					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P19S					Τίτλος εγγράφου: **Πολιτική Διαχείρισης Ευπαθειών και Διορθώσεων P19S**							
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	
ISO/IEC 27002:2022	Έλεγχοι 8.8, 8.9	
NIST SP 800-53 Αναθ. 5	RA-5, SI-2, CM-2	
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(d), 21(2)(e)	
Κανονισμός DORA της ΕΕ	Άρθρα 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
ΓΚΠΔ της ΕΕ	Άρθρο 32(1)(β)	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο ο οργανισμός εντοπίζει, αξιολογεί και μετριάζει τις ευπάθειες σε συστήματα, εφαρμογές και στην υποδομή πληροφορικής.

1.2 Σκοπός της είναι η μείωση του κινδύνου κυβερνοασφάλειας μέσω της έγκαιρης εφαρμογής διορθώσεων και πρακτικών αποκατάστασης βάσει κινδύνου, κατάλληλων για μικρές και μεσαίες επιχειρήσεις (ΜΜΕ).

1.3 Η παρούσα πολιτική υποστηρίζει τη συμμόρφωση με το ISO/IEC 27001:2022 και συμβάλλει στην εκπλήρωση κανονιστικών υποχρεώσεων βάσει του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ και του Κανονισμού DORA της ΕΕ, απαιτώντας την προληπτική διαχείριση τεχνικών ευπαθειών.

1.4 Ο οργανισμός αναγνωρίζει ότι τα μη ενημερωμένα συστήματα συνιστούν σημαντική απειλή για την ασφάλεια των πληροφοριών και πρέπει να αντιμετωπίζονται συστηματικά και χωρίς καθυστέρηση.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλους τους διακομιστές, σταθμούς εργασίας, φορητούς υπολογιστές, κινητές συσκευές, δικτυακό εξοπλισμό και πλατφόρμες υπολογιστικού νέφους που χρησιμοποιούνται από τον οργανισμό

2.1.2 Όλα τα λειτουργικά συστήματα, το λογισμικό τρίτων, τα πρόσθετα και τις εφαρμογές που χρησιμοποιούνται στις επιχειρησιακές λειτουργίες

2.1.3 Το εσωτερικό προσωπικό πληροφορικής ή τους εξωτερικούς παρόχους υπηρεσιών που είναι υπεύθυνοι για τη συντήρηση συστημάτων, τις ενημερώσεις ή την παρακολούθηση

2.1.4 Κάθε κώδικα προσαρμοσμένης ανάπτυξης ή ενσωματωμένο λογισμικό που συντηρείται από ή για λογαριασμό του οργανισμού

2.2 Η πολιτική καλύπτει τόσο την υποδομή πληροφορικής που διαχειρίζεται άμεσα ο οργανισμός όσο και τα συστήματα που διαχειρίζονται συμβεβλημένοι προμηθευτές ή πάροχοι φιλοξενίας.

3. Στόχοι

3.1 Έγκαιρος και συνεπής εντοπισμός και αξιολόγηση γνωστών ευπαθειών σε όλα τα περιουσιακά στοιχεία πληροφορικής

3.2 Εφαρμογή διορθώσεων και ενημερώσεων λογισμικού βάσει της σοβαρότητας και του κινδύνου για τις λειτουργίες του οργανισμού ή για δεδομένα προσωπικού χαρακτήρα

3.3 Πρόληψη της εκμετάλλευσης τεχνικών αδυναμιών που θα μπορούσαν να οδηγήσουν σε διακοπή υπηρεσιών, παραβίαση δεδομένων ή κανονιστική μη συμμόρφωση

3.4 Διατήρηση ακριβών αρχείων για τις εφαρμοσμένες διορθώσεις, τα εκκρεμή ζητήματα και τις εξαιρέσεις, ώστε να διασφαλίζεται η ετοιμότητα για έλεγχο

3.5 Χρήση εργαλείων και διαδικασιών κατάλληλων για το μέγεθος και την επιχειρησιακή πολυπλοκότητα του οργανισμού, χωρίς συμβιβασμό ως προς την αποτελεσματικότητα

3.6 Υποστήριξη της νομικής και κανονιστικής συμμόρφωσης, συμπεριλαμβανομένου του Άρθρου 32 του ΓΚΠΔ και του Ελέγχου 8 του Παραρτήματος Α του ISO

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής

4.1.1 Έχει τη συνολική ευθύνη για τη διασφάλιση της υλοποίησης δραστηριοτήτων διαχείρισης διορθώσεων και ευπαθειών

4.1.2 Εγκρίνει εξαιρέσεις κινδύνου όταν δεν είναι δυνατή η εφαρμογή διορθώσεων και ανασκοπεί τις σχετικές στρατηγικές μετριασμού

4.1.3 Ανασκοπεί τις αναφορές κατάστασης διορθώσεων και διασφαλίζει τη διαθεσιμότητα των αναγκαίων πόρων για την εκπλήρωση των σχετικών υποχρεώσεων

4.2 Πάροχος Υποστήριξης Πληροφορικής / Εσωτερικός Διαχειριστής Πληροφορικής

4.2.1 Παρακολουθεί τα συστήματα για ευπάθειες και διαθέσιμες διορθώσεις μέσω ειδοποιήσεων προμηθευτών, ενημερώσεων απειλών και ειδοποιήσεων σε επίπεδο λειτουργικού συστήματος

4.2.2 Εφαρμόζει ενημερώσεις λειτουργικού συστήματος, υλικολογισμικού και εφαρμογών εντός των καθορισμένων χρονικών ορίων

4.2.3 Τηρεί επίσημο αρχείο καταγραφής διορθώσεων και τεκμηριώνει τις μη επιλυθείσες ή αναβληθείσες ενημερώσεις

4.2.4 Διενεργεί δοκιμές και προγραμματισμό κρίσιμων ενημερώσεων ώστε να ελαχιστοποιείται η επιχειρησιακή διαταραχή

[... 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 Ετήσια ανασκόπηση

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον Γενικό Διευθυντή, με συνεισφορά από τον Πάροχο Πληροφορικής και τον Συντονιστή Ιδιωτικότητας

9.2 Εναύσματα ανασκόπησης

9.2.1 Ενδιάμεσες ανασκοπήσεις πρέπει να πραγματοποιούνται εάν:

9.2.1.1 Μια σοβαρή ευπάθεια ή εκμετάλλευση επηρεάζει συστήματα εντός του πεδίου εφαρμογής

9.2.1.2 Προκύπτουν σημαντικές αλλαγές σε συστήματα ή λογισμικό

9.2.1.3 Έλεγχος εντοπίσει κενά στις διαδικασίες εφαρμογής διορθώσεων

9.2.1.4 Καταγραφεί περιστατικό ή παραβίαση που σχετίζεται με τη διαχείριση διορθώσεων

9.3 Έλεγχος εκδόσεων πολιτικής

9.3.1 Όλες οι επικαιροποιήσεις πρέπει να καταγράφονται σε αρχείο εκδόσεων με σύνοψη των αλλαγών

9.3.2 Οι αλλαγές πρέπει να γνωστοποιούνται στο επηρεαζόμενο προσωπικό

9.3.3 Οι παρωχημένες εκδόσεις πρέπει να αρχειοθετούνται με περιορισμένη πρόσβαση

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζει και εξαρτάται από αρκετές άλλες πολιτικές ΜΜΕ:

10.1.1 P12S – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Προσδιορίζει την κυριότητα και την ταξινόμηση συστημάτων, διασφαλίζοντας ότι όλα τα περιουσιακά στοιχεία που απαιτούν εφαρμογή διορθώσεων είναι καταγεγραμμένα και αποτυπωμένα στο αποθετήριο

10.1.2 P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Διασφαλίζει ότι τα συστήματα που έχουν προγραμματιστεί για παροπλισμό ενημερώνονται με ασφάλεια ή υποβάλλονται σε διαγραφή, μειώνοντας την έκθεση σε ευπάθειες

10.1.3 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Δίνει προτεραιότητα στην αποκατάσταση ευπαθειών για συστήματα που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, ώστε να διασφαλίζεται η συμμόρφωση με τη νομοθεσία περί ιδιωτικότητας

10.1.4 P22S – Πολιτική Καταγραφής και Παρακολούθησης: Υποστηρίζει τον εντοπισμό συστημάτων χωρίς εφαρμοσμένες διορθώσεις ή ύποπτων συμπεριφορών που ενδέχεται να υποδεικνύουν εκμετάλλευση ευπάθειας

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Καθορίζει διαδικασίες για την απόκριση σε ευπάθειες που οδηγούν σε περιστατικά ασφάλειας, συμπεριλαμβανομένων βημάτων κλιμάκωσης και αναφοράς

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 8.1 – Απαιτεί την εφαρμογή ελέγχων για την αντιμετώπιση του λειτουργικού κινδύνου, συμπεριλαμβανομένης της διαχείρισης ευπαθειών

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 8.8 – Καθορίζει διαδικασίες για τη σάρωση και τη διόρθωση γνωστών αδυναμιών σε συστήματα

11.2.2 Έλεγχος 8.9 – Δίνει έμφαση στην ασφαλή διαμόρφωση, την επικύρωση διορθώσεων και τον έλεγχο αλλαγών, ώστε να αποφεύγεται νέα έκθεση σε κίνδυνο κατά τις ενημερώσεις

11.3 NIST SP 800-53 Αναθ. 5

11.3.1 RA-5 – Απαιτεί τον εντοπισμό ευπαθειών και την αποκατάστασή τους εντός καθορισμένων χρονικών ορίων

11.3.2 SI-2 – Απαιτεί την άμεση εφαρμογή διορθώσεων και ενημερώσεων βάσει σοβαρότητας

11.3.3 CM-2 – Διέπει τις βασικές γραμμές ρυθμίσεων συστημάτων και την τεκμηρίωση ενημερώσεων ώστε να διασφαλίζονται συνεπείς προστασίες

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 32(1)(β) – Απαιτεί από τους οργανισμούς να εφαρμόζουν κατάλληλα τεχνικά μέτρα, συμπεριλαμβανομένης της εφαρμογής διορθώσεων, για τη διατήρηση της ασφάλειας της επεξεργασίας

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(d) – Απαιτεί τη διαχείριση ευπαθειών μέσω συστηματικής σάρωσης και αποκατάστασης

11.5.2 Άρθρο 21(2)(e) – Επιβάλλει την ασφαλή διαμόρφωση και τη διαχείριση διορθώσεων για τη διασφάλιση της ανθεκτικότητας των ΤΠΕ

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 8(1) – Απαιτεί τον εντοπισμό και τον μετριασμό κινδύνων ΤΠΕ, συμπεριλαμβανομένων τεχνικών ευπαθειών

11.6.2 Άρθρο 10(2) – Επιβάλλει στις χρηματοοικονομικές οντότητες να αποκαθιστούν αδυναμίες που επηρεάζουν συστήματα και λειτουργίες ΤΠΕ

11.7 COBIT 2019

11.7.1 DSS05.02 – Απαιτεί την αντιμετώπιση γνωστών τεχνικών ευπαθειών για τη διατήρηση ασφαλών λειτουργιών

11.7.2 APO12.01 – Ευθυγραμμίζει τη διαχείριση κινδύνων με την προληπτική παρακολούθηση και διόρθωση αδυναμιών συστημάτων