					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P24S					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**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	**Ρήτρα/Άρθρο**	**Σχόλιο**
ISO/IEC 27001:2022	Ρήτρα 8	Σχετικοί έλεγχοι ασφάλειας για επιχειρησιακές πρακτικές, συμπεριλαμβανομένης της ασφαλούς ανάπτυξης
ISO/IEC 27002:2022	Έλεγχοι 8.25–8.27	Καλύπτει τον ασφαλή κύκλο ζωής ανάπτυξης, τις δοκιμές και τις αρμοδιότητες ασφάλειας τρίτων προγραμματιστών
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Αντιμετωπίζει τον ασφαλή κύκλο ζωής ανάπτυξης λογισμικού, τον έλεγχο πρόσβασης και τη διαχείριση ευπαθειών στην ανάπτυξη
ΓΚΠΔ της ΕΕ	Άρθρο 25	Απαιτεί προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού κατά την ανάπτυξη λογισμικού
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a), (e), (h)	Επιβάλλει πολιτικές ασφαλούς ανάπτυξης, εποπτεία της χρήσης λογισμικού ανοικτού κώδικα και τεκμηρίωση μέτρων μετριασμού
Κανονισμός DORA της ΕΕ	Άρθρα 6(7), 9(1)(c), 10(2)(c)	Ασφάλεια κύκλου ζωής για κρίσιμα συστήματα ΤΠΕ στον χρηματοοικονομικό τομέα
COBIT 2019	BAI	Πλαίσιο για δομημένη, ιχνηλάσιμη και ανθεκτική διαχείριση της ασφαλούς ανάπτυξης

1. Σκοπός

1.1 Η παρούσα πολιτική διασφαλίζει ότι όλο το λογισμικό, τα σενάρια και τα εργαλεία που βασίζονται στον ιστό, τα οποία δημιουργούνται ή τροποποιούνται από τον οργανισμό ή τους εξωτερικούς συνεργάτες του, αναπτύσσονται με ασφαλή τρόπο, ελαχιστοποιώντας τον κίνδυνο ευπαθειών, μη εξουσιοδοτημένης πρόσβασης σε δεδομένα ή επιχειρησιακής διαταραχής.

1.2 Καθορίζει υποχρεωτικούς κανόνες ασφαλούς ανάπτυξης και πρακτικές κωδικοποίησης που οφείλουν να ακολουθούν όλοι οι εσωτερικοί προγραμματιστές, οι ανάδοχοι και οι προμηθευτές, ανεξαρτήτως μεγέθους ή πολυπλοκότητας του έργου.

1.3 Η παρούσα πολιτική αποσκοπεί στην προστασία των δεδομένων πελατών, στην πρόληψη παραβιάσεων και στη διασφάλιση ότι το λογισμικό που δημιουργείται ή προσαρμόζεται από ή για τον οργανισμό μπορεί να ανταποκρίνεται σε ελέγχους ασφάλειας, να συμμορφώνεται με νομικές απαιτήσεις (π.χ. ΓΚΠΔ της ΕΕ, NIS2, DORA) και να υποστηρίζει την πιστοποίηση κατά ISO/IEC 27001.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα φυσικά πρόσωπα και νομικά πρόσωπα που εμπλέκονται στην ανάπτυξη, παραμετροποίηση, εγκατάσταση ή διαχείριση των ακόλουθων για λογαριασμό του οργανισμού:

2.1.1 Ιστότοποι, εφαρμογές ή εργαλεία αυτοματοποίησης

2.1.2 Εσωτερικά αναπτυγμένα σενάρια ή λογισμικό

2.1.3 Κώδικας που παράγεται από τρίτους προγραμματιστές ή ελεύθερους επαγγελματίες

2.1.4 Πρόσθετα, βιβλιοθήκες και συστατικά λογισμικού που ενσωματώνονται σε συστήματα παραγωγής

2.2 Καλύπτει όλα τα περιβάλλοντα που χρησιμοποιούνται για δραστηριότητες ανάπτυξης, συμπεριλαμβανομένων των εξής:

2.2.1 Περιβάλλοντα ανάπτυξης και δοκιμών

2.2.2 Περιβάλλοντα σταδιοποίησης και προπαραγωγής

2.2.3 Συστήματα παραγωγής που χρησιμοποιούνται για την εκτέλεση κώδικα προσαρμοσμένης ανάπτυξης

2.3 Η πολιτική διέπει επίσης τον χειρισμό δεδομένων κατά την ανάπτυξη και την εγκατάσταση, ιδίως κάθε χρήση δεδομένων παραγωγής σε συστήματα μη παραγωγικής λειτουργίας.

