA Art. 14 — Non soggetti a embargo

VULNERABILITÀ ATTIVAMENTE SFRUTTATA:
- 24h dalla conoscenza: early warning da trasmettere attraverso la Single Reporting Platform, SRP, gestita da ENISA
- 72h dalla conoscenza: vulnerability notification con natura exploit e misure adottate
- 14 giorni dalla disponibilità della patch: final report

INCIDENTE SEVERO (quando ha o può avere un impatto negativo significativo sulla disponibilità, autenticità, integrità o riservatezza di un prodotto con elementi digitali o dei dati/funzioni da esso trattati; oppure ha causato o è in grado di causare un danno materiale o immateriale a persone fisiche o giuridiche):
- 24h dalla conoscenza: early warning ad ACN + ENISA simultaneamente
- 72h dalla conoscenza: incident notification con valutazione iniziale
- 1 mese dalla notification a 72h: final report

UTENTI FINALI: notifica senza indebito ritardo dalla conoscenza dell'evento.

Il segnalante di una vulnerabilità viene informato quando DAB Pumps procede a una notifica obbligatoria alle autorità, nei limiti consentiti dalla riservatezza dell'operazione.

7.1 Contenuto minimo delle notifiche

In conformità all'Art. 14(2)(a) e (3) del CRA, l'early warning entro 24 ore deve contenere almeno:

- Identificazione del prodotto interessato (nome, versione/i, categoria);

- descrizione sintetica della natura della vulnerabilità o dell'incidente, anche parziale se l'indagine è in corso;
- indicazione dello stato di sfruttamento attivo (confermato/sospetto, con sintesi delle evidenze);
- Stati membri nei quali il prodotto risulta disponibile, ove noti;
- eventuali misure di mitigazione interinali già disponibili;
- tempistica prevista per la notifica successiva (72 ore).

La notifica a 72 ore integra le informazioni con: valutazione iniziale della gravità e dell'impatto, natura dello sfruttamento, e ogni misura correttiva o di mitigazione adottata o pianificata. Il rapporto finale è trasmesso entro 14 giorni dalla disponibilità della patch, oppure entro un mese dalla notifica a 72h per incidenti gravi include la descrizione dettagliata della vulnerabilità, la relativa gravità e il relativo impatto, le informazioni sull'eventuale autore dell'attacco, se disponibili, e i dettagli della misura correttiva rilasciata.

7.2 Decorrenza dei termini

Ai fini del computo dei termini di cui all'Art. 14 del CRA, il momento di "conoscenza dell'evento" coincide con la conferma, da parte del referente o della funzione responsabile individuata nella Procedura DAB-IOT-SEC-001, che la segnalazione ricevuta (o l'evidenza raccolta autonomamente) integra gli estremi di una vulnerabilità attivamente sfruttata o di un incidente severo ai sensi del CRA.

8. REGOLE DI INGAGGIO PER I RICERCATORI

DAB Pumps si impegna a non intraprendere azioni legali nei confronti di ricercatori che segnalano vulnerabilità in buona fede e nel rispetto delle seguenti condizioni:

1. Non causare danni ai sistemi, ai dati o agli utenti di DAB Pumps durante le attività di ricerca
2. Non accedere, modificare o esfiltrare dati di proprietà di DAB Pumps o dei suoi clienti al di là di quanto strettamente necessario per dimostrare l'esistenza della vulnerabilità
3. Non disturbare o degradare i servizi cloud DAB o le funzionalità dei prodotti connessi
4. Non divulgare pubblicamente i dettagli della vulnerabilità prima della scadenza del periodo di embargo concordato
5. Segnalare la vulnerabilità a DAB Pumps prima di qualsiasi divulgazione pubblica (coordinated disclosure)
6. Agire nel rispetto delle leggi applicabili

DAB Pumps si riserva il diritto di non applicare le tutele previste dalla presente policy qualora le attività del segnalante abbiano causato danni intenzionali, , abbiano violato le condizioni sopra indicate o eccedano quanto ragionevolmente necessario per dimostrare la vulnerabilità.

9. CONTATTI E INFORMAZIONI

Informazione	Dettaglio
Canale di segnalazione principale	Form "Security Breach Notification" all'hyperlink: www.internofpumps.com
Email dedicata	dab.consumer.cybersecurity@dabpumps.com
Referente interno	IoT & Smart Solutions Manager — Referente CSIRT-IOT
Registrazione ACN	Referente CSIRT-IOT nominato sulla piattaforma nazionale ACN (Agenzia per la Cybersicurezza Nazionale)
Procedura interna di riferimento	DAB-IOT-SEC-001 — Procedura di Triage, Escalation e Notifica delle Vulnerabilità
Lingua della policy	Italiano (versione principale). Versione in inglese in fase di predisposizione.
Sede legale	DAB Pumps S.p.A. — Via M. Polo 14, 35035 Mestrino (PD), Italia

10. RIFERIMENTI NORMATIVI

- Cyber Resilience Act — Regolamento (UE) 2024/2847NIS2 — Direttiva (UE) 2022/2555; recepimento IT: D.Lgs. 138/2024
- EN 40000-1-3 — Vulnerability handling requirements (PRE-2, PRE-4, PRE-5)
- ISO/IEC 29147:2018 — Vulnerability disclosure
- ISO/IEC 30111:2019 — Vulnerability handling processes
- Regolamento (UE) 2016/679 — GDPR (trattamento dati personali del segnalante)
- ENISA Good Practices for Security of IoT (2019)

11. REVISIONE E AGGIORNAMENTO

La presente policy è soggetta a revisione periodica con cadenza almeno annuale, o in occasione di:

- Modifiche normative che impattano gli obblighi di vulnerability disclosure (CRA, NIS2)
- Aggiornamenti significativi alla Procedura interna DAB-IOT-SEC-001
- Variazioni nei canali di contatto o nell'organizzazione interna responsabile
- Post-mortem di incidenti reali gestiti con questa procedura

La versione aggiornata viene pubblicata su internofpumps.com con indicazione della data di revisione. Le versioni precedenti sono archiviate internamente sul sito SharePoint CRA_Vulnerability_Management.

Nota sulla pubblicazione

Il presente documento è classificato PUBBLICO ed è destinato alla pubblicazione su internofpumps.com.

È il documento di riferimento esterno per la gestione coordinata delle vulnerabilità dei prodotti IoT DAB Pumps.

Il documento interno di processo è DAB-IOT-SEC-001 (classificato CONFIDENZIALE).