					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P28S					Τίτλος εγγράφου: **Πολιτική Εξωτερικής Ανάθεσης Ανάπτυξης Λογισμικού P28S**							
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	Ρήτρες 5.1, 6.1, 8	Εφαρμοστέοι έλεγχοι του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) και έλεγχοι που σχετίζονται με προμηθευτές
ISO/IEC 27002:2022	Έλεγχοι 5.19, 5.20, 8.25–8.27	Έλεγχοι για προμηθευτές και για τον ασφαλή κύκλο ζωής ανάπτυξης
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Απαιτήσεις για απόκτηση, εφοδιαστική αλυσίδα, ασφαλή ανάπτυξη και συμφωνίες με προμηθευτές
ΓΚΠΔ της ΕΕ	Άρθρο 28	Συμβατικές απαιτήσεις και απαιτήσεις προστασίας δεδομένων για επεξεργασία από τρίτα μέρη
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a), (h)	Έλεγχοι ασφάλειας εφοδιαστικής αλυσίδας και ασφαλούς ανάπτυξης εφαρμογών
Κανονισμός DORA της ΕΕ	Άρθρο 10	Διαχείριση κινδύνων ΤΠΕ από τρίτα μέρη, συμπεριλαμβανομένης της εξωτερικής ανάθεσης ανάπτυξης
COBIT 2019	BAI03, DSS05	Απαιτήσεις για εξωτερική ανάπτυξη και εξωτερικούς παρόχους υπηρεσιών πληροφορικής

1. Σκοπός

1.1 Η παρούσα πολιτική διασφαλίζει ότι κάθε ανάπτυξη λογισμικού που ανατίθεται σε τρίτους — είτε υλοποιείται από ελεύθερους επαγγελματίες, εταιρείες ανάπτυξης ή άλλους εξωτερικούς παρόχους — εκτελείται με ασφάλεια, υπό συμβατικό έλεγχο και σε ευθυγράμμιση με τις εφαρμοστέες νομικές, κανονιστικές και ελεγκτικές απαιτήσεις.

1.2 Η πολιτική προστατεύει τον οργανισμό από κινδύνους που σχετίζονται με μη ασφαλή κώδικα, ασαφή ιδιοκτησία, έκθεση δεδομένων και ανεπαρκή διαχείριση προμηθευτών, εφαρμόζοντας δεσμευτικά πρότυπα ανάπτυξης και εποπτεία προμηθευτών, ακόμη και όταν δεν υπάρχει ειδικό τμήμα πληροφορικής.

1.3 Η παρούσα πολιτική υποστηρίζει την πιστοποίηση κατά ISO/IEC 27001:2022, παρέχοντας σαφώς καθορισμένες απαιτήσεις ανάπτυξης, λογοδοσία και τεκμηριωμένους ελέγχους για δραστηριότητες ανάπτυξης από τρίτα μέρη.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλους τους εξωτερικούς προγραμματιστές, συμπεριλαμβανομένων των ελεύθερων επαγγελματιών και των εταιρειών ανάπτυξης

2.1.2 Κάθε εργασία ανάπτυξης που αφορά εσωτερικά εργαλεία, δημόσια προσβάσιμους ιστότοπους, εφαρμογές λογισμικού ή επιχειρησιακό αυτοματισμό

2.1.3 Το προσωπικό που είναι υπεύθυνο για την επιλογή, τη διαχείριση ή την εποπτεία εξωτερικών προγραμματιστών

2.1.4 Κάθε διασύνδεση συστημάτων από τρίτο μέρος, ανάπτυξη σεναρίων ή ανάπτυξη λογισμικού που αλληλεπιδρά με δεδομένα ή συστήματα της εταιρείας

2.2 Περιλαμβάνει επίσης κάθε τρίτο μέρος ή πλατφόρμα που διαθέτει πρόσβαση σε διαπιστευτήρια της εταιρείας, αποθετήρια δεδομένων, αποθετήρια πηγαίου κώδικα, περιβάλλοντα δοκιμών αποδοχής ή συστήματα παραγωγής.

3. Στόχοι

3.1 Να διασφαλίζεται ότι κάθε εξωτερικά ανατιθέμενη ανάπτυξη τηρεί τις αρχές της ασφαλούς κωδικοποίησης και ότι οι προγραμματιστές δεσμεύονται συμβατικά να ακολουθούν τεκμηριωμένα πρότυπα και ρήτρες εμπιστευτικότητας.

3.2 Να καθιερώνεται σαφής ιδιοκτησία για όλα τα παραδοτέα — κώδικα, περιουσιακά στοιχεία, διαπιστευτήρια και τεκμηρίωση — διασφαλίζοντας την πλήρη μεταβίβαση δικαιωμάτων στην εταιρεία και ιχνηλάσιμη παράδοση με την ολοκλήρωση του έργου.

3.3 Να προλαμβάνονται συνήθεις κίνδυνοι ανάπτυξης, συμπεριλαμβανομένης της επαναχρησιμοποίησης ιδιόκτητου κώδικα, επιθέσεων στην εφοδιαστική αλυσίδα μέσω βιβλιοθηκών, της χρήσης μη υποστηριζόμενων πλαισίων ανάπτυξης και της μη ελεγχόμενης διαχειριστικής πρόσβασης.

3.4 Να απαιτείται τεκμηρίωση πριν από την έναρξη κάθε έργου εξωτερικής ανάθεσης, συμπεριλαμβανομένων συμβάσεων, συμφωνίας εμπιστευτικότητας και ελάχιστων απαιτήσεων ασφάλειας.

3.5 Να προστατεύονται τα δεδομένα πελατών, τα συστήματα και οι εσωτερικές διεργασίες μέσω εφαρμογής αυστηρής εποπτείας της ανάπτυξης, δοκιμών μετά την παράδοση και ασφαλούς διαχείρισης πρόσβασης στα συστήματα.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Εγκρίνει όλες τις σχέσεις με προμηθευτές και υπογράφει τις συμφωνίες ανάπτυξης.

4.1.2 Διασφαλίζει ότι κάθε εξωτερικά ανατιθέμενη ανάπτυξη συμμορφώνεται με την παρούσα πολιτική.

4.1.3 Αφαιρεί την πρόσβαση στα συστήματα της εταιρείας μετά την ολοκλήρωση του έργου.

4.1.4 Ανασκοπεί την τεκμηρίωση και τα αποτελέσματα μετά την παράδοση.

4.2 Ιδιοκτήτης έργου (συνήθως εσωτερικός εργαζόμενος ή ορισμένος συντονιστής)

4.2.1 Διαχειρίζεται τον καθημερινό συντονισμό με τον εξωτερικό προγραμματιστή.

4.2.2 Επαληθεύει ότι ικανοποιούνται οι λειτουργικές απαιτήσεις και ότι τα παραδοτέα έχουν υποβληθεί σε δοκιμές.

4.2.3 Διασφαλίζει την ασφαλή παράδοση κώδικα και διαπιστευτηρίων.

4.2.4 Αναφέρει στον GM οποιοδήποτε ζήτημα ή περιστατικό που σχετίζεται με την ανάπτυξη.

[... 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 από τον Γενικό Διευθυντή (GM) τουλάχιστον μία φορά ετησίως. Η ανασκόπηση διασφαλίζει ότι εξακολουθεί να καλύπτει:

9.1.1.1 Τις απαιτήσεις πιστοποίησης ISO/IEC 27001

9.1.1.2 Τις αλλαγές στις νομικές υποχρεώσεις (π.χ. Άρθρο 28 του ΓΚΠΔ, Άρθρο 10 του DORA)

9.1.1.3 Τις τρέχουσες πρακτικές ανάπτυξης σε επίπεδο SME και τους κινδύνους από τρίτα μέρη

9.2 Ενδιάμεσες ανασκοπήσεις

9.2.1 Ανασκοπήσεις της πολιτικής πρέπει επίσης να διενεργούνται όταν:

9.2.1.1 Εντάσσεται νέος προμηθευτής ή νέα πλατφόρμα εξωτερικής ανάθεσης ανάπτυξης

9.2.1.2 Συμβαίνει σημαντικό περιστατικό που αφορά εξωτερικά ανατιθέμενη ανάπτυξη

9.2.1.3 Υπάρχουν ουσιώδεις αλλαγές στα εργαλεία, τις πλατφόρμες ή τα περιβάλλοντα που χρησιμοποιούνται

9.3 Διαδικασία ανασκόπησης

9.3.1 Ο GM είναι υπεύθυνος για:

9.3.1.1 Την επαλήθευση ότι οι συμβάσεις, οι συμφωνίες εμπιστευτικότητας και οι διεργασίες ελέγχου πρόσβασης παραμένουν αποτελεσματικές

9.3.1.2 Την επιβεβαίωση ότι οι τρέχοντες προμηθευτές και οι ελεύθεροι επαγγελματίες είναι ευθυγραμμισμένοι με την πολιτική

9.3.1.3 Την αναθεώρηση των όρων βάσει ανατροφοδότησης από προηγούμενα έργα ή περιστατικά

9.4 Έλεγχος εκδόσεων και επικοινωνία

9.4.1 Όλες οι αλλαγές πρέπει να:

9.4.1.1 Καταγράφονται με ημερομηνία, αιτία και περιγραφή της αλλαγής

9.4.1.2 Εγκρίνονται από τον GM και να προστίθενται στο ιστορικό εκδόσεων

9.4.1.3 Κοινοποιούνται σε όλο το προσωπικό ή στους ιδιοκτήτες έργων που συνεργάζονται με εξωτερικούς προγραμματιστές

9.4.1.4 Αναδιανέμονται, όπου απαιτείται, σε όλους τους επηρεαζόμενους προμηθευτές ή άλλους τρίτους

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζει άμεσα και εξαρτάται από την εφαρμογή των ακόλουθων πολιτικών ευθυγραμμισμένων με τις ανάγκες SME:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Αποσαφηνίζει ποιος είναι υπεύθυνος για την έγκριση προμηθευτών, τον έλεγχο πρόσβασης και την αποδοχή κινδύνου κατά τη χρήση εξωτερικών προγραμματιστών.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Ορίζει τη σωστή δημιουργία, τον περιορισμό και τον τερματισμό λογαριασμών χρηστών και της διαχειριστικής πρόσβασης που χρησιμοποιούνται κατά την εξωτερική ανάθεση ανάπτυξης.

10.1.3 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι το εσωτερικό προσωπικό κατανοεί πώς να συντονίζεται με ασφάλεια με εξωτερικούς προγραμματιστές, συμπεριλαμβανομένου του χειρισμού διαπιστευτηρίων και αρχείων έργου.

10.1.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Καθορίζει απαιτήσεις ασφάλειας και νομικές απαιτήσεις για τον χειρισμό δεδομένων προσωπικού χαρακτήρα που ενδέχεται να υποβάλλονται σε επεξεργασία από εξωτερικούς προγραμματιστές στο πλαίσιο του ΓΚΠΔ.

10.1.5 P24S – Πολιτική Ασφαλούς Ανάπτυξης: Προσδιορίζει πώς η εσωτερική και εξωτερική ανάπτυξη πρέπει να ακολουθεί πρακτικές ασφαλούς κωδικοποίησης και έλεγχο βιβλιοθηκών και πλαισίων ανάπτυξης.

10.1.6 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Απαιτείται όταν η εξωτερικά ανατιθέμενη ανάπτυξη οδηγεί σε περιστατικά ασφάλειας ή ευπάθειες, καθοδηγώντας τη συντονισμένη διερεύνηση και αποκατάσταση.

10.2 Οι πολιτικές αυτές πρέπει να εφαρμόζονται παράλληλα, ώστε η εξωτερική ανάθεση ανάπτυξης να μην δημιουργεί μη διαχειριζόμενο κίνδυνο ούτε να παραβιάζει τις υποχρεώσεις συμμόρφωσης των SME.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 6.1 – Οι οργανισμοί πρέπει να αξιολογούν και να αντιμετωπίζουν τους κινδύνους ασφάλειας πληροφοριών που σχετίζονται με προμηθευτές.

11.1.2 Ρήτρα 8.1 – Απαιτεί επιχειρησιακό σχεδιασμό και έλεγχο, συμπεριλαμβανομένων υπηρεσιών τρίτων μερών όπως η εξωτερική ανάθεση ανάπτυξης.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 5.19 – Συνιστά την αξιολόγηση της ικανότητας των προμηθευτών να ανταποκρίνονται στις απαιτήσεις ασφάλειας πληροφοριών.

11.2.2 Έλεγχος 5.20 – Ενθαρρύνει την τακτική παρακολούθηση και την περιοδική ανασκόπηση των υπηρεσιών τρίτων μερών.

11.2.3 Έλεγχοι 8.25–8.27 – Περιγράφουν πρακτικές ασφαλούς κύκλου ζωής ανάπτυξης που εφαρμόζονται στην εξωτερικά ανατιθέμενη ανάπτυξη.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Απαιτεί οι στρατηγικές απόκτησης να περιλαμβάνουν μέτρα ασφάλειας πληροφοριών.

11.3.2 SA-9 – Αντιμετωπίζει την εξωτερική ανάπτυξη συστημάτων και τους κινδύνους της εφοδιαστικής αλυσίδας.

11.3.3 SA-11 – Ορίζει πρακτικές ασφαλούς ανάπτυξης, συμπεριλαμβανομένης της ανασκόπησης κώδικα και της αποκατάστασης αδυναμιών.

11.3.4 SA-15 – Ενθαρρύνει τη χρήση αυτοματοποιημένων εργαλείων για τον εντοπισμό αδυναμιών και τη διασφάλιση λογισμικού.

11.3.5 SR-3 – Επιβάλλει οι συμφωνίες με προμηθευτές να περιλαμβάνουν απαιτήσεις κυβερνοασφάλειας.

11.4 Γενικός Κανονισμός για την Προστασία Δεδομένων της ΕΕ (ΓΚΠΔ)

11.4.1 Άρθρο 28 – Απαιτεί συμβάσεις με εκτελούντες την επεξεργασία τρίτων μερών ώστε να διασφαλίζονται κατάλληλες δικλίδες προστασίας δεδομένων, με άμεση εφαρμογή σε προγραμματιστές που επεξεργάζονται ή αποκτούν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(a), (h) – Απαιτεί ελέγχους ασφάλειας για την εφοδιαστική αλυσίδα και πρακτικές ασφαλούς ανάπτυξης λογισμικού για παρόχους ψηφιακών υπηρεσιών που εμπίπτουν στο πεδίο εφαρμογής, συμπεριλαμβανομένων των SME όπου εφαρμόζεται.

11.6 Κανονισμός Ψηφιακής Επιχειρησιακής Ανθεκτικότητας της ΕΕ (DORA)

11.6.1 Άρθρο 10 – Απαιτεί διαχείριση κινδύνων ΤΠΕ από τρίτα μέρη, συμπεριλαμβανομένων συμφωνιών ανάπτυξης, υποχρεώσεων ασφάλειας και ελέγχων κινδύνου που σχετίζονται με τρίτους παρόχους.

11.7 COBIT 2019

11.7.1 BAI03 – Διαχείριση προσδιορισμού και υλοποίησης λύσεων – Διασφαλίζει ότι η εξωτερική ανάπτυξη καλύπτει τις επιχειρησιακές απαιτήσεις και τις απαιτήσεις ασφάλειας.

11.7.2 DSS05 – Διαχείριση υπηρεσιών ασφάλειας – Απαιτεί οι εξωτερικές υπηρεσίες ασφάλειας και οι πάροχοι ανάπτυξης να λειτουργούν υπό εφαρμοστέους κανόνες ασφάλειας και εποπτεία.