3. Στόχοι

3.1 Να αποτρέπεται η εισαγωγή αδυναμιών ασφάλειας ή ευπαθειών σε λογισμικό προσαρμοσμένης ανάπτυξης ή σε λογισμικό που έχει αναπτυχθεί από τρίτους.

3.2 Να διασφαλίζεται ότι οι πρακτικές ασφαλούς κωδικοποίησης και η πρόληψη ευπαθειών ενσωματώνονται σε κάθε φάση του κύκλου ζωής ανάπτυξης λογισμικού.

3.3 Να μειώνονται οι κίνδυνοι που συνδέονται με τη χρήση συστατικών ανοικτού κώδικα ή τρίτων μέσω υποχρεωτικής αξιολόγησης και παρακολούθησής τους.

3.4 Να απαιτείται επίσημη ανασκόπηση κώδικα και δοκιμές ασφάλειας εφαρμογών πριν από την έκδοση.

3.5 Να ελέγχεται η πρόσβαση στα περιβάλλοντα ανάπτυξης και να διασφαλίζεται ο διαχωρισμός τους από τα ενεργά συστήματα παραγωγής.

3.6 Να ικανοποιούνται οι υποχρεωτικές απαιτήσεις διεθνών προτύπων και κανονιστικών απαιτήσεων (π.χ. ISO/IEC 27001, ΓΚΠΔ της ΕΕ, DORA, NIS2).

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Εγκρίνει και έχει την κυριότητα της παρούσας πολιτικής.

4.1.2 Διασφαλίζει ότι κάθε ανάπτυξη λογισμικού, είτε εσωτερική είτε εξωτερικά ανατεθειμένη, συμμορφώνεται με την παρούσα πολιτική.

4.1.3 Ανασκοπεί και υπογράφει συμβάσεις ανάπτυξης ή παροχής υπηρεσιών που περιλαμβάνουν ρήτρες ασφαλούς ανάπτυξης.

4.1.4 Επαληθεύει τη συμμόρφωση των προμηθευτών μέσω τακτικών ελέγχων προόδου ή κατόπιν αιτήματος παροχής τεκμηρίων ασφάλειας.

4.2 Εσωτερικός Προγραμματιστής ή Ιδιοκτήτης Εφαρμογής

4.2.1 Ακολουθεί πρακτικές ασφαλούς κωδικοποίησης και εγκατάστασης.

4.2.2 Εφαρμόζει τον κατάλογο ελέγχου ασφαλούς ανάπτυξης σε κάθε έργο.

4.2.3 Επικυρώνει την ασφάλεια κάθε συστατικού ανοικτού κώδικα ή τρίτου που χρησιμοποιείται.

4.2.4 Αναφέρει αμέσως στον GM οποιεσδήποτε ευπάθειες εντοπίζονται.

[... 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 από τον Γενικό Διευθυντή τουλάχιστον μία φορά ετησίως, ώστε να:

9.1.1 Επαληθεύεται η συνεχιζόμενη συμμόρφωση με το ISO/IEC 27001, τον ΓΚΠΔ της ΕΕ, την Οδηγία NIS2 της ΕΕ και τον Κανονισμό DORA της ΕΕ

9.1.2 Αντικατοπτρίζονται οι επικαιροποιημένες απειλές ή οι αλλαγές στις βέλτιστες πρακτικές ασφαλούς ανάπτυξης

9.1.3 Διασφαλίζεται η συμβατότητα με νέα εργαλεία, πλατφόρμες ή σχέσεις με προμηθευτές

9.2 Ενδιάμεσες ανασκοπήσεις πρέπει να ενεργοποιούνται από:

9.2.1 Οποιοδήποτε αναφερόμενο περιστατικό ασφάλειας λογισμικού

9.2.2 Την εισαγωγή νέου framework ανάπτυξης ή πλατφόρμας φιλοξενίας

9.2.3 Αλλαγή στους τρίτους συνεργάτες ανάπτυξης

9.2.4 Κανονιστικές επικαιροποιήσεις που επηρεάζουν τις υποχρεώσεις λογισμικού ή ασφάλειας

9.3 Όλες οι αλλαγές στην παρούσα πολιτική πρέπει να:

9.3.1 Τεκμηριώνονται με την ημερομηνία, σύνοψη της αλλαγής και έγκριση του GM

9.3.2 Κοινοποιούνται με σαφήνεια σε όλο το εσωτερικό και εξωτερικό προσωπικό ανάπτυξης

9.3.3 Αποθηκεύονται ως μέρος του ελέγχου εκδόσεων και του ιστορικού μεταβολών πολιτικών του οργανισμού

9.4 Οι επικαιροποιημένες εκδόσεις πρέπει να είναι εύκολα προσβάσιμες, είτε μέσω εσωτερικών πλατφορμών, είτε μέσω έντυπης τεκμηρίωσης, είτε μέσω υπηρεσιών νέφους προσβάσιμων στους προμηθευτές.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζει και εξαρτάται από την αποτελεσματική εφαρμογή αρκετών άλλων πολιτικών SME:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τη λογοδοσία για την ανάθεση και την επαλήθευση ελέγχων ασφάλειας ανάπτυξης σε έργα και προμηθευτές.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Παρέχει βασικούς κανόνες για τον περιορισμό της πρόσβασης σε περιβάλλοντα ανάπτυξης και αποθετήρια κώδικα, συμπεριλαμβανομένου του διαχωρισμού καθηκόντων (SoD).

10.1.3 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι οι εσωτερικοί προγραμματιστές και οι ανάδοχοι κατανοούν τις πρακτικές ασφαλούς κωδικοποίησης και τις σχετικές αρμοδιότητες ασφάλειας.

10.1.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Αποσαφηνίζει τον τρόπο με τον οποίο πρέπει να γίνεται ο χειρισμός δεδομένων προσωπικού χαρακτήρα κατά τις διαδικασίες ανάπτυξης, δοκιμών και καταγραφής, ώστε να διατηρείται η συμμόρφωση με τον ΓΚΠΔ της ΕΕ.

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών (P30): Ορίζει τον τρόπο με τον οποίο πρέπει να αναφέρονται, να αξιολογούνται και να αποκαθίστανται τα περιστατικά ασφάλειας που σχετίζονται με την ανάπτυξη, συμπεριλαμβανομένων των περιστατικών που σχετίζονται με κώδικα.

10.2 Καθεμία από αυτές τις πολιτικές λειτουργεί συμπληρωματικά, ώστε η ασφαλής ανάπτυξη να είναι εφικτή και επαληθεύσιμη, ακόμη και σε μικρό ή μη τεχνικό οργανισμό.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 8.1 – Απαιτεί την εφαρμογή επιχειρησιακών ελέγχων, συμπεριλαμβανομένης της ασφαλούς ανάπτυξης, που ευθυγραμμίζονται με τους επιχειρησιακούς στόχους και τη στάση κινδύνου.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 8.25 – Συνιστά την ενσωμάτωση της ασφάλειας σε όλο τον κύκλο ζωής του λογισμικού, συμπεριλαμβανομένου του ελέγχου πηγαίου κώδικα, του ελέγχου εκδόσεων και της πρόσβασης προγραμματιστών.

11.2.2 Έλεγχος 8.26 – Προσδιορίζει μεθόδους για δοκιμές εφαρμογών και επαλήθευση της λειτουργικότητας ασφάλειας πριν από τη θέση σε παραγωγική λειτουργία.

11.2.3 Έλεγχος 8.27 – Απαιτεί από τους τρίτους προγραμματιστές να τηρούν τα ίδια πρότυπα ανάπτυξης και να έχουν σαφώς καθορισμένες τις αρμοδιότητες ασφάλειάς τους.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 έως SA-15 – Ορίζουν διαδικασίες ασφαλούς ανάπτυξης, συμπεριλαμβανομένων του ελέγχου πρόσβασης προγραμματιστών, των δοκιμών, της μοντελοποίησης απειλών και της τεκμηρίωσης.

11.3.2 SI-10 – Απαιτεί από τους προγραμματιστές να εντοπίζουν και να μετριάζουν συνήθεις αδυναμίες λογισμικού και να χρησιμοποιούν αυτοματοποιημένα εργαλεία όπου εφαρμόζεται.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 25 – Η «προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού» επιβάλλει την ενσωμάτωση μέτρων ασφάλειας και ιδιωτικότητας κατά τον σχεδιασμό και την ανάπτυξη λογισμικού, ιδίως όπου γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(a), (e) και (h) – Απαιτεί πολιτικές ασφαλούς ανάπτυξης, εποπτεία της χρήσης ανοικτού κώδικα και τεκμηριωμένο μετριασμό κινδύνων που σχετίζονται με εφαρμογές σε βασικούς και σημαντικούς φορείς.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρα 6(7), 9(1)(c) και 10(2)(c) – Επιβάλλουν υποχρεώσεις ασφάλειας του κύκλου ζωής ανάπτυξης για οντότητες του χρηματοοικονομικού τομέα, συμπεριλαμβανομένων των SME, ιδίως για κρίσιμα συστήματα ΤΠΕ.

11.7 COBIT 2019

11.7.1 BAI03 – Το «Manage Solutions Identification and Build» υποστηρίζει την εφαρμογή δομημένων ελέγχων ανάπτυξης που δίνουν έμφαση στην ασφάλεια, την ιχνηλασιμότητα και την ανθεκτικότητα, προσαρμοσμένων στους περιορισμούς των SME.