					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P24					Τίτλος εγγράφου: **Πολιτική Ασφαλούς Ανάπτυξης**							
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**

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικές απαιτήσεις ασφάλειας για τις δραστηριότητες ανάπτυξης λογισμικού και συστημάτων εντός του οργανισμού, συμπεριλαμβανομένων των εσωτερικών έργων, της εξωτερικής ανάθεσης ανάπτυξης και της ενσωμάτωσης κώδικα τρίτων μερών.

1.2 Στόχος είναι να διασφαλίζεται ότι η ασφάλεια ενσωματώνεται σε ολόκληρο τον Κύκλο Ζωής Ανάπτυξης Λογισμικού (SDLC) και ότι οι ευπάθειες εντοπίζονται, μετριάζονται και αποτρέπονται πριν από την εγκατάσταση στο περιβάλλον παραγωγής.

1.3 Η παρούσα πολιτική υποστηρίζει την εφαρμογή της ρήτρας 8.1 του ISO/IEC 27001:2022 και των ελέγχων 8.25–8.28 του Παραρτήματος Α, μέσω της τυποποίησης της διακυβέρνησης της ασφαλούς ανάπτυξης, των πρακτικών επικύρωσης κώδικα και της εποπτείας της ανάπτυξης από τρίτα μέρη.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα ακόλουθα:

2.1.1 Λογισμικό, εφαρμογές, σενάρια, διασυνδέσεις και εργαλεία αυτοματοποίησης που αναπτύσσονται εσωτερικά ή εξωτερικά

2.1.2 Ομάδες ανάπτυξης, ιδιοκτήτες προϊόντων, ομάδες DevOps, QA, αρχιτέκτονες, διαχειριστές έργων και ανάδοχοι

2.1.3 Περιβάλλοντα SDLC, συμπεριλαμβανομένων συστημάτων ανάπτυξης, δοκιμών, σταδιοποίησης και προπαραγωγής

2.1.4 Συστατικά ανοικτού κώδικα και στοιχεία τρίτων μερών που ενσωματώνονται σε εσωτερικές εφαρμογές

2.1.5 Λογισμικό που εγκαθίσταται εντός εγκαταστάσεων, σε ιδιωτικά περιβάλλοντα νέφους, υβριδικά ή δημόσια περιβάλλοντα νέφους

2.2 Όλοι οι χρήστες και οι οντότητες που συμμετέχουν στην ανάπτυξη, στις δοκιμές ή στην εγκατάσταση συστημάτων στο πλαίσιο του οργανισμού υπάγονται στην παρούσα πολιτική, συμπεριλαμβανομένων των παρόχων διαχειριζόμενων υπηρεσιών (MSPs) και των προμηθευτών πλατφορμών.

3. Στόχοι

3.1 Να ενσωματώνονται έλεγχοι ασφάλειας σε όλες τις φάσεις ανάπτυξης λογισμικού, από τον σχεδιασμό έως την εγκατάσταση, διασφαλίζοντας ότι η μείωση του κινδύνου είναι προληπτική και συνεχής.

3.2 Να αποτρέπεται η εισαγωγή εκμεταλλεύσιμων ευπαθειών, όπως ελαττώματα έγχυσης, ανασφαλής αυθεντικοποίηση και έκθεση σε γνωστές αδυναμίες τρίτων μερών.

3.3 Να καθιερώνονται και να εφαρμόζονται πρακτικές ασφαλούς κωδικοποίησης ευθυγραμμισμένες με το OWASP, το SANS CWE και οδηγίες ειδικές για κάθε πλαίσιο ανάπτυξης.

3.4 Να διασφαλίζεται ότι όλος ο κώδικας υποβάλλεται σε ομότιμη ανασκόπηση, αυτοματοποιημένη ανάλυση και επικύρωση ασφάλειας πριν από την εγκατάσταση.

3.5 Να αντιμετωπίζονται οι κίνδυνοι ανάπτυξης που απορρέουν από την εξωτερική ανάθεση, την ενσωμάτωση κώδικα τρίτων μερών και την επαναχρησιμοποίηση λογισμικού ανοικτού κώδικα.

3.6 Να προστατεύονται τα περιβάλλοντα ανάπτυξης, δοκιμών και σταδιοποίησης από μη εξουσιοδοτημένη πρόσβαση και να αποτρέπεται η χρήση δεδομένων παραγωγής χωρίς εγκεκριμένη απόκρυψη δεδομένων ή ανωνυμοποίηση.

3.7 Να ενισχύεται η ευαισθητοποίηση σε θέματα ασφάλειας μεταξύ προγραμματιστών, διαχειριστών προϊόντων και επαγγελματιών διασφάλισης ποιότητας μέσω εκπαίδευσης βάσει ρόλων και συνεχούς ενημέρωσης σχετικά με αναδυόμενες απειλές.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει ότι οι απαιτήσεις ασφαλούς ανάπτυξης εφαρμόζονται σε ολόκληρο τον οργανισμό.

4.1.2 Εγκρίνει τα πρότυπα ασφαλούς κωδικοποίησης και τις συμβάσεις ανάπτυξης με τρίτα μέρη.

4.1.3 Επικυρώνει τις αποφάσεις αντιμετώπισης κινδύνων για ευπάθειες που παραμένουν ανεπίλυτες ή έχουν αναβληθεί.

4.2 Επικεφαλής Ασφάλειας Εφαρμογών / Διευθυντής DevSecOps

4.2.1 Αναπτύσσει, συντηρεί και προωθεί τις οδηγίες ασφαλούς κωδικοποίησης.

4.2.2 Ενσωματώνει στατικές και δυναμικές δοκιμές ασφάλειας στους αγωγούς CI/CD.

4.2.3 Διενεργεί ανασκοπήσεις ασφάλειας κώδικα και καθορίζει υποχρεωτικές ενέργειες αποκατάστασης.

[... 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 ως απόκριση σε:

9.1.1 Σημαντικές αναθεωρήσεις στις μεθοδολογίες ανάπτυξης ή στα εργαλεία DevOps

9.1.2 Ουσιώδη περιστατικά ασφάλειας που προκύπτουν από ευπάθειες εφαρμογών

9.1.3 Αλλαγές σε κανονιστικές απαιτήσεις που σχετίζονται με το ασφαλές λογισμικό (π.χ. ΓΚΠΔ της ΕΕ, Κανονισμός DORA της ΕΕ)

9.1.4 Νέα πρότυπα κλάδου ή πληροφορίες απειλών (π.χ. OWASP Top 10, SLSA, MITRE CWE)

9.2 Η ανασκόπηση της πολιτικής διενεργείται από τον Επικεφαλής Ασφάλειας Εφαρμογών σε συντονισμό με τον CISO, τους αρχιτέκτονες λογισμικού, την ηγεσία QA και τον νομικό σύμβουλο (για επιπτώσεις που αφορούν κώδικα τρίτων μερών).

9.3 Κάθε αναθεώρηση πρέπει να καταγράφεται στο Μητρώο Ελέγχου Εγγράφων του ISMS, να υπόκειται σε έλεγχο έκδοσης και να κοινοποιείται στις επηρεαζόμενες ομάδες μέσω σημειώσεων έκδοσης ή υποχρεωτικής εκπαίδευσης.

9.4 Οι προηγούμενες εκδόσεις πρέπει να διατηρούνται στο αρχειακό αποθετήριο για σκοπούς νομικής κάλυψης και ελεγκτικής ιχνηλασιμότητας.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 – Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει τη στρατηγική κατεύθυνση για την ενσωμάτωση της ασφάλειας σε όλα τα πληροφοριακά συστήματα, εκ των οποίων η ασφαλής ανάπτυξη αποτελεί θεμελιώδη επιχειρησιακό έλεγχο.

10.2 P4 – Πολιτική Ελέγχου Πρόσβασης. Καθορίζει τα μέτρα ελέγχου για τον περιορισμό της πρόσβασης σε περιβάλλοντα ανάπτυξης, αποθετήρια, εργαλεία build και αγωγούς CI/CD.

10.3 P5 – Πολιτική Διαχείρισης Αλλαγών. Διασφαλίζει ότι οι αλλαγές κώδικα, οι εκδόσεις και οι εγκαταστάσεις υπόκεινται σε κατάλληλη έγκριση, σχεδιασμό επαναφοράς και επαλήθευση μετά την εγκατάσταση.

10.4 P12 – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων. Υποστηρίζει την απογραφή των περιβαλλόντων ανάπτυξης, των αποθετηρίων πηγαίου κώδικα και των συστημάτων build ως διαχειριζόμενων περιουσιακών στοιχείων που υπόκεινται σε ταξινόμηση και προστασία.

10.5 P22 – Πολιτική Καταγραφής και Παρακολούθησης. Εφαρμόζεται στους αγωγούς ανάπτυξης, διασφαλίζοντας ότι οι διαδικασίες build, οι προωθήσεις κώδικα και τα συμβάντα εγκατάστασης καταγράφονται, παρακολουθούνται και αναλύονται για ανωμαλίες ασφάλειας.

10.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών. Παρέχει το πλαίσιο για την ανάλυση και την απόκριση σε αδυναμίες ασφάλειας που εντοπίζονται μετά την εγκατάσταση ή κατά τις δοκιμές ασφάλειας εφαρμογών.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί την ενσωμάτωση διαδικασιών και ελέγχων ασφαλούς ανάπτυξης στις λειτουργίες.

11.2 ISO/IEC 27002:2022 – Έλεγχοι 8.25–8.28

11.2.1 Έλεγχος 8.25 του Παραρτήματος Α – Κύκλος ζωής ασφαλούς ανάπτυξης: Επιβάλλει την επίσημη ενσωμάτωση της ασφάλειας στον σχεδιασμό και στην ανάπτυξη λογισμικού.

11.2.2 Έλεγχος 8.26 του Παραρτήματος Α – Απαιτήσεις ασφάλειας εφαρμογών: Απαιτεί τον καθορισμό ασφαλούς κωδικοποίησης και κριτηρίων αποδοχής ασφάλειας.

11.2.3 Έλεγχος 8.27 του Παραρτήματος Α – Αρχιτεκτονική ασφαλών συστημάτων και αρχές μηχανικής: Απαιτεί την εφαρμογή αρχών σχεδιασμού ασφάλειας και τον μετριασμό γνωστών αδυναμιών.

11.2.4 Έλεγχος 8.28 του Παραρτήματος Α – Ασφαλής κωδικοποίηση: Απαιτεί την εφαρμογή πρακτικών ασφαλούς κωδικοποίησης καθ' όλη τη διάρκεια της ανάπτυξης λογισμικού.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 έως SA-15: Καθορίζει δομημένες πρακτικές ανάπτυξης ασφάλειας εφαρμογών, συμπεριλαμβανομένων απαιτήσεων για σχεδιασμό, ακεραιότητα κώδικα και δοκιμές.

11.3.2 SI-10 – Επικύρωση εισόδου πληροφοριών: Καλύπτει άμυνες ασφαλούς κωδικοποίησης.

11.3.3 SR-3 – Προστασία εφοδιαστικής αλυσίδας: Απαιτεί έλεγχο καταλληλότητας λογισμικού τρίτων μερών, συστατικών και παρόχων ανάπτυξης.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 25 – Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού: Επιβάλλει την ενσωμάτωση ασφάλειας και ιδιωτικότητας στην ανάπτυξη συστημάτων.

11.4.2 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Υποστηρίζει τεχνικά μέτρα όπως επικύρωση εισόδου, έλεγχοι πρόσβασης και ασφαλή εγκατάσταση.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(e), (f): Απαιτεί πρακτικές ανάπτυξης λογισμικού που περιλαμβάνουν διαχείριση ευπαθειών, ασφάλεια κώδικα και αναφορά περιστατικών.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 9 – Διαχείριση κινδύνων ΤΠΕ: Απαιτεί πρακτικές ασφαλούς ανάπτυξης για χρηματοοικονομικές οντότητες, συμπεριλαμβανομένων ελέγχων ποιότητας λογισμικού και αποκατάστασης ελαττωμάτων.

11.6.2 Άρθρο 10 – Επιχειρησιακή συνέχεια και δοκιμές: Ενθαρρύνει αυστηρές δοκιμές και επικύρωση συστημάτων ΤΠΕ, συμπεριλαμβανομένων εφαρμογών.

11.7 COBIT 2019

11.7.1 BAI03 – Διαχείριση προσδιορισμού λύσεων και υλοποίησης: Διέπει τον σχεδιασμό, την ανάπτυξη και την ενσωμάτωση της ασφάλειας σε νέες λύσεις.

11.7.2 BAI07 – Διαχείριση αποδοχής αλλαγών και μετάβασης: Διασφαλίζει την ασφαλή εγκατάσταση και την αξιολόγηση μετά την εγκατάσταση.

11.7.3 DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Εφαρμόζει επικύρωση ασφάλειας στην παροχή λογισμικού και υπηρεσιών.