Όνομα Οργανισμού

Πολιτική Ασφάλειας Συστημάτων και Εφαρμογών

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Ασφάλειας Συστημάτων & Εφαρμογών |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

Πίνακας Περιεχομένων

[1. Εισαγωγή 4](#_Toc188534312)

[1.1. Σκοπός 4](#_Toc188534313)

[1.2. Πεδίο Εφαρμογής 4](#_Toc188534314)

[2. Πολιτική Ασφαλείας Συστημάτων & Εφαρμογών 5](#_Toc188534315)

[2.1. Καταπολέμηση κακόβουλου λογισμικού 5](#_Toc188534317)

[2.2. Θωράκιση συστημάτων και βασικές απαιτήσεις ασφάλειας 6](#_Toc188534318)

[2.3. Ασφάλεια κινητών συσκευών 6](#_Toc188534319)

[2.4. Άλλα προτεινόμενα μέτρα προστασίας κινητών συσκευών/φορητού εξοπλισμού 7](#_Toc188534320)

[2.5. Προστασία Λειτουργικών συστημάτων 8](#_Toc188534321)

[3. Ασφάλεια Εφαρμογών 9](#_Toc188534322)

[4. Κύκλος Ζωής Εφαρμογών 11](#_Toc188534323)

[4.1. Σκοπός 11](#_Toc188534324)

[4.2. Καθορισμός Απαιτήσεων 11](#_Toc188534325)

[4.3. Σχεδιασμός 12](#_Toc188534326)

[4.4. Ανάπτυξη και Υλοποίηση 12](#_Toc188534327)

[4.4.1. Διαχωρισμός Περιβάλλοντων 12](#_Toc188534328)

[4.5. Δοκιμή και Εγκατάσταση 13](#_Toc188534329)

[4.6. Μέτρα Εγκατάστασης Εφαρμογών 13](#_Toc188534330)

[4.7. Εγχειρίδια Εφαρμογών 14](#_Toc188534331)

[4.8. Εκπαίδευση Χρηστών 14](#_Toc188534332)

[4.9. Διαδικασία Διαχείρισης Αλλαγών 14](#_Toc188534333)

[5. Ανάθεση Ανάπτυξης σε Τρίτα Μέρη 16](#_Toc188534334)

[6. Αναθεώρηση 16](#_Toc188534335)

[7. Αναφορές 17](#_Toc188534336)

# Εισαγωγή

## Σκοπός

Το παρόν έγγραφο περιλαμβάνει ενδεικτικούς Όρους Πολιτικής για προστασία των πληροφοριακών περιουσιακών στοιχείων και της τεχνολογικής υποδομής του οργανισμού από μια σειρά απειλών. Επιπλέον, περιλαμβάνει όρους ώστε να διασφαλίζει ότι όλες οι εφαρμογές και τα συστήματα που χρησιμοποιούνται εντός του [Όνομα Οργανισμού] σχεδιάζονται, υλοποιούνται, συντηρούνται και προστατεύονται κατάλληλα, καθώς αποτελούν αναπόσπαστο στοιχείο για τη εύρυθμη λειτουργία του [Όνομα Οργανισμού].

Η πολιτική αυτή αποσκοπεί μεταξύ άλλων:

* Στην προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων που υποβάλλονται σε επεξεργασία και αποθηκεύονται σε εφαρμογές και συστήματα.
* Στον καθορισμό απαιτήσεων ασφαλείας για το σχεδιασμό, την ανάπτυξη, τη δοκιμή και την συντήρηση εφαρμογών και συστημάτων.
* Για μετριασμό των κινδύνων που συνδέονται με διάφορες ευπάθειες, επιβάλλοντας την υλοποίηση ασφαλή πρακτικών προγραμματισμού, διαχείρισης διορθώσεων και τακτικές αξιολογήσεις ευπαθειών.
* Τη διασφάλιση της συμμόρφωσης με διάφορα πρότυπα που σχετίζονται με την ασφάλεια εφαρμογών και συστημάτων (π.χ. coding standards).
* Την προώθηση της υπευθυνότητας και της ευαισθητοποίησης σε θέματα ασφάλειας μεταξύ των προγραμματιστών, των διαχειριστών και τελικών χρηστών, προωθώντας μια κουλτούρα ασφαλούς διαχείρισης συστημάτων.

## Πεδίο Εφαρμογής

Η Πολιτική Ασφάλειας Συστημάτων και Εφαρμογών του [Όνομα Οργανισμού] περιλαμβάνει όλα τα πληροφοριακά συστήματα, τις εφαρμογές, λειτουργικά συστήματα και τα συναφή στοιχεία που χρησιμοποιούνται, αναπτύσσονται, διαχειρίζονται ή φιλοξενούνται από τον [Όνομα Οργανισμού], συμπεριλαμβανομένων εκείνων που παρέχονται από τρίτα μέρη στον [Όνομα Οργανισμού] ή διαχειρίζονται εξ ολοκλήρου από εξωτερικούς συνεργάτες.

Εφαρμόζεται σε όλα τα στάδια του κύκλου ζωής των εφαρμογών και των συστημάτων - σχεδιασμός, ανάπτυξη, δοκιμή, συντήρηση και την τελική απόσυρση του.

# Πολιτική Ασφαλείας Συστημάτων & Εφαρμογών



## Καταπολέμηση κακόβουλου λογισμικού

Ο [Όνομα Οργανισμού] προστατεύει τα συστήματα και τις εφαρμογές του από απειλές κακόβουλου λογισμικού μέσω προληπτικών μέτρων. Αυτό περιλαμβάνει την εφαρμογή λύσεων προστασίας από ιούς και άλλο κακόβουλο λογισμικό, τη διεξαγωγή τακτικών σαρώσεων, την έγκαιρη εφαρμογή διορθώσεων και την παρακολούθηση ύποπτων δραστηριοτήτων. Πιο συγκεκριμένα:

* Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί διαδικασία / πολιτική και μέτρα για την προστασία των συστημάτων από μολύνσεις από κακόβουλο λογισμικό και κώδικα, προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των πληροφοριών.
* Σε όλες τις τερματικές συσκευές του [Όνομα Οργανισμού] υπάρχει εγκατεστημένο και διατηρείται ενημερωμένο, λογισμικό προστασίας από ιούς, του οποίου η διαχείριση πραγματοποιείτε μέσω κεντρικοποιημένης πλατφόρμας. Η κεντροποιημένη πλατφόρμα επιτρέπει τη συνεχή παρακολούθηση και αυτόματη ενημέρωση του αρμόδιου προσωπικού σε σχέση με την προστασία από ιούς και κακόβουλο κώδικα σε όλα τα συστήματα (workstations, servers, mobile devices, firewalls, κα).
* Σε όλες τις τερματικές συσκευές, όπου είναι δυνατόν, πρέπει να ενεργοποιούνται μηχανισμοί προστασίας από ιούς, εντοπισμού εισβολών και άλλοι προηγμένοι μηχανισμοί ασφαλείας, όπως το web filtering, μέσω του λογισμικού προστασίας από ιούς.
* Το λογισμικό προστασίας από ιούς πρέπει να είναι κατάλληλα διαμορφωμένο ώστε να διενεργεί τα ακόλουθα:

• αυτόματη σάρωση εισερχομένων

• σάρωση και αποκλεισμός ηλεκτρονικών επικοινωνιών που περιέχουν κακόβουλο κώδικα ή τύπους αρχείων που ενέχουν αυξημένο κίνδυνο

• τακτικές σαρώσεις στα σημεία αποθήκευσης πληροφοριών

• διακοπή αυτόματης έναρξης λογισμικών από διάφορα μέσα

• ειδοποίηση σε περιπτώσεις αναγνώρισης απειλής

• αυτόματη διαγραφή ή απομόνωση των αναγνωρισμένων απειλών

• αυτόματη ενημέρωση του λογισμικού και των υπογραφών

* O [Όνομα Οργανισμού]έχει επιπρόσθετα υλοποιήσει λύσεις antimalware που περιλαμβάνουν δυνατότητες αναγνώρισης ευπαθειών και φίλτρα anti-exploitation για την ενίσχυση της ασφάλειας των συστημάτων.
* Όπου είναι δυνατό ο [Όνομα Οργανισμού] υλοποιεί μηχανισμούς anti-tampering protection ώστε να αποτρέπεται η απενεργοποίηση της σχετικής προστασίας από μη εξουσιοδοτημένα άτομα.

## Θωράκιση συστημάτων και βασικές απαιτήσεις ασφάλειας

Ο [Όνομα Οργανισμού] διασφαλίζει ότι όλες οι εφαρμογές και τα συστήματα έχουν ρυθμιστεί με ασφάλεια μέσω μιας συστηματικής διαδικασίας θωράκισης υπηρεσιών του συστήματος (system hardening). Αυτό περιλαμβάνει την αφαίρεση περιττού λογισμικού, την απενεργοποίηση αχρησιμοποίητων υπηρεσιών και τη διαμόρφωση ρυθμίσεων ασφαλείας για την ελαχιστοποίηση των τρωτών σημείων. Πιο συγκεκριμένα λαμβάνονται τα ακόλουθα μέτρα:

* Στα συστήματα του [Όνομα Οργανισμού]πραγματοποιείται όπου είναι δυνατό κατάργηση υπηρεσιών/ υποστηρικτικών προγραμμάτων που δεν είναι απαραίτητα.
* Στις τερματικές συσκευές του [Όνομα Οργανισμού]εγκαθίσταται host-based firewall, όπου είναι εφικτό, με σκοπό την προστασία από κακόβουλο κώδικα, τον έλεγχο χρήσης αφαιρούμενων μέσων, κτλ.
* Η εγκατάσταση ή παραμετροποίηση του λογισμικού πραγματοποιείται αποκλειστικά από ειδικά εξουσιοδοτημένο προσωπικό του [Όνομα Οργανισμού].
* Ο [Όνομα Οργανισμού] διασφαλίζει ότι οι χρήστες με απλά δικαιώματα (non-privileged) δεν έχουν τη δυνατότητα να απενεργοποιήσουν ή να τροποποιήσουν ρυθμίσεις ασφαλείας στα συστήματα.
* Ο [Όνομα Οργανισμού] να διασφαλίζει ότι οι χρήστες με απλά δικαιώματα (non-privileged) δεν έχουν τη δυνατότητα να εγκαθιστούν λογισμικό σε κρίσιμα συστήματα.
* Για κάθε σύστημα του [Όνομα Οργανισμού] έχει αναγνωριστεί ιδιοκτήτης, ο οποίος σε συνεργασία με το λοιπό τεχνικό προσωπικό, είναι υπεύθυνος για τους ρόλους που απαιτούν πρόσβαση, καθώς και το επίπεδο της πρόσβασης.
* Για κάθε σύστημα του [Όνομα Οργανισμού] πρέπει να διατίθεται αρχείο (golden copy), που περιλαμβάνει την πιο επίκαιρη, σταθερή και ασφαλή παραμετροποίησή του .
* Ο [Όνομα Οργανισμού] πρέπει να ακολουθεί τις οδηγίες ασφαλούς παραμετροποίησης που παρέχονται από τον κατασκευαστή ή άλλες αξιόπιστες πηγές (π.χ. CIS Benchmarks) για την προστασία των συστημάτων του.

## Ασφάλεια κινητών συσκευών

Οι κινητές συσκευές και άλλος φορητός εξοπλισμός διατρέχουν σημαντικό κίνδυνο καθώς μετακινούνται με μεγάλη ευκολία εκτός των εγκαταστάσεων του [Όνομα Οργανισμού]. Ως εκ τούτου αυξάνεται η πιθανότητα να απολεσθεί ή/και να καταστραφεί ή/και να κλαπεί. Καθώς ο κίνδυνος είναι μεγάλος, όλες οι κινητές συσκευές/φορητός εξοπλισμός που έχουν πρόσβαση σε δεδομένα ή συστήματα του [Όνομα Οργανισμού] πρέπει να συμμορφώνονται με τα καθιερωμένα πρωτόκολλα ασφαλείας, συμπεριλαμβανομένης της κρυπτογράφησης των συσκευών, της ασφαλούς πιστοποίησης ταυτότητας και των δυνατοτήτων απομακρυσμένης διαγραφής. Πιο συγκεκριμένα λαμβάνονται τα ακόλουθα μέτρα:

* Ο [Όνομα Οργανισμού] εφαρμόζει και να διατηρεί μέτρα ασφάλειας κινητών συσκευών προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα των πληροφοριών που διαχειρίζονται.
* Όλες οι κινητές συσκευές πρέπει να διαθέτουν επαρκή μέτρα για την προστασία από κλοπή και απώλεια δεδομένων (π.χ. κρυπτογράφηση σε επίπεδο συσκευής, ισχυρή επαλήθευση ταυτότητας, ασφαλής επικοινωνία και δικτύωση (VPN)).
* Όλες οι κινητές συσκευές (συμπεριλαμβανομένων των εφαρμογών τους) που χρησιμοποιούν οργανωτικά δεδομένα του [Όνομα Οργανισμού], πρέπει να διαχειρίζονται από κεντρικό σύστημα διαχείρισης κινητών συσκευών (λύσεις τύπου MDM και MAM).

## Άλλα προτεινόμενα μέτρα προστασίας κινητών συσκευών/φορητού εξοπλισμού

* Μόνο εξουσιοδοτημένο προσωπικό μπορεί να χρησιμοποιεί, για λογαριασμό του [Όνομα Οργανισμού], φορητό εξοπλισμό. Νοείται ότι το προσωπικό θα πρέπει παράλληλα να συμμορφώνεται με την Πολιτική Αποδεκτής Χρήσης.
* Ο φορητός εξοπλισμός που παραδίδεται σε εξουσιοδοτημένο χρήστη τηρείται σε σχετικό μητρώο. Ο εξοπλισμός επιστρέφεται σε περίπτωση τερματισμού απασχόλησης ή δεν όταν αυτός δεν είναι πλέον απαραίτητος για την άσκηση των καθηκόντων.
* Μόνο εξουσιοδοτημένος φορητός εξοπλισμός επιτρέπεται να χρησιμοποιείται στις εγκαταστάσεις του [Όνομα Οργανισμού].
* Απαγορεύεται η χρήση εξουσιοδοτημένου φορητού εξοπλισμού για το προσωπικό όφελος του χρήστη.
* Ο [Όνομα Οργανισμού] διατηρεί το δικαίωμα παρακολούθησης του φορητού εξοπλισμού, καθώς και το δικαίωμα ανάκτησης, τροποποίησης, διαγραφής και εφεδρείας της οποιασδήποτε αποθηκευμένης πληροφορίας στον εξοπλισμό αυτό, χωρίς προηγούμενη ενημέρωση εάν αφορά θέματα ασφάλειας πληροφοριών του Οργανισμού.
* Ο [Όνομα Οργανισμού] διατηρεί το δικαίωμα αναίρεσης της οποιασδήποτε σχετικής εξουσιοδότησης εφόσον η χρήση τέτοιας συσκευής αποτελεί πηγή κινδύνου για την ασφάλεια των συστημάτων και πληροφοριών του [Όνομα Οργανισμού].
* Ο φορητός εξοπλισμός θα πρέπει να κλειδώνεται αυτόματα όταν δεν χρησιμοποιείται **πέραν των** [XX] **λεπτών**.
* Όπου είναι δυνατό ο φορητός εξοπλισμός πρέπει να προστατεύεται από λογισμικό αντιμετώπισης κακόβουλων λογισμικών.
* Ο φορητός εξοπλισμός πρέπει να προστατεύεται από το τοπικό Firewall, ειδικά σε περιπτώσεις που θα συνδέεται σε άγνωστα ή/ και μη αξιόπιστα ή/ και δημόσια δίκτυα (βλέπε Πολιτική Ασφάλειας Δικτύου).
* Ο φορητός εξοπλισμός πρέπει να προστατεύεται με λογισμικό απώλειας δεδομένων (DLP) το οποίο ανιχνεύει και αποτρέπει μη εξουσιοδοτημένες μεταφορές δεδομένων.

## Προστασία Λειτουργικών συστημάτων

Για την ετοιμασία και διαμόρφωση των λειτουργικών συστημάτων (Operating Systems) θα πρέπει να καθοριστεί και να ακολουθείται διαδικασία ρύθμισης πρωτότυπων λειτουργικών συστημάτων. H διαδικασία μεταξύ άλλων περιλαμβάνει τα ακόλουθα:

* αναθεώρηση των βέλτιστων πρακτικών ασφαλούς διαμόρφωσης λειτουργικών συστημάτων.
* τη ρύθμιση των λειτουργικών συστημάτων λαμβάνοντας υπόψη τις βέλτιστες πρακτικές ασφαλείς διαμορφώσεις του εκάστοτε λειτουργικού συστήματος (system hardening)
* τη διεξαγωγή δοκίμων λειτουργίας και ασφάλειας.
* ετήσια αναθεώρηση των λειτουργικών συστημάτων. Οι οποιεσδήποτε επιπρόσθετες ρυθμίσεις ασφαλείας και οι οποιεσδήποτε ενημερώσεις ασφάλειας πρέπει να γίνονται/εγκαθίστανται ετησίως.

Περαιτέρω τα Λειτουργικά Συστήματα:

* που βρίσκονται στο εσωτερικό δίκτυο του [Όνομα Οργανισμού], όπου είναι εφικτό, πρέπει να είναι μέλη ενός Domain.
* που πρέπει να είναι εκτιθέμενα σε εξωτερικό δίκτυο συστήνεται όπως βρίσκονται σε ξεχωριστό περιμετρικό τμήμα δικτύου, απομονωμένο και διαχωρισμένο από το υπόλοιπο εσωτερικό δίκτυο, ώστε να υπάρχει ένα επιπλέον επίπεδο ασφαλείας. Εάν είναι απαραίτητο, θα πρέπει να δημιουργείτε ένας ξεχωριστός τομέας στο Active Directory (AD) ειδικά για τα συστήματα DMZ χωρίς σχέση εμπιστοσύνης με τον εσωτερικό τομέα.
* πρέπει να είναι συγχρονισμένα σε κεντρικό σύστημα τύπου NTP (Πρωτόκολλο Χρόνου Δικτύου) για τον ομοιόμορφο καθορισμό της ώρας / ημερομηνίας.
* πρέπει να έχουν εγκατεστημένες τις τελευταίες ενημερώσεις και αναβαθμίσεις ανάλογα και με την κρισιμότητα τους.
* πρέπει να έχουν εγκατεστημένες μόνο τις εξουσιοδοτημένες, από τον [Όνομα Οργανισμού], εφαρμογές. Οι εν λόγω εφαρμογές πρέπει να είναι ενημερωμένες με τις τελευταίες ενημερώσεις ασφαλείας.
* οι προκαθορισμένοι λογαριασμοί όπως «administrator», «root», «guest», «default» θα πρέπει να είναι απενεργοποιημένοι
* πρέπει να προστατεύονται με κωδικούς ασφάλειας. Οι κωδικοί θα πρέπει να συμμορφώνονται σύμφωνα με την Πολιτική Ελέγχου Πρόσβασης και όπου είναι δυνατό να γίνεται χρήση MFA.
* όπου είναι δυνατό οι δίσκοι να είναι κρυπτογραφημένοι.
* πρέπει να είναι ενεργοποιημένες μόνο οι αναγκαίες υπηρεσίες. Υπηρεσίες για τις οποίες δεν υπάρχει υπηρεσιακή ανάγκη θα πρέπει να είναι απενεργοποιημένες όπως η υπηρεσία Bluetooth και WiFi.
* όπου είναι εφικτό θα πρέπει να έχουν απενεργοποιημένη την επιλογή εκκίνησης του λειτουργικού συστήματος από εναλλακτικές πήγες εκτός του πρωτεύοντος σκληρού δίσκου.
* πρέπει να κλειδώνονται αυτόματα όταν δεν χρησιμοποιούνται πέραν των 15 λεπτών και 5 λεπτών όταν είναι συστήματα υψηλού κινδύνου.
* πρέπει να προστατεύονται με λογισμικό αντιμετώπισης κακόβουλων λογισμικών.
* πρέπει να έχουν απενεργοποιημένη την απομακρυσμένη πρόσβαση όταν δεν είναι αναγκαία. Μόνο εξουσιοδοτημένα άτομα θα πρέπει να μπορούν να έχουν απομακρυσμένη πρόσβαση.
* πρέπει να έχουν ενεργοποιημένο το τοπικό Firewall ενώ μόνο οι αναγκαίες θύρες (ports) πρέπει να είναι ανοικτές.
* πρέπει να αποφεύγεται η χρήση σε αυτά κοινών φακέλων (shared folders). Σε περίπτωση που υπάρχει ανάγκη για κοινόχρηστους φακέλους τα κατάλληλα δικαιώματα πρόσβασης πρέπει να καθορίζονται και να αναθεωρούνται τακτικά.
* η παράμετρος autorun θα πρέπει να είναι απενεργοποιημένη.
* για κάθε στοιχείο λογισμικού να αναγνωριστεί ιδιοκτήτης ο οποίος σε συνεργασία με το λοιπό τεχνικό προσωπικό, θα προσδιορίζει τους ρόλους για τους οποίους απαιτείται πρόσβαση(στο λογισμικό) καθώς και το επίπεδο της πρόσβασης.

# Ασφάλεια Εφαρμογών

Η ασφάλεια των εξατομικευμένων (customised) εφαρμογών αποτελεί σημαντική παράμετρος του συνολικού πλαισίου κυβερνοασφάλειας του [Όνομα Οργανισμού], διασφαλίζοντας ότι οι εφαρμογές σχεδιάζονται, αναπτύσσονται και συντηρούνται με ισχυρή προστασία έναντι ευπαθειών και απειλών. Με την ενσωμάτωση πρακτικών ασφαλούς κωδικοποίησης, σενάρια δοκιμών και συνεχούς παρακολούθησης, ο [Όνομα Οργανισμού] στοχεύει στην προστασία των εφαρμογών κινδύνους σχετικούς με την ασφάλεια πληροφορικών και το κυβερνοχώρο. Πιο συγκεκριμένα:

* Ο [Όνομα Οργανισμού] έχει θεσπίσει διαδικασία ασφαλούς διαχείρισης του κύκλου ανάπτυξης λογισμικού (Secure Development Lifecycle). Βλέπε ενότητα 4 πιο κάτω.
* Ο [Όνομα Οργανισμού] έχει θεσπίσει απαιτήσεις ασφάλειας για τις εφαρμογές και τα λογισμικά που αναπτύσσονται, οι οποίες λαμβάνονται υπόψη σε κάθε νέα ανάπτυξη εφαρμογής ή λογισμικού.
* Στα τελικά στάδια της ανάπτυξης και πριν την μεταφορά στο παραγωγικό περιβάλλον, πρέπει να διεξάγονται δοκιμές του συστήματος, σύμφωνα με τα καθορισμένα κριτήρια και τις απαιτήσεις ποιότητας, λειτουργικότητας και ασφάλειας.
* Πρέπει να διατηρούνται ξεχωριστά περιβάλλοντα ανάπτυξης και παραγωγής.
* Κατά τη διεξαγωγή δοκιμών ανάπτυξης εφαρμογών, πρέπει να χρησιμοποιούνται ανώνυμα δεδομένα.
* Σε περίπτωση που η ανάπτυξη εφαρμογών ανατίθεται σε τρίτα μέρη, πρέπει να παρέχονται τουλάχιστον προδιαγραφές ασφαλείας που πρέπει να ικανοποιεί η εφαρμογή. Πρέπει να ζητούνται επίσης επαρκείς εγγυήσεις, διαβεβαιώσεις και στοιχεία που επιβεβαιώνουν την κάλυψη των απαιτήσεων αυτών πριν την αποδοχή ή τη λειτουργία της εφαρμογής.
* Ο [Όνομα Οργανισμού] πρέπει να διαθέτει οδηγίες για ασφαλή ανάπτυξη λογισμικού, εξειδικευμένες ανά γλώσσα ή περιβάλλον ανάπτυξης (coding standards), σύμφωνα με διεθνείς βέλτιστες πρακτικές.
* Πρέπει να διενεργούνται risk assessments και/ή threat profiling κατά τον σχεδιασμό ενός λογισμικού για τον καθορισμό των μέτρων ασφαλείας του.
* Οι εφαρμογές και τα λογισμικά πρέπει να αναπτύσσονται βάσει των αρχών "security and privacy by design".
* Πρέπει να διενεργούνται κατ’ελάχιστο τα ακόλουθα:
  + αξιολόγηση κινδύνου στο αρχικό στάδιο του έργου,
  + δοκιμές ασφάλειας και εξέταση κώδικα στα στάδια ανάπτυξης του έργου,
  + αξιολόγηση ασφάλειας και ασφαλούς διαμόρφωσης στην παράδοση του έργου.
* Πρέπει να υφίσταται πλήρης διαχωρισμός καθηκόντων ανάμεσα στο προσωπικό που διενεργεί την ανάπτυξη, τις δοκιμές και την παραγωγική λειτουργία των συστημάτων.
* Αλλαγές στο λογισμικό πρέπει να γίνονται μέσα από την διαδικασία διαχείρισης αλλαγών.

# Κύκλος Ζωής Εφαρμογών

Σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] οφείλει να διασφαλίσει επαρκή μέτρα ασφάλειας στο πλαίσιο των δραστηριοτήτων ανάπτυξης λογισμικού που αναπτύσσει ο οργανισμός. Η διαχείριση του κύκλου ανάπτυξης λογισμικού (Software Development Life Cycle - SDLC) αποτελεί κρίσιμο κομμάτι της διαδικασίας ανάπτυξης λογισμικού. Ο κύκλος ανάπτυξης λογισμικού (SDLC) αναφέρεται στη σειρά των διαδικασιών και των σταδίων που περνά ένα λογισμικό από τη σχεδίαση μέχρι την υλοποίηση, τον έλεγχο ποιότητας, την διασφάλιση, την συντήρηση και, τελικά, την απόσυρση. Κάθε στάδιο έχει τις δικές του πρακτικές και διαδικασίες, και είναι σχεδιασμένο για να εξασφαλίζει την ποιότητα, την ασφάλεια, και τη δυνατότητα συντήρησης του λογισμικού κατά τη διάρκεια όλου του κύκλου ζωής του.

Όλες οι εφαρμογές πρέπει να συνοδεύονται από το εγχειρίδιο του κύκλου ζωής τους. Έμφαση πρέπει να δοθεί στη γενική ασφάλεια της εφαρμογής και στην προστασία του περιεχομένου (data) αυτής. Σε κάθε στάδιο του κύκλου ζωής θα πρέπει να χρησιμοποιούνται δικλείδες ασφαλείας όπως κρυπτογράφηση.

Για κάθε ανάπτυξη νέας εφαρμογής θα πρέπει να δημιουργείτε καινούργιο χωριστό έργο και σε κάθε καινούργιο έργο θα πρέπει να τηρούνται μέτρα ασφαλείας όπου θα είναι ενσωματωμένα στον κύκλο ζωής. Κατά το κύκλο ζωής μίας εφαρμογής θα πρέπει να τηρούνται τουλάχιστο τα παρακάτω στάδια/ενέργειες:



## Σκοπός

* Η εφαρμογή πρέπει να αξιολογηθεί και να χαρακτηριστεί με το ανάλογο επίπεδο επικινδυνότητας.
* Έχοντας υπόψη τη διαβάθμιση πληροφοριών, οι νέες ή αναθεωρημένες εφαρμογές πρέπει να αξιολογηθούν σχετικώς.
* Το επίπεδο πρόσβασης που απαιτείται από ομάδες χρηστών πρέπει να καθοριστεί σύμφωνα με τη λειτουργικότητα της εφαρμογής.
* Οποιαδήποτε άλλα μέτρα ασφαλείας πρέπει να εντοπιστούν.

## Καθορισμός Απαιτήσεων

Σε σχέση με τη ασφάλεια πληροφορικών, για κάθε εφαρμογή πρέπει να προσδιορίζονται και να καταγράφονται. τα πιο κάτω:

* Τα δικαιώματα και οι ρόλοι των χρηστών ανάλογα με τη θέση εργασίας τους. Περιττά δικαιώματα αναιρούνται.
* Οι ανάγκες για την προστασία της εφαρμογής από κακόβουλο λογισμικό
* Σχέδιο εφεδρείας και ανάκτησης των πληροφοριών και της εφαρμογής
* Διαδικασία Διαχείρισης Αλλαγών.
* Διαδικασία διαχείρισης του κύκλου ανάπτυξης λογισμικού

## Σχεδιασμός

Ο σχεδιασμός της κάθε εφαρμογής πρέπει να συμπεριλαμβάνει την εκπλήρωση των απαιτήσεων της εφαρμογής και το πώς θα αναμένεται να υλοποιηθεί. Κατά την διάρκεια του σχεδιασμού θα πρέπει να διενεργείτε αξιολόγηση κινδύνου (risk assessment) ή καθορισμός απειλών (threat profiling) και σύμφωνα με τα αποτελέσματα θα σχεδιάζονται τα κατάλληλα μέτρα ασφαλείας.

Η αξιολόγηση κινδύνου και το threat profiling είναι σημαντικά στοιχεία της διαδικασίας ανάπτυξης εφαρμογών. Με την αξιολόγηση κινδύνων θα πρέπει να πραγματοποιηθεί

• Αναγνώριση και καταγραφή δυνητικών κινδύνων για το λογισμικό.

• Καθορισμός της πιθανότητας εκδήλωσης κάθε κινδύνου και του αντίκτυπου του στην προτεινόμενη εφαρμογή..

• Κατάταξη των κινδύνων με βάση τη σοβαρότητα τους.

Με το καθορισμός απειλών θα πρέπει να πραγματοποιείται:

• Αναγνώριση πιθανών απειλών (threats) στο περιβάλλον του λογισμικού.

• Ανάλυση των δυνητικών απειλών για τον κώδικα, τα δεδομένα και την ευπάθεια του συστήματος

## Ανάπτυξη και Υλοποίηση

Κατά τη διάρκεια της ανάπτυξης της εφαρμογής πρέπει να διενεργούνται σχέδια δοκιμών καθώς και σενάρια διείσδυσης της ασφάλειας της εφαρμογής. Επιπρόσθετα θα πρέπει να υλοποιούνται μέτρα για τον διαχωρισμό των περιβαλλόντων ανάπτυξης λογισμικού και ελέγχου από το επιχειρησιακό περιβάλλον παραγωγής.

## Διαχωρισμός Περιβάλλοντων

Ο διαχωρισμός των περιβαλλόντων ανάπτυξης εφαρμογών από το περιβάλλον παραγωγής είναι σημαντικός για την ασφάλεια, την αξιοπιστία και τη σταθερότητα των συστημάτων. Αυτό γίνεται με την εφαρμογή κατάλληλων μέτρων. Πιο αναλυτικά:

1. Διαχωρισμός Υποδομών: Η ανάπτυξη εφαρμογών πραγματοποιείτε πάντοτε σε ένα περιβάλλον ανάπτυξης, ενώ το περιβάλλον παραγωγής βρίσκεται σε ένα διαφορετικό περιβάλλον. Αυτός ο διαχωρισμός εξασφαλίζει ότι τυχόν σφάλματα ή προβλήματα που μπορεί να προκύψουν κατά την ανάπτυξη δεν θα επηρεάσουν τον παραγωγικό κώδικα.
2. Χρήση Αντιγράφων Βάσεων Δεδομένων: κατά τη διάρκεια της ανάπτυξης, συστήνεται όπως χρησιμοποιούνται αντίγραφα των βάσεων δεδομένων. Είναι σημαντικό να ελέγχεται προσεκτικά η χρήση αυτών των δεδομένων ώστε να μην επηρεάζεται η παραγωγική βάση δεδομένων.
3. Καθαρισμός Δεδομένων: Κατά τη μετάβαση από το περιβάλλον ανάπτυξης στο περιