					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P25					Τίτλος εγγράφου: **Πολιτική Απαιτήσεων Ασφάλειας Εφαρμογών**							
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	Clause 8	—
ISO/IEC 27002:2022	Controls 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
ΓΚΠΔ της ΕΕ	Articles 25, 32	—
Οδηγία NIS2 της ΕΕ	Articles 21(2)(f), 23	—
Κανονισμός DORA της ΕΕ	Articles 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικές απαιτήσεις ασφάλειας σε επίπεδο εφαρμογής για λογισμικό που αναπτύσσεται, αποκτάται, ενσωματώνεται ή εγκαθίσταται από τον οργανισμό. Διασφαλίζει ότι όλες οι εφαρμογές σχεδιάζονται, υλοποιούνται και συντηρούνται σύμφωνα με τις αρχές της ασφαλούς ανάπτυξης, τις κανονιστικές υποχρεώσεις και τη διάθεση ανάληψης κινδύνου του οργανισμού.

1.2 Η πολιτική επιβάλλει την ενσωμάτωση της ασφάλειας σε όλο τον κύκλο ζωής των εφαρμογών, καλύπτοντας την αυθεντικοποίηση χρηστών, τις πρακτικές διαχείρισης δεδομένων, την προστασία διεπαφών και την ασφαλή αλληλεπίδραση με API ή υπηρεσίες.

1.3 Με την υιοθέτηση της παρούσας πολιτικής, ο οργανισμός αποσκοπεί στην αποτροπή της εισαγωγής ευπαθειών λογισμικού, στην προστασία ευαίσθητων πληροφοριών και στη διασφάλιση ιχνηλασιμότητας και ανθεκτικότητας έναντι εκμετάλλευσης και κακόβουλης χρήσης.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα ακόλουθα:

2.1.1 Εφαρμογές που αναπτύσσονται εσωτερικά ή προέρχονται από εξωτερικές πηγές, συμπεριλαμβανομένων λύσεων SaaS και εργαλείων κατά παραγγελία

2.1.2 Εφαρμογές που υποστηρίζουν κρίσιμες επιχειρησιακές λειτουργίες, πρόσβαση πελατών ή επεξεργασία ρυθμιζόμενων δεδομένων

2.1.3 Ομάδες ανάπτυξης, DevOps, QA, διαχείρισης προϊόντος και ασφάλειας

2.1.4 Τρίτους προγραμματιστές, προμηθευτές λογισμικού και συνεργάτες ενσωμάτωσης με πρόσβαση σε εφαρμογές ή API του οργανισμού

2.2 Εφαρμόζεται σε όλα τα περιβάλλοντα: ανάπτυξης, δοκιμών, προπαραγωγής, παραγωγής και αποκατάστασης καταστροφών, ανεξαρτήτως εάν φιλοξενούνται εντός εγκαταστάσεων, σε ιδιωτικά κέντρα δεδομένων ή σε περιβάλλοντα νέφους.

3. Στόχοι

3.1 Να καθοριστούν βασικές λειτουργικές και μη λειτουργικές απαιτήσεις ασφάλειας που πρέπει να πληρούνται από όλες τις εφαρμογές, ανεξαρτήτως μεθόδου ανάπτυξης ή τεχνολογικής στοίβας.

3.2 Να διασφαλιστεί η ενσωμάτωση μηχανισμών προστασίας σε επίπεδο εφαρμογής, συμπεριλαμβανομένων της επικύρωσης εισόδου, της κωδικοποίησης εξόδου, του χειρισμού σφαλμάτων και της ασφάλειας συνεδριών.

3.3 Να απαιτείται η ασφαλής υλοποίηση μηχανισμών αυθεντικοποίησης, εξουσιοδότησης και ελέγχου πρόσβασης, ευθυγραμμισμένων με τις πολιτικές διαχείρισης ταυτοτήτων και πρόσβασης του οργανισμού.

3.4 Να επιβάλλεται η ασφαλής αλληλεπίδραση με API, διαδικτυακές διεπαφές και συστατικά τρίτων μέσω εγκεκριμένων πρωτοκόλλων και ελέγχων ασφάλειας.

3.5 Να καθίσταται δυνατός ο έγκαιρος εντοπισμός και ο μετριασμός ευπαθειών μέσω στατικής και δυναμικής ανάλυσης, ανασκόπησης κώδικα και μοντελοποίησης απειλών.

3.6 Να προστατεύονται ευαίσθητες πληροφορίες σε συμμόρφωση με τις κανονιστικές απαιτήσεις, μέσω της επιβολής κρυπτογράφησης, ταξινόμησης και ορθολογικής διατήρησης δεδομένων.

3.7 Να διασφαλίζεται η συνεχής επικύρωση της στάσης κινδύνου των εφαρμογών μετά την εγκατάσταση, μέσω δοκιμών, παρακολούθησης και ετοιμότητας για έλεγχο.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει την ευθυγράμμισή της με τη στρατηγική ασφάλειας πληροφοριών και τη στάση κινδύνου του οργανισμού.

4.1.2 Εγκρίνει τις απαιτήσεις ασφάλειας εφαρμογών και διασφαλίζει την εφαρμογή υποχρεωτικών ελέγχων στις λειτουργίες ανάπτυξης και προμήθειας.

4.2 Επικεφαλής Ασφάλειας Εφαρμογών / Διευθυντής DevSecOps

4.2.1 Καθορίζει τις βασικές γραμμές ελέγχου ασφάλειας και τις μεθοδολογίες δοκιμών για τα συστατικά των εφαρμογών.

4.2.2 Ασκεί εποπτεία στην ασφαλή ενσωμάτωση εργαλείων όπως SAST, DAST, IAST και SCA στην αλυσίδα παράδοσης λογισμικού.

4.2.3 Τηρεί τον Κατάλογο Ελέγχου Απαιτήσεων Ασφάλειας Εφαρμογών και τα κριτήρια επικύρωσης.

[... 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 ετησίως ή συχνότερα σε απόκριση σε:

9.1.1 Κρίσιμες ανακοινώσεις ευπαθειών που επηρεάζουν κοινά πλαίσια ανάπτυξης ή εξαρτήσεις

9.1.2 Επικαιροποιήσεις κανονιστικών υποχρεώσεων για την ασφάλεια εφαρμογών, όπως η Οδηγία NIS2 της ΕΕ και ο Κανονισμός DORA της ΕΕ

9.1.3 Μείζονες αλλαγές στις πρακτικές ανάπτυξης λογισμικού, στα εργαλεία ή στην αρχιτεκτονική νέφους του οργανισμού

9.1.4 Ευρήματα από εσωτερικούς ελέγχους ή εξωτερικές δοκιμές διείσδυσης

9.2 Η ανασκόπηση διενεργείται από τον Επικεφαλής Ασφάλειας Εφαρμογών, σε συντονισμό με τον CISO, την τεχνική ηγεσία DevOps, τη Νομική Υπηρεσία, τη λειτουργία προμηθειών και την ηγεσία QA.

9.3 Όλες οι αναθεωρήσεις πρέπει να υπάγονται σε έλεγχο εκδόσεων στο Μητρώο Ελέγχου Εγγράφων του ISMS και να κοινοποιούνται σε όλες τις επηρεαζόμενες ομάδες ανάπτυξης και διαχείρισης προϊόντος.

9.4 Οι εκδόσεις που έχουν αντικατασταθεί πρέπει να αρχειοθετούνται για τουλάχιστον τρία έτη για σκοπούς ιχνηλασιμότητας, ελεγκτικής τεκμηρίωσης και υποστήριξης διερεύνησης παραβιάσεων.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 – Πολιτική Ασφάλειας Πληροφοριών. Θέτει το θεμέλιο για την προστασία συστημάτων και δεδομένων, στο πλαίσιο του οποίου απαιτούνται έλεγχοι σε επίπεδο εφαρμογής για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, διαρροής δεδομένων και εκμετάλλευσης.

10.2 P4 – Πολιτική Ελέγχου Πρόσβασης. Καθορίζει τα πρότυπα διαχείρισης ταυτότητας και συνεδριών που πρέπει να εφαρμόζονται από όλες τις εφαρμογές, συμπεριλαμβανομένων της ισχυρής αυθεντικοποίησης, του ελάχιστου προνομίου και των απαιτήσεων αναθεώρησης δικαιωμάτων πρόσβασης.

10.3 P5 – Πολιτική Διαχείρισης Αλλαγών. Ρυθμίζει την προώθηση κώδικα εφαρμογών και ρυθμίσεων παραμέτρων σε περιβάλλοντα παραγωγής, διασφαλίζοντας ότι αποκλείονται μη εξουσιοδοτημένες ή μη δοκιμασμένες αλλαγές.

10.4 P17 – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας. Απαιτεί από τις εφαρμογές να υλοποιούν προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό και να διασφαλίζουν τον νόμιμο χειρισμό, την κρυπτογράφηση και τη διατήρηση δεδομένων προσωπικού χαρακτήρα και ευαίσθητων δεδομένων σε όλα τα περιβάλλοντα.

10.5 P24 – Πολιτική Ασφαλούς Ανάπτυξης. Παρέχει το ευρύτερο πλαίσιο για την ενσωμάτωση της ασφάλειας στον κύκλο ζωής ανάπτυξης λογισμικού (SDLC), του οποίου η παρούσα πολιτική καθορίζει τις συγκεκριμένες απαιτήσεις και τους τεχνικούς ελέγχους που πρέπει να εφαρμόζονται σε επίπεδο εφαρμογής.

10.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών. Επιβάλλει δομημένο χειρισμό περιστατικών ασφάλειας εφαρμογών, συμπεριλαμβανομένων ευπαθειών που εντοπίζονται μετά την εγκατάσταση ή κατά τη διάρκεια δοκιμών διείσδυσης, και περιγράφει διαδικασίες κλιμάκωσης, περιορισμού και αποκατάστασης.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001:2022

11.1.1 Ρήτρα 8.1 – Επιχειρησιακός Σχεδιασμός και Έλεγχος: Απαιτεί η ασφάλεια εφαρμογών να ενσωματώνεται σε διεργασίες και συστήματα ώστε να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

11.2 ISO/IEC 27002:2022

11.2.1 Οι έλεγχοι 8.25–8.26 περιγράφουν τις προσδοκίες για την ασφάλεια σε επίπεδο εφαρμογής, συμπεριλαμβανομένων πρακτικών ασφαλούς κωδικοποίησης, μοντελοποίησης απειλών, αρχιτεκτονικών ελέγχων και επικύρωσης λογισμικού τρίτων.

11.2.2 Παράρτημα Α, Έλεγχος 8.25 – Κύκλος Ζωής Ασφαλούς Ανάπτυξης: Επιβάλλει την ενσωμάτωση της ασφάλειας σε όλο τον κύκλο ζωής των εφαρμογών.

11.2.3 Παράρτημα Α, Έλεγχος 8.26 – Απαιτήσεις Ασφάλειας Εφαρμογών: Επιβάλλει τον καθορισμό και την εφαρμογή τεχνικών ελέγχων για την προστασία των εφαρμογών από κακή χρήση και παραβίαση της ασφάλειας.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Developer Security Testing and Evaluation: Επιβάλλει στατικές, δυναμικές δοκιμές και δοκιμές διείσδυσης κατά την ανάπτυξη.

11.3.2 SA-15 – Development Process, Standards, and Tools: Καθιερώνει επίσημα πρότυπα για την ασφαλή ανάπτυξη εφαρμογών.

11.3.3 SI-10 – Information Input Validation: Απαιτεί μηχανισμούς ελέγχου για την αποτροπή επιθέσεων έγχυσης και σφαλμάτων ανάλυσης συντακτικού.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 25 – Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού: Απαιτεί την ενσωμάτωση της προστασίας δεδομένων και της ιδιωτικότητας στη λογική και στις ροές εργασίας των εφαρμογών.

11.4.2 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Επιβάλλει κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως επικύρωση εισόδου, κρυπτογράφηση και ασφαλείς έλεγχοι πρόσβασης.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(f): Απαιτεί χειρισμό ευπαθειών και πρακτικές ασφαλούς κύκλου ζωής εφαρμογών για ουσιώδεις και σημαντικές οντότητες.

11.5.2 Άρθρο 23 – Αναφορά περιστατικών ασφάλειας: Καθιστά αναγκαίες δυνατότητες καταγραφής και παρακολούθησης σε επίπεδο εφαρμογής για τον εντοπισμό και την αναφορά σημαντικών περιστατικών.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 9 – Διαχείριση κινδύνων ΤΠΕ: Υποχρεώνει τις χρηματοοικονομικές οντότητες να διασφαλίζουν ότι οι εφαρμογές είναι ασφαλείς, ελεγμένες και ανθεκτικές σε κυβερνοαπειλές.

11.6.2 Άρθρο 11 – Δοκιμές εργαλείων ΤΠΕ: Ενθαρρύνει την περιοδική διενέργεια δοκιμών διείσδυσης και ασκήσεων red team σε κρίσιμες εφαρμογές και υπηρεσίες.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build: Καθιερώνει απαιτήσεις σχεδιασμού και ελέγχου κατά την ανάπτυξη εφαρμογών.

11.7.2 BAI09 – Manage Applications: Δίνει έμφαση στην ασφαλή συντήρηση, παρακολούθηση και βελτίωση εφαρμογών σε λειτουργία.

11.7.3 DSS05 – Manage Security Services: Συνδέει την προστασία εφαρμογών με τις ευρύτερες λειτουργίες και τους ελέγχους ασφάλειας του οργανισμού.