| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου | | | | | | | |
| Αριθμός εγγράφου:<br>P28 | | | | | Τίτλος εγγράφου:<br>**Πολιτική Εξωτερικής Ανάθεσης Ανάπτυξης Λογισμικού P28S** | | | | | | | |
| Έκδοση:<br>1.0 | | Ημερομηνία έναρξης ισχύος:<br>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** |
| | | | |
| | | | |

Ευθυγράμμιση με πρότυπα και κανονιστικές απαιτήσεις

| Πρότυπο/Κανονιστικό πλαίσιο | Ρήτρα/Άρθρο | Σχόλιο |
|---|---|---|
| ISO/IEC 27001:2022 | Ρήτρα 8.1 | Δ/Ε |
| ISO/IEC 27002:2022 | Έλεγχοι 5.19-5.22, 8 | Δ/Ε |
| NIST SP 800-53 Rev.5 | SA-4, SA-9, SA-10 | Δ/Ε |
| ΓΚΠΔ της ΕΕ | Άρθρα 28, 32 | Δ/Ε |
| Οδηγία NIS2 της ΕΕ | Άρθρα 21(2)(a), (h), 23 | Δ/Ε |
| Κανονισμός DORA της ΕΕ | Άρθρα 28(1), (2) | Δ/Ε |
| COBIT 2019 | APO10, BAI03, DSS | Δ/Ε |

**1. Σκοπός**

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικούς ελέγχους για την εξωτερική ανάθεση της ανάπτυξης λογισμικού ή συστημάτων σε προμηθευτές, τρίτους αναδόχους ή εξειδικευμένα γραφεία, διασφαλίζοντας ότι ασφαλείς πρακτικές ενσωματώνονται σε ολόκληρο τον κύκλο ζωής της ανάπτυξης.

1.2 Στόχος της είναι η πρόληψη ευπαθειών ασφάλειας, απώλειας δεδομένων, έκθεσης διανοητικής ιδιοκτησίας (IP) και παραβιάσεων συμμόρφωσης που απορρέουν από συνεργασίες εξωτερικής ανάπτυξης.

1.3 Η πολιτική επιβάλλει απαιτήσεις για τη διακυβέρνηση προμηθευτών, τα πρότυπα ασφαλούς κωδικοποίησης, τη διαχείριση πρόσβασης, τις υποχρεώσεις παρακολούθησης και τη διαδικασία αποχώρησης κατά τη λήξη της σύμβασης, ώστε να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα του λογισμικού που αναπτύσσεται.

**2. Πεδίο εφαρμογής**

**2.1 Η παρούσα πολιτική εφαρμόζεται σε όλες τις οργανωτικές μονάδες που συνεργάζονται με εξωτερικές οντότητες για την ανάπτυξη λογισμικού ή συστημάτων, συμπεριλαμβανομένων των εξής:**

2.1.1 διαδικτυακών εφαρμογών, εφαρμογών κινητών συσκευών, ενσωματωμένων συστημάτων, API, σεναρίων αυτοματισμού, ροών εργασιών αυτοματισμού ή ενοτήτων πλατφόρμας

2.1.2 εξατομικευμένης ανάπτυξης για εσωτερικές πλατφόρμες, συστήματα που απευθύνονται σε πελάτες ή εμπορικά προϊόντα

2.1.3 συνεργασιών με τρίτους προγραμματιστές, ελεύθερους επαγγελματίες, εξειδικευμένα γραφεία ή υπεράκτιες ομάδες

2.2 Η πολιτική διέπει επίσης κάθε εξωτερική οντότητα που αποκτά πρόσβαση σε πηγαίο κώδικα, περιβάλλοντα δοκιμών ή αγωγούς CI/CD κατά τη διάρκεια της ανάπτυξης.

2.3 Οι απαιτήσεις είναι δεσμευτικές ανεξαρτήτως τύπου σύμβασης, μεθοδολογίας ανάπτυξης ή γεωγραφικής τοποθεσίας του παρόχου στον οποίο έχει ανατεθεί η ανάπτυξη.

**3. Στόχοι**

3.1 Να εφαρμόζονται πρακτικές ασφαλούς κύκλου ζωής ανάπτυξης λογισμικού (SDLC) σε όλες τις συνεργασίες εξωτερικής ανάθεσης, από τον σχεδιασμό έως την επικύρωση μετά την εγκατάσταση.

3.2 Να διασφαλίζεται ότι όλες οι συμβάσεις με εξωτερικούς προγραμματιστές περιλαμβάνουν υποχρεωτικές ρήτρες για την προστασία δεδομένων, την ασφαλή κωδικοποίηση και τη διασφάλιση της διανοητικής ιδιοκτησίας.

3.3 Να καθορίζονται απαιτήσεις ελέγχου πρόσβασης, παρακολούθησης και ελέγχου για τρίτους προγραμματιστές που αλληλεπιδρούν με εσωτερικά συστήματα.

3.4 Να προστατεύεται ο οργανισμός από απειλές της εφοδιαστικής αλυσίδας, νομικές παραβάσεις και βλάβη στη φήμη που σχετίζονται με λογισμικό το οποίο έχει αναπτυχθεί από εξωτερικά μέρη.

3.5 Να διατηρείται συνεχής συμμόρφωση με πλαίσια ασφάλειας, συμπεριλαμβανομένων των ISO/IEC 27001, NIST, ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ, του Κανονισμού DORA της ΕΕ και του COBIT 2019.

**4. Ρόλοι και αρμοδιότητες**

**4.1 Ανώτατη Διοίκηση**

4.1.1 Εγκρίνει έργα εξωτερικής ανάθεσης ανάπτυξης υψηλού κινδύνου και επικυρώνει εξαιρέσεις από την πολιτική, όπου αυτό αιτιολογείται.

4.1.2 Διασφαλίζει ότι οι αποφάσεις εξωτερικής ανάθεσης ευθυγραμμίζονται με τους στρατηγικούς στόχους και τη διάθεση ανάληψης κινδύνου του οργανισμού.

**4.2 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)**

4.2.1 Εγκρίνει την ένταξη προμηθευτών από πλευράς ασφάλειας.

4.2.2 Καθορίζει τις απαιτήσεις ελέγχων ασφάλειας για συνεργασίες εξωτερικής ανάθεσης και ανασκοπεί τις αναφορές περιστατικών.

[ ... 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 τουλάχιστον μία φορά ετησίως ή συχνότερα στις ακόλουθες περιπτώσεις:**

9.1.1 εισαγωγή νέων μοντέλων εξωτερικής ανάθεσης ανάπτυξης, νέων προμηθευτών ή νέων δικαιοδοσιών

9.1.2 επικαιροποιήσεις κανονιστικών πλαισίων, όπως ο ΓΚΠΔ της ΕΕ, η Οδηγία NIS2 της ΕΕ ή ο Κανονισμός DORA της ΕΕ

9.1.3 κατόπιν περιστατικού ασφάλειας που αφορά κώδικα, πρόσβαση ή παραδοτέα εξωτερικής ανάθεσης

9.1.4 στο πλαίσιο ευρημάτων Εσωτερικού Ελέγχου ή βελτιώσεων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)

**9.2 Ο Επικεφαλής Ασφάλειας Πληροφοριών (CISO) είναι υπεύθυνος για την έναρξη και τον συντονισμό της ανασκόπησης της πολιτικής, σε διαβούλευση με:**

9.2.1.1 τη Νομική Υπηρεσία, τη Συμμόρφωση και τις Προμήθειες (για ευθυγράμμιση της εφαρμογής των συμβατικών απαιτήσεων)

9.2.1.2 τους Ιδιοκτήτες έργων και προϊόντων (για επιχειρησιακή εφικτότητα)

9.2.1.3 την Ασφάλεια Πληροφοριών (για επικαιροποιήσεις απειλών και ελέγχων)

9.2.1.4 την Ανώτατη Διοίκηση (για τελική έγκριση)

**9.3 Όλες οι επικαιροποιήσεις της πολιτικής πρέπει:**

9.3.1.1 να υπόκεινται σε έλεγχο έκδοσης και να αποθηκεύονται σε καθορισμένο Αποθετήριο Εγγράφων

9.3.1.2 να γνωστοποιούνται στα ενδιαφερόμενα μέρη που συμμετέχουν σε δραστηριότητες εξωτερικής ανάθεσης ανάπτυξης

9.3.1.3 να συνδέονται με τυχόν επικαιροποιήσεις σε συναφείς πολιτικές ή διαδικαστική τεκμηρίωση

9.4 Κάθε έκδοση της πολιτικής πρέπει να συνοδεύεται από αρχείο μεταβολών, ώστε να διασφαλίζεται η ιχνηλασιμότητα των τροποποιήσεων και των εγκρίσεων.

## 10. Συναφείς πολιτικές και διασυνδέσεις

### 10.1 Η παρούσα πολιτική υποστηρίζει και υποστηρίζεται από τα ακόλουθα συναφή έγγραφα:

10.1.1 P1 - Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις αρχές ασφάλειας σε επίπεδο οργανισμού που εφαρμόζονται τόσο στην εσωτερική ανάπτυξη όσο και στην ανάπτυξη από τρίτα μέρη.

10.1.2 P5 - Πολιτική Διαχείρισης Αλλαγών: Διασφαλίζει ότι όλες οι αλλαγές που σχετίζονται με εγκατάσταση από βάσεις κώδικα εξωτερικής ανάθεσης ανασκοπούνται και εγκρίνονται πριν από την εφαρμογή τους.

10.1.3 P13 - Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθορίζει τον τρόπο με τον οποίο αναγνωρίζονται τα ευαίσθητα δεδομένα πριν από την έκθεσή τους σε προμηθευτές ανάπτυξης ή αποθετήρια.

10.1.4 P18 - Πολιτική Κρυπτογραφικών Ελέγχων: Καθοδηγεί τον τρόπο με τον οποίο πρέπει να χειρίζονται τα κλειδιά, τα μυστικά και τα ευαίσθητα διαπιστευτήρια κατά την ανάπτυξη και την παράδοση.

10.1.5 P24 - Πολιτική Ασφαλούς Ανάπτυξης: Καθορίζει τις απαιτήσεις βασικής γραμμής για εσωτερικές και εξωτερικές πρακτικές ανάπτυξης λογισμικού.

10.1.6 P30 - Πολιτική Αντιμετώπισης Περιστατικών: Διέπει τον τρόπο με τον οποίο οι παραβιάσεις ή τα ζητήματα ασφάλειας που αφορούν εξωτερική ανάθεση ανάπτυξης κλιμακώνονται, διερευνώνται και επιλύονται.

10.1.7 P33 - Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Παρέχει απαιτήσεις για την ανασκόπηση δραστηριοτήτων εξωτερικής ανάθεσης ανάπτυξης κατά τη διάρκεια ελέγχων ή ανασκοπήσεων συμμόρφωσης.

## 11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική είναι ευθυγραμμισμένη με διεθνώς αναγνωρισμένα πλαίσια ασφάλειας και κανονιστικές απαιτήσεις, ώστε να διασφαλίζεται η ασφαλής εξωτερική ανάθεση ανάπτυξης λογισμικού και οι πρακτικές διαχείρισης προμηθευτών.

### 11.2 ISO/IEC 27001

11.2.1 Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος: Επιβάλλει ελέγχους διεργασιών για ασφαλή ανάπτυξη και παράδοση από τρίτα μέρη.

### 11.3 ISO/IEC 27002:2022 - Έλεγχοι 5.19 έως 5.21, 8.

11.3.1 Παράρτημα Α Έλεγχος 5.19 - Διαχείριση σχέσεων με προμηθευτές: Απαιτεί επίσημες συμφωνίες με ρήτρες ασφάλειας και συμμόρφωσης.

11.3.2 Παράρτημα Α Έλεγχος 5.20 - Αντιμετώπιση της ασφάλειας πληροφοριών στις συμφωνίες με προμηθευτές: Διασφαλίζει ότι έλεγχοι ειδικοί για την ανάπτυξη ενσωματώνονται στις συμβάσεις.

11.3.3 Παράρτημα Α Έλεγχος 5.21 - Διαχείριση της παροχής υπηρεσιών προμηθευτών: Περιλαμβάνει την παρακολούθηση παραδοτέων και κινδύνων ανάπτυξης από τρίτα μέρη.

11.3.4 Παράρτημα Α Έλεγχος 8.27 - Εξωτερική ανάθεση ανάπτυξης: Επιβάλλει καθορισμένες απαιτήσεις ασφάλειας και ελέγχου πρόσβασης για λογισμικό που αναπτύσσεται εξωτερικά.

11.3.5 Οι έλεγχοι αυτοί καθορίζουν δομημένες απαιτήσεις για την επιλογή, τη σύναψη συμβάσεων και την εποπτεία εξωτερικών προγραμματιστών, συμπεριλαμβανομένων πρακτικών ασφαλούς ανάπτυξης, χειρισμού κώδικα και επικύρωσης απόδοσης.

### 11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Διαδικασία απόκτησης: Απαιτεί τον καθορισμό απαιτήσεων ασφαλούς ανάπτυξης κατά τον χρόνο απόκτησης.

11.4.2 SA-9 - Υπηρεσίες εξωτερικών συστημάτων: Διέπει τον τρόπο με τον οποίο τρίτοι προγραμματιστές αλληλεπιδρούν με εσωτερικές υπηρεσίες με ασφαλή τρόπο.

11.4.3 SA-10 - Διαχείριση διαμόρφωσης από προγραμματιστές: Ευθυγραμμίζεται με τις υποχρεώσεις ελέγχου εκδόσεων, πρόσβασης σε κώδικα και παρακολούθησης αλλαγών για εξωτερικές ομάδες.

**11.5 ΓΚΠΔ της ΕΕ (2016/679)**

11.5.1 Άρθρο 28 - Υποχρεώσεις εκτελούντος την επεξεργασία: Απαιτεί οι συμβάσεις με τρίτους προγραμματιστές να προσδιορίζουν απαιτήσεις ασφάλειας, ελέγχου και δικαιωμάτων ελέγχου για τον χειρισμό δεδομένων προσωπικού χαρακτήρα.

11.5.2 Άρθρο 32 - Ασφάλεια της επεξεργασίας: Επιβάλλει κατάλληλες δικλίδες ασφαλείας (π.χ. κρυπτογράφηση, έλεγχος πρόσβασης) κατά την ανάπτυξη συστημάτων που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.

**11.6 Οδηγία NIS2 της ΕΕ (2022/2555)**

11.6.1 Άρθρα 21(2)(a), (h), 23: Απαιτούν την εφαρμογή πρακτικών ασφαλούς ανάπτυξης σε όλες τις συνεργασίες με τρίτα μέρη και σε ολόκληρη την ψηφιακή εφοδιαστική αλυσίδα, με εποπτεία και τεχνική επαλήθευση.

**11.7 Κανονισμός DORA της ΕΕ (2022/2554)**

11.7.1 Άρθρα 28(1), (2): Απαιτούν από τις χρηματοοικονομικές οντότητες να διαχειρίζονται τον κίνδυνο τρίτων μερών στις ΤΠΕ μέσω συμβατικών ελέγχων και εποπτείας ασφαλούς ανάπτυξης, ιδίως για κρίσιμη εξωτερική ανάθεση ανάπτυξης.

**11.8 COBIT 2019**

11.8.1 APO10 - Διαχείριση προμηθευτών: Καθορίζει δομημένες απαιτήσεις για αξιολόγηση προμηθευτών, συμβάσεις και παρακολούθηση απόδοσης.

11.8.2 BAI03 - Διαχείριση ανάπτυξης λύσεων: Αντιστοιχίζεται άμεσα σε διαδικασίες ασφαλούς SDLC, ανασκοπήσεις κώδικα και επικύρωση ανάπτυξης.

11.8.3 DSS05 - Διαχείριση υπηρεσιών ασφάλειας: Ευθυγραμμίζεται με την παρακολούθηση και προστασία συστημάτων που αναπτύσσονται εξωτερικά ή από τρίτα μέρη.