					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P25S					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	Ρήτρα 8	Επιχειρησιακοί έλεγχοι, συμπεριλαμβανομένης της ασφάλειας εφαρμογών
ISO/IEC 27002:2022	Έλεγχοι 8.25–8.26	Ασφαλής σχεδιασμός, ανάπτυξη, δοκιμές και ανασκόπηση κώδικα
NIST SP 800-53 Rev.5	SA-11, SI-10	Δοκιμές από προγραμματιστές/εφαρμογές, ανάλυση κώδικα, πρόληψη σφαλμάτων
ΓΚΠΔ της ΕΕ	Άρθρο 25	Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a), (e)	Τεχνικά μέτρα για την ασφάλεια εφαρμογών και τον εντοπισμό κινδύνων
Κανονισμός DORA της ΕΕ	Άρθρα 9(2)(c), 10(2)(c)	Ασφάλεια εφαρμογών για ψηφιακή επιχειρησιακή ανθεκτικότητα
COBIT 2019	BAI03	Διαχείριση της ασφαλούς ανάπτυξης/απόκτησης λογισμικού

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τους ελάχιστους υποχρεωτικούς ελέγχους ασφάλειας εφαρμογών που απαιτούνται για όλες τις λύσεις λογισμικού και συστημάτων που χρησιμοποιεί ο οργανισμός, ανεξαρτήτως του αν αναπτύσσονται εσωτερικά ή προμηθεύονται από εξωτερικούς προμηθευτές ή άλλους τρίτους.

1.2 Διασφαλίζει ότι οι εφαρμογές σχεδιάζονται, υλοποιούνται και συντηρούνται κατά τρόπο που προστατεύει τα δεδομένα πελατών, εργαζομένων και της επιχείρησης από μη εξουσιοδοτημένη πρόσβαση, κακή χρήση, αλλοίωση ή καταστροφή.

1.3 Η παρούσα πολιτική υποστηρίζει τις προσπάθειες του οργανισμού για την επίτευξη και διατήρηση πιστοποίησης ISO/IEC 27001, τη συμμόρφωση με τις υποχρεώσεις του ΓΚΠΔ της ΕΕ και της Οδηγίας NIS2 της ΕΕ, καθώς και τη μείωση των λειτουργικών κινδύνων που συνδέονται με μη ασφαλείς εγκαταστάσεις λογισμικού.

1.4 Συμβάλλει στη δημιουργία συνεπούς και ελέγξιμης προσέγγισης στην ασφάλεια εφαρμογών για ΜΜΕ, μέσω της θέσπισης ενιαίου καταλόγου ελέγχου χαρακτηριστικών και πρακτικών ασφάλειας, προσαρμοσμένου σε περιβάλλοντα με περιορισμένους εσωτερικούς τεχνικούς πόρους.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλες τις εφαρμογές, τα συστήματα, τα εργαλεία και τις πλατφόρμες που:

2.1.1 Αναπτύσσονται εσωτερικά, παραμετροποιούνται ή υλοποιούνται με δέσμες ενεργειών για εσωτερική χρήση

2.1.2 Αποκτώνται ως εμπορικό λογισμικό, λογισμικό ως υπηρεσία (SaaS) ή πλατφόρμες που βασίζονται σε υπολογιστικό νέφος

2.1.3 Επεξεργάζονται, αποθηκεύουν ή διαβιβάζουν δεδομένα προσωπικού χαρακτήρα, επιχειρησιακά αρχεία ή ευαίσθητες λειτουργικές πληροφορίες

2.1.4 Είναι προσβάσιμες από εργαζομένους, αναδόχους, πελάτες ή συνεργάτες μέσω εσωτερικών δικτύων, του διαδικτύου ή φορητών πλατφορμών

2.2 Η πολιτική καλύπτει:

2.2.1 Προγραμματιστές (εσωτερικούς ή εξωτερικούς συνεργάτες)

2.2.2 Προμηθευτές λογισμικού και παρόχους υπηρεσιών νέφους

2.2.3 Προσωπικό υποστήριξης Πληροφορικής ή διαχειριστές ΤΠ που είναι υπεύθυνοι για την εγκατάσταση και την υποστήριξη

2.2.4 Ιδιοκτήτες Εφαρμογών και επιχειρησιακούς χρήστες που συμμετέχουν στην έγκριση συστημάτων και στην εποπτεία τους

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλες οι εφαρμογές που χρησιμοποιεί ο οργανισμός διαθέτουν ενσωματωμένους και επαληθεύσιμους ελέγχους ασφάλειας, οι οποίοι μετριάζουν συνήθεις ευπάθειες λογισμικού.

3.2 Να προστατεύεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων που υποβάλλονται σε επεξεργασία από εφαρμογές, ανεξαρτήτως του τόπου φιλοξενίας τους.

3.3 Να απαιτούνται επίσημες δοκιμές, ανασκόπηση και επικύρωση της ασφάλειας εφαρμογών πριν από την έγκριση οποιασδήποτε νέας εφαρμογής ή σημαντικής επικαιροποίησης για χρήση σε περιβάλλον παραγωγής.

3.4 Να διασφαλίζεται ο συνεπής και ασφαλής χειρισμός διαπιστευτηρίων χρηστών, δεδομένων συνεδρίας και δικαιωμάτων πρόσβασης σε όλα τα επιχειρησιακά κρίσιμα συστήματα.

3.5 Να απαιτούνται ασφαλής καταγραφή, δυνατότητες ελέγχου και δυνατότητες παρακολούθησης σε όλες τις εφαρμογές, ώστε να υποστηρίζεται ο εντοπισμός ύποπτης δραστηριότητας και η απόκριση σε αυτήν.

3.6 Να μειώνονται οι νομικοί και κανονιστικοί κίνδυνοι, διασφαλίζοντας ότι οι εφαρμογές συμμορφώνονται με τις ισχύουσες κανονιστικές απαιτήσεις ασφάλειας.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Έχει τη συνολική λογοδοσία για την ασφάλεια εφαρμογών σε όλο τον οργανισμό.

4.1.2 Εγκρίνει την παρούσα πολιτική και διασφαλίζει ότι όλες οι προμήθειες ή τα έργα ανάπτυξης συμμορφώνονται με αυτήν.

4.1.3 Διασφαλίζει ότι οι προμηθευτές και οι πάροχοι υπηρεσιών δεσμεύονται συμβατικά ως προς τις απαιτήσεις ασφάλειας εφαρμογών.

4.1.4 Ανασκοπεί και εγκρίνει εξαιρέσεις κινδύνου όταν δεν είναι δυνατή η πλήρης συμμόρφωση λόγω επιχειρησιακών περιορισμών.

4.2 Ιδιοκτήτης Εφαρμογής (εφόσον έχει οριστεί)

4.2.1 Προσδιορίζει τις ειδικές απαιτήσεις ασφάλειας της εφαρμογής κατά την επιλογή συστήματος ή την έναρξη έργου.

4.2.2 Επαληθεύει ότι περιλαμβάνονται βασικά χαρακτηριστικά, όπως η ασφαλής σύνδεση, η κρυπτογράφηση και τα αρχεία καταγραφής δραστηριότητας.

4.2.3 Συμμετέχει στις ανασκοπήσεις πριν από την εγκατάσταση και επιβεβαιώνει ότι οι έλεγχοι ασφάλειας καλύπτουν τις επιχειρησιακές ανάγκες.

[... 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 ανά ημερολογιακό έτος, ώστε να:

9.1.1 Αντανακλά μεταβολές στις κανονιστικές απαιτήσεις (π.χ. ΓΚΠΔ της ΕΕ, Οδηγία NIS2 της ΕΕ, Κανονισμός DORA της ΕΕ)

9.1.2 Ενσωματώνει νέες ή αναδυόμενες απειλές και τεχνικές επίθεσης

9.1.3 Επικαιροποιεί τη διατύπωση και τις απαιτήσεις ώστε να αντανακλούν μεταβολές σε πλατφόρμες, προμηθευτές ή μεθόδους ανάπτυξης

9.2 Ενδιάμεσες ανασκοπήσεις πρέπει επίσης να διενεργούνται όταν:

9.2.1 Εισάγονται νέες εφαρμογές

9.2.2 Υφιστάμενες εφαρμογές υφίστανται σημαντικές επικαιροποιήσεις ή διασυνδέσεις

9.2.3 Συμβαίνει περιστατικό ή παραβίαση σχετιζόμενη με εφαρμογή

9.2.4 Εντοπίζονται νέοι κίνδυνοι από εξωτερικές ειδοποιήσεις ή κλαδικές προειδοποιήσεις

9.3 Όλες οι επικαιροποιήσεις της παρούσας πολιτικής πρέπει να:

9.3.1 Εγκρίνονται από τον Γενικό Διευθυντή

9.3.2 Τεκμηριώνονται με ιστορικό εκδόσεων και αιτιολόγηση της αλλαγής

9.3.3 Γνωστοποιούνται σε όλους τους εργαζομένους, προγραμματιστές και προμηθευτές που εμπλέκονται στη διαχείριση εφαρμογών

9.3.4 Αποθηκεύονται με ασφαλή τρόπο για αναφορά σε ελέγχους και συμμόρφωση

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζεται άμεσα από τις ακόλουθες πολιτικές ασφάλειας ευθυγραμμισμένες με ΜΜΕ και συμβάλλει στην εφαρμογή τους:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Αναθέτει την ευθύνη για την έγκριση εφαρμογών, την εφαρμογή της πολιτικής και τη διαχείριση προμηθευτών.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Διασφαλίζει ότι η πρόσβαση σε εφαρμογές ευθυγραμμίζεται με την αρχή των ελαχίστων προνομίων και τις αρχές ελέγχου συνεδρίας.

10.1.3 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι οι χρήστες και οι προγραμματιστές εκπαιδεύονται στην αναγνώριση και αναφορά απειλών που σχετίζονται με εφαρμογές.

10.1.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Παρέχει δικλίδες ιδιωτικότητας δεδομένων που πρέπει να εφαρμόζονται από κάθε εφαρμογή που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα.

10.1.5 P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Καθορίζει πώς τα αρχεία καταγραφής, τα αντίγραφα ασφαλείας και τα ευαίσθητα δεδομένα που παράγονται από εφαρμογές πρέπει να διατηρούνται, να αρχειοθετούνται και να καταστρέφονται με ασφαλή τρόπο.

10.1.6 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Περιγράφει τα βήματα για τον εντοπισμό, την αναφορά και τον περιορισμό συμβάντων ασφάλειας που σχετίζονται με εφαρμογές.

10.2 Από κοινού, οι πολιτικές αυτές διασφαλίζουν ότι η ασφάλεια εφαρμογών έχει ενσωματωθεί πλήρως στο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) του οργανισμού και υποστηρίζει την ετοιμότητα ελέγχου.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Η Ρήτρα 8.1 απαιτεί από τους οργανισμούς να θεσπίζουν επιχειρησιακούς ελέγχους για την αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών, συμπεριλαμβανομένων εκείνων που σχετίζονται με εφαρμογές και συστήματα λογισμικού.

11.2 ISO/IEC 27002

11.2.1 Ο Έλεγχος 8.25 συνιστά την εφαρμογή πρακτικών ασφαλούς σχεδιασμού, ανάπτυξης και ανασκόπησης κώδικα σε όλες τις εφαρμογές, συμπεριλαμβανομένων εκείνων που παρέχονται από προμηθευτές.

11.2.2 Ο Έλεγχος 8.26 συνιστά επίσημες δοκιμές των ελέγχων ασφάλειας εφαρμογών, ιδίως σε τομείς που περιλαμβάνουν έλεγχο πρόσβασης, επικύρωση εισόδου και διαχείριση συνεδρίας.

11.3 NIST SP 800-53 Rev.5

11.3.1 Το SA-11 καθορίζει απαιτήσεις για δοκιμές από προγραμματιστές, ανάλυση κώδικα και δυναμική σάρωση εφαρμογών πριν από την εγκατάσταση.

11.3.2 Το SI-10 καλύπτει τον εντοπισμό και την πρόληψη συνήθων σφαλμάτων λογισμικού, με έμφαση στην ευαισθητοποίηση των προγραμματιστών και στις τεχνικές δικλίδες ασφαλείας.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Το Άρθρο 25, «προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού», επιβάλλει την ενσωμάτωση της ιδιωτικότητας και της ασφάλειας στον βασικό σχεδιασμό εφαρμογών που χειρίζονται δεδομένα προσωπικού χαρακτήρα.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Το Άρθρο 21(2)(a) και (e) απαιτεί από ουσιώδεις και σημαντικές οντότητες να εφαρμόζουν τεχνικά μέτρα για την ασφάλεια εφαρμογών και τον εντοπισμό κινδύνων που σχετίζονται με το λογισμικό.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Το Άρθρο 9(2)(c), 10(2)(c) απαιτεί από ΜΜΕ του χρηματοοικονομικού τομέα να ενσωματώνουν ελέγχους ασφάλειας σε επίπεδο εφαρμογής και να διενεργούν τακτικές αξιολογήσεις για τη διατήρηση της ψηφιακής επιχειρησιακής ανθεκτικότητας.

11.7 COBIT 2019

11.7.1 Το BAI03, «Manage Solutions Identification and Build», καθοδηγεί την ανάπτυξη ή απόκτηση ασφαλούς λογισμικού ευθυγραμμισμένου με τον κίνδυνο, τη συμμόρφωση και τις επιχειρησιακές απαιτήσεις, ακόμη και σε περιβάλλοντα ΜΜΕ με περιορισμένους πόρους.