					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P19					Τίτλος εγγράφου: **Πολιτική Διαχείρισης Ευπαθειών και Ενημερώσεων Ασφαλείας**							
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	Ρήτρα 8	Συστηματική αντιμετώπιση τεχνικών ευπαθειών και διαρκής αποτελεσματικότητα των ελέγχων ασφάλειας.
ISO/IEC 27002:2022	Μέτρα 8.8, 8.9, 5	Οδηγίες εφαρμογής για ενημερώσεις συστημάτων, σαρώσεις ευπαθειών, ακεραιότητα λογισμικού, ασφαλή διαμόρφωση και απογραφή περιουσιακών στοιχείων.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Επιβάλλονται συχνές σαρώσεις, αποκατάσταση αδυναμιών και διαχείριση διαμορφώσεων.
ΓΚΠΔ της ΕΕ	Άρθρο 32, Αιτιολογική σκέψη 49	Τεχνικά μέτρα για άμεση εφαρμογή ενημερώσεων, αντιμετώπιση ευπαθειών και διατήρηση της ασφάλειας.
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(d)	Εντοπισμός, απόκριση και μετριασμός ευπαθειών για υψηλό επίπεδο κυβερνοϋγιεινής.
Κανονισμός DORA της ΕΕ	Άρθρα 8, 10(2)(f)	Έγκαιρη αποκατάσταση ευπαθειών ΤΠΕ και συνεχείς αξιολογήσεις με γνώμονα τις απειλές.
COBIT 2019	DSS05.02, DSS01.03, MEA	Σάρωση, παρακολούθηση και μετριασμός τεχνικών αδυναμιών, παρακολούθηση για εκμετάλλευση και έλεγχος αποτελεσματικότητας, συμπεριλαμβανομένης της κατάστασης ενημερώσεων.

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις υποχρεωτικές απαιτήσεις του οργανισμού για τον εντοπισμό, την ταξινόμηση, την αποκατάσταση και την παρακολούθηση τεχνικών ευπαθειών και σφαλμάτων λογισμικού σε όλα τα πληροφοριακά συστήματα και περιουσιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ).

1.2 Διασφαλίζει ότι όλες οι γνωστές ευπάθειες αξιολογούνται και αντιμετωπίζονται έγκαιρα και βάσει κινδύνου, μέσω συντονισμένης εφαρμογής ενημερώσεων, προσαρμογών παραμέτρων ρύθμισης ή αντισταθμιστικών δικλίδων, σε ευθυγράμμιση με τις επιχειρησιακές ανάγκες και τις υποχρεώσεις συμμόρφωσης.

1.3 Η παρούσα πολιτική υποστηρίζει τη συμμόρφωση με το μέτρο 8.8 του Παραρτήματος Α του ISO/IEC 27001 και τις οδηγίες του ISO/IEC 27002 και καλύπτει κανονιστικές απαιτήσεις των άρθρων 8 του DORA, 21 της NIS2, 32 του ΓΚΠΔ και των περιοχών DSS και APO του COBIT 2019.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα πληροφοριακά συστήματα, τα περιουσιακά στοιχεία και τα περιβάλλοντα που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν δεδομένα τα οποία υπόκεινται στη διακυβέρνηση του ΣΔΑΠ, συμπεριλαμβανομένων των εξής:

2.1.1 Λειτουργικά συστήματα, εφαρμογές, συσκευές δικτύου, υλικολογισμικό, πλατφόρμες υπολογιστικού νέφους, διεπαφές API και λογισμικό τρίτων.

2.1.2 Συστήματα σε ανάπτυξη, προπαραγωγή, παραγωγή, περιβάλλοντα αντιγράφων ασφαλείας και περιβάλλοντα ανάκαμψης από καταστροφή.

2.1.3 Τερματικά σημεία, διακομιστές, συσκευές IoT, υποδομή εικονικοποίησης και εμπορευματοκιβώτια.

2.2 Είναι δεσμευτική για:

2.2.1 Εσωτερικό προσωπικό: διαχειριστές ΤΠ, μηχανικούς συστημάτων, προγραμματιστές εφαρμογών, αναλυτές ασφάλειας και ομάδες υποδομών.

2.2.2 Εξωτερικά μέρη: αναδόχους και παρόχους υπηρεσιών τρίτων, παρόχους διαχειριζόμενων υπηρεσιών (MSP), προμηθευτές λογισμικού και ολοκληρωτές συστημάτων με τεχνικές αρμοδιότητες επί περιουσιακών στοιχείων εντός πεδίου εφαρμογής.

2.3 Η πολιτική καλύπτει ολόκληρο τον κύκλο ζωής διαχείρισης ευπαθειών και ενημερώσεων ασφαλείας, συμπεριλαμβανομένων των εξής:

2.3.1 Σάρωση και εντοπισμός

2.3.2 Ταξινόμηση και ιεράρχηση κινδύνου

2.3.3 Απόκτηση, δοκιμή, εγκατάσταση και επαναφορά ενημερώσεων

2.3.4 Διαχείριση εξαιρέσεων και σχεδιασμός αντισταθμιστικών δικλίδων

2.3.5 Καταγραφή, αναφορά και ιχνηλασιμότητα ελέγχου

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλες οι γνωστές ευπάθειες εντοπίζονται, αξιολογούνται και αποκαθίστανται με τρόπο που ελαχιστοποιεί την έκθεση σε κίνδυνο και ευθυγραμμίζεται με τις επιχειρησιακές προτεραιότητες.

3.2 Να καθιερώνονται συνεπείς διαδικασίες διαχείρισης ευπαθειών σε επίπεδο οργανισμού για σαρώσεις ευπαθειών, ταξινόμηση σοβαρότητας (π.χ. CVSS) και διαχείριση ενημερώσεων ασφαλείας, συμπεριλαμβανομένου του χειρισμού επειγουσών περιπτώσεων και του σχεδιασμού επαναφοράς.

3.3 Να καθίσταται δυνατή η διαχείριση ασφαλούς διαμόρφωσης μέσω ευθυγράμμισης με βασικές γραμμές σκλήρυνσης, πρακτικές ελέγχου αλλαγών και πληροφορίες απειλών σε πραγματικό χρόνο.

3.4 Να παρέχεται μετρήσιμη συμμόρφωση με κανονιστικούς και προτυποποιημένους ελέγχους που αφορούν την ακεραιότητα συστημάτων, την υγιεινή ενημερώσεων και την έγκαιρη αποκατάσταση σφαλμάτων.

3.5 Να ορίζονται υπευθυνότητα και λογοδοσία μεταξύ των ρόλων για ολόκληρο τον κύκλο ζωής διαχείρισης ευπαθειών, διασφαλίζοντας ότι όλα τα ενδιαφερόμενα μέρη ενεργούν εντός καθορισμένων SLA και αναφέρουν μετρήσεις ελέγχων που υπόκεινται σε αναφορά.

3.6 Να ενισχύεται η ετοιμότητα για έλεγχο και να βελτιώνεται η ανθεκτικότητα έναντι αναδυόμενων απειλών, συμπεριλαμβανομένων ευπαθειών μηδενικής ημέρας, ενεργών αλυσίδων εκμετάλλευσης και ανακοινώσεων υψηλής σημασίας από προμηθευτές.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Έχει την κυριότητα της πολιτικής και διασφαλίζει την ενσωμάτωσή της στο ΣΔΑΠ.

4.1.2 Καθορίζει τη διάθεση ανάληψης κινδύνου του οργανισμού και διασφαλίζει την ευθυγράμμιση με κανονιστικές απαιτήσεις και απαιτήσεις ελέγχου.

4.2 Επικεφαλής Διαχείρισης Ευπαθειών / Διευθυντής Λειτουργιών Ασφάλειας

4.2.1 Έχει την εποπτεία των συνολικών λειτουργιών διαχείρισης ευπαθειών και ενημερώσεων ασφαλείας από άκρο σε άκρο.

4.2.2 Συντονίζει προγράμματα σαρώσεων, μοντέλα ιεράρχησης και χρονοδιαγράμματα αποκατάστασης.

4.2.3 Τηρεί το Μητρώο Ευπαθειών και συνεργάζεται για την αξιολόγηση αντισταθμιστικών δικλίδων.

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

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον ετησίως ή σε περίπτωση:

9.1.1 Σημαντικών κανονιστικών επικαιροποιήσεων (π.χ. αλλαγές σε DORA, NIS2)

9.1.2 Αλλαγών σε πλαίσια ιεράρχησης ευπαθειών (π.χ. ενημερώσεις CVSS)

9.1.3 Σημαντικών αλλαγών στο περιβάλλον ΤΠ (π.χ. μεταφορά υπηρεσιών σε περιβάλλον υπολογιστικού νέφους, συνολική αναβάθμιση EDR)

9.1.4 Παραβιάσεων υψηλού προφίλ ή εξωτερικών ειδοποιήσεων που απαιτούν ενίσχυση της πολιτικής

9.2 Οι ανασκοπήσεις πρέπει να διενεργούνται από τον CISO σε συνεργασία με τις Λειτουργίες Ασφάλειας, τη Διαχείριση Κινδύνων και την ηγεσία Υποδομών.

9.3 Οι επικαιροποιήσεις της πολιτικής πρέπει να:

9.3.1 Τεκμηριώνονται στο Μητρώο Εγγράφων του ΣΔΑΠ

9.3.2 Ανασκοπούνται και εγκρίνονται από την Ανώτατη Διοίκηση

9.3.3 Κοινοποιούνται σε όλα τα επηρεαζόμενα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των εκτελούντων την επεξεργασία τρίτων

9.4 Οι ιστορικές εκδόσεις πρέπει να διατηρούνται με ασφαλή τρόπο για σκοπούς ελέγχου και λογοδοσίας.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 - Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει τη συνολική δέσμευση για την προστασία συστημάτων και δεδομένων, η οποία περιλαμβάνει την προληπτική διαχείριση ευπαθειών και τη διασφάλιση της ακεραιότητας του λογισμικού.

10.2 P5 - Πολιτική Διαχείρισης Αλλαγών. Διέπει κάθε εγκατάσταση ενημερώσεων και προσαρμογή παραμέτρων ρύθμισης, απαιτώντας τεκμηρίωση, δοκιμές, έγκριση και διαδικασίες επαναφοράς που συμπληρώνουν τις διαδικασίες αποκατάστασης ευπαθειών.

10.3 P6 - Πολιτική Διαχείρισης Κινδύνων. Υποστηρίζει την ταξινόμηση και την αντιμετώπιση ευπαθειών που δεν έχουν αποκατασταθεί, μέσω δομημένων αξιολογήσεων κινδύνου, ανάλυσης αντικτύπου και διαδικασιών αποδοχής υπολειπόμενου κινδύνου.

10.4 P12 - Πολιτική Διαχείρισης Περιουσιακών Στοιχείων. Διασφαλίζει ότι τα συστήματα καταγράφονται και ταξινομούνται με ακρίβεια, επιτρέποντας συνεπείς σαρώσεις ευπαθειών, ανάθεση κυριότητας και κάλυψη ενημερώσεων σε όλο τον κύκλο ζωής.

10.5 P22 - Πολιτική Καταγραφής και Παρακολούθησης. Καθορίζει απαιτήσεις για τον εντοπισμό συμβάντων και τη δημιουργία διαδρομής ελέγχου. Η παρούσα πολιτική υποστηρίζει την ορατότητα στη δραστηριότητα εφαρμογής ενημερώσεων, στις μη εξουσιοδοτημένες αλλαγές και στις απόπειρες εκμετάλλευσης που στοχεύουν γνωστές ευπάθειες.

10.6 P30 - Πολιτική Αντιμετώπισης Περιστατικών. Καθορίζει πρωτόκολλα κλιμάκωσης και στρατηγικές περιορισμού για ευπάθειες που έχουν αποτελέσει αντικείμενο εκμετάλλευσης, διερευνήσεις παραβιάσεων και διορθωτικές ενέργειες ευθυγραμμισμένες με τους ελέγχους της παρούσας πολιτικής.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001: Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί συστηματική αντιμετώπιση τεχνικών ευπαθειών ώστε να διασφαλίζεται η διαρκής αποτελεσματικότητα των ελέγχων ασφάλειας.

11.2 ISO/IEC 27002:2022 - Μέτρα 8.8, 8.9, 5: Παρέχει οδηγίες εφαρμογής για ενημερώσεις συστημάτων, σαρώσεις ευπαθειών, ακεραιότητα λογισμικού και την ενσωμάτωση με την ασφαλή διαμόρφωση και την απογραφή περιουσιακών στοιχείων.

11.3 NIST SP 800-53 Rev.5: RA-5 - Παρακολούθηση και σάρωση ευπαθειών: Επιβάλλει συχνές σαρώσεις και παρακολούθηση της αποκατάστασης. SI-2 - Αποκατάσταση σφαλμάτων: Απαιτεί άμεση αξιολόγηση και μετριασμό σφαλμάτων με διαθέσιμες ενημερώσεις ή άλλες ενέργειες. CM-2 / CM-6 - Βασικές γραμμές και έλεγχοι διαχείρισης διαμορφώσεων: Θεμελιώνει τις ασφαλείς διαμορφώσεις συστημάτων που συνδέονται με την εφαρμογή ενημερώσεων.

11.4 ΓΚΠΔ της ΕΕ (2016/679): Άρθρο 32 - Ασφάλεια της επεξεργασίας: Απαιτεί την εφαρμογή κατάλληλων τεχνικών μέτρων, όπως η άμεση εφαρμογή ενημερώσεων και η αντιμετώπιση ευπαθειών, ώστε να διασφαλίζονται η εμπιστευτικότητα και η ανθεκτικότητα των συστημάτων. Αιτιολογική σκέψη 49: Ενθαρρύνει τους οργανισμούς να εφαρμόζουν προληπτικούς ελέγχους έναντι γνωστών απειλών για την υποστήριξη της ασφάλειας και της συνέχειας.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555): Άρθρο 21(2)(d): Υποχρεώνει τους ουσιώδεις και σημαντικούς φορείς να εντοπίζουν, να αποκρίνονται και να μετριάζουν ευπάθειες συστημάτων και να διατηρούν υψηλό επίπεδο κυβερνοϋγιεινής.

11.6 Κανονισμός DORA της ΕΕ (2022/2554): Άρθρο 8 - Διαχείριση κινδύνων ΤΠΕ: Απαιτεί τον εντοπισμό και την έγκαιρη αποκατάσταση ευπαθειών στις τεχνολογίες πληροφοριών και επικοινωνιών που χρησιμοποιούνται σε χρηματοοικονομικά συστήματα. Άρθρο 10(2)(f): Τονίζει τις συνεχείς αξιολογήσεις ευπαθειών και την εφαρμογή ενημερώσεων με γνώμονα τις απειλές ως μέρος της λειτουργικής ανθεκτικότητας.

11.7 COBIT 2019: DSS05.02 - Διαχείριση ευπαθειών ασφάλειας: Κατευθύνει τους οργανισμούς να σαρώνουν, να παρακολουθούν και να μετριάζουν γνωστές τεχνικές αδυναμίες. DSS01.03 - Παρακολούθηση υποδομών: Διασφαλίζει ότι τα συστήματα παρακολουθούνται για ενδείξεις εκμετάλλευσης ή αδυναμίας. MEA03 - Παρακολούθηση, αξιολόγηση και εκτίμηση συμμόρφωσης: Απαιτεί τακτικό έλεγχο της αποτελεσματικότητας των ελέγχων, συμπεριλαμβανομένης της κατάστασης ενημερώσεων και του χειρισμού εξαιρέσεων.