					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P39					Τίτλος εγγράφου: **Πολιτική Συντονισμένης Γνωστοποίησης Ευπαθειών**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
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	
ΓΚΠΔ της ΕΕ	Art. 32(1)(d)	
Οδηγία NIS2 της ΕΕ	Art. 21(2)(e)	
Κανονισμός DORA της ΕΕ	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Σκοπός

1.1 Η θέσπιση επίσημης διαδικασίας για τη λήψη, τον χειρισμό και τη γνωστοποίηση πληροφοριών σχετικά με ευπάθειες που επηρεάζουν τα συστήματα ή τις υπηρεσίες του οργανισμού, όπως απαιτείται από το άρθρο 21(2)(e) της Οδηγίας NIS2 της ΕΕ για τον χειρισμό και τη γνωστοποίηση ευπαθειών.

1.2 Η ενθάρρυνση εξωτερικών ερευνητών ασφάλειας, συνεργατών και χρηστών να αναφέρουν ευπάθειες με υπεύθυνο τρόπο (Coordinated Vulnerability Disclosure - CVD) και ο καθορισμός του τρόπου με τον οποίο ο οργανισμός κοινοποιεί πληροφορίες για ευπάθειες στα ενδιαφερόμενα μέρη.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα δικτυακά και πληροφοριακά συστήματα που ανήκουν στον οργανισμό ή τελούν υπό τη διαχείρισή του, καθώς και σε κάθε ευπάθεια που εντοπίζεται στα συστήματα αυτά.

2.2 Καλύπτει τις εσωτερικές ομάδες (ασφάλειας, Πληροφορικής, ανάπτυξης) και κάθε εξωτερικό μέρος που αναφέρει ευπάθειες (π.χ. ερευνητές, πελάτες, προμηθευτές). Ρυθμίζει επίσης την επικοινωνία με προμηθευτές προϊόντων ή παρόχους υπηρεσιών όταν στα εμπλεκόμενα στοιχεία περιλαμβάνονται δικά τους συστατικά ή υπηρεσίες.

3. Στόχοι

3.1 Ο έγκαιρος εντοπισμός και η έγκαιρη αποκατάσταση ευπαθειών ασφάλειας, μέσω τόσο εσωτερικών αξιολογήσεων όσο και εξωτερικών γνωστοποιήσεων.

3.2 Η παροχή σαφών οδηγιών στους εξωτερικούς αναφέροντες για την ασφαλή και νόμιμη υποβολή πληροφοριών ευπάθειας, καθώς και στον οργανισμό για αποτελεσματική απόκριση και αποκατάσταση.

3.3 Η διασφάλιση της ευθυγράμμισης με τις απαιτήσεις της Οδηγίας NIS2 της ΕΕ και με τις βέλτιστες πρακτικές του κλάδου (ISO/IEC 29147 και ISO/IEC 30111) για τη συντονισμένη γνωστοποίηση ευπαθειών, με στόχο την ενίσχυση της συνολικής ασφάλειας του οικοσυστήματος.

4. Ρόλοι και αρμοδιότητες

4.1 Ομάδα Απόκρισης σε Ευπάθειες (VRT): Ορισμένη ομάδα, υπό την ευθύνη του Επικεφαλής Ασφάλειας Πληροφοριών (CISO) ή του Υπεύθυνου Διαχείρισης Ευπαθειών, η οποία παραλαμβάνει και διενεργεί την αρχική αξιολόγηση των αναφορών ευπαθειών, αξιολογεί τον κίνδυνο και τον αντίκτυπο και συντονίζει την αποκατάσταση και τη δημόσια γνωστοποίηση.

4.2 Ομάδες Πληροφορικής και ανάπτυξης: Συνεργάζονται με την VRT για την επικύρωση των αναφερόμενων ευπαθειών, την ανάπτυξη και δοκιμή διορθώσεων ή μετριαστικών μέτρων και την εγκατάσταση των επιδιορθώσεων. Παρέχουν επίσης τεχνικές λεπτομέρειες για ενημερωτικές ανακοινώσεις, όταν απαιτείται.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Παρακολούθηση και έλεγχος

9.1 Η VRT τηρεί αρχείο καταγραφής γνωστοποιήσεων ευπαθειών, το οποίο παρακολουθεί κάθε αναφορά από την παραλαβή έως το κλείσιμό της. Το αρχείο αυτό ανασκοπείται μηνιαίως, ώστε να διασφαλίζεται η έγκαιρη πρόοδος των ανοικτών θεμάτων. Εκκρεμότητες που υπερβαίνουν τις προθεσμίες κλιμακώνονται.

9.2 Ο Εσωτερικός Έλεγχος ή ανεξάρτητος αξιολογητής ασφάλειας ανασκοπεί ετησίως την αποτελεσματικότητα της διαδικασίας χειρισμού ευπαθειών, ελέγχοντας ενδεικτικά ότι δείγματα υποθέσεων ευπαθειών αντιμετωπίστηκαν σύμφωνα με την πολιτική, δηλαδή επιβεβαιώθηκαν, αποκαταστάθηκαν και γνωστοποιήθηκαν έγκαιρα. Επαληθεύει επίσης ότι ο δημόσια προσβάσιμος δίαυλος γνωστοποίησης λειτουργεί, για παράδειγμα ότι λαμβάνονται και διεκπεραιώνονται δοκιμαστικά μηνύματα ηλεκτρονικού ταχυδρομείου.

9.3 Μετρικές σχετικές με τις ευπάθειες, όπως ο όγκος ανά επίπεδο σοβαρότητας και οι χρόνοι αποκατάστασης, συγκεντρώνονται ανά τρίμηνο και παρουσιάζονται στην επιτροπή διακυβέρνησης κυβερνοασφάλειας, ώστε να υποστηρίζουν την επικαιροποίηση της αξιολόγησης κινδύνου.

10. Ανασκόπηση και συντήρηση

10.1 Η παρούσα πολιτική ανασκοπείται τουλάχιστον ετησίως. Επιπρόσθετα, κάθε σημαντική αλλαγή στο περιβάλλον Πληροφορικής του οργανισμού, όπως η θέση σε λειτουργία νέας υπηρεσίας εκτεθειμένης στο διαδίκτυο, ή κάθε σχετική κανονιστική εξέλιξη, όπως νέα ενωσιακή νομοθεσία για τη γνωστοποίηση ευπαθειών προϊόντων, ενεργοποιεί έκτακτη ανασκόπηση εκτός του τακτικού κύκλου.

10.2 Οι επικαιροποιήσεις της πολιτικής ενσωματώνουν ανατροφοδότηση από εξωτερικούς αναφέροντες και διδάγματα από εσωτερικές αναλύσεις μετά από περιστατικά. Σημαντικές αλλαγές εγκρίνονται από τον Επικεφαλής Ασφάλειας Πληροφοριών (CISO), γνωστοποιούνται σε όλους τους εργαζομένους και δημοσιεύονται στο ηλεκτρονικό αποθετήριο πολιτικών ασφάλειας του οργανισμού για λόγους διαφάνειας.

11. Συναφείς πολιτικές και διασυνδέσεις

11.1 P01 – Πολιτική Ασφάλειας Πληροφοριών. Διοικητική κατεύθυνση για τον χειρισμό και τη γνωστοποίηση ευπαθειών.

11.2 P19 – Πολιτική Διαχείρισης Ευπαθειών και Διορθώσεων. Εσωτερική ροή αποκατάστασης που συνδέεται με την παραλαβή αναφορών CVD.

11.3 P24 – Πολιτική Ασφαλούς Ανάπτυξης. Τροφοδοτεί διορθώσεις και σκλήρυνση του Κύκλου Ζωής Ανάπτυξης Λογισμικού (SDLC) από αναφερόμενα ζητήματα.

11.4 P25 – Πολιτική Απαιτήσεων Ασφάλειας Εφαρμογών. Διασφαλίζει ότι τα προϊόντα διαθέτουν απαιτήσεις ασφάλειας κατάλληλες για διαδικασίες γνωστοποίησης.

11.5 P30 – Πολιτική Αντιμετώπισης Περιστατικών. Αντιμετωπίζει ενεργή εκμετάλλευση γνωστοποιημένων ευπαθειών.

11.6 P31 – Πολιτική Συλλογής Τεκμηρίων και Ψηφιακής Εγκληματολογίας. Διαφυλάσσει τεχνουργήματα από αναφερόμενα ή εκμεταλλευόμενα ελαττώματα.

11.7 P26 – Πολιτική Ασφάλειας Τρίτων Μερών και Προμηθευτών. Συντονίζει γνωστοποιήσεις που αφορούν στοιχεία προμηθευτών.

11.8 P37 – Πολιτική Νομικής και Κανονιστικής Συμμόρφωσης. Ρυθμίζει τις γνωστοποιήσεις, τη διατύπωση του ασφαλούς πλαισίου και τη δημοσίευση.

12. Αναφορές

12.1 Οδηγία NIS2 (ΕΕ 2022/2555), άρθρο 21(2), στοιχείο (e) (ασφάλεια στην ανάπτυξη και χειρισμός και γνωστοποίηση ευπαθειών)

12.2 Εκτελεστικός Κανονισμός (ΕΕ) 2024/2690 της Επιτροπής, Παράρτημα, Ενότητα 6.10 (Τεχνικές απαιτήσεις για διαδικασίες χειρισμού και γνωστοποίησης ευπαθειών)

12.3 Τεχνική καθοδήγηση του ENISA για μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας – ενότητα για τον χειρισμό και τη γνωστοποίηση ευπαθειών

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (έλεγχος A.5.7 για πληροφορίες απειλών και γνωστοποίηση ευπαθειών· έλεγχος A.8.28 για ασφαλή ανάπτυξη)

12.5 ISO/IEC 29147:2018 (Κατευθυντήριες γραμμές για γνωστοποίηση ευπαθειών) και ISO/IEC 30111:2019 (Κατευθυντήριες γραμμές για διαδικασίες χειρισμού ευπαθειών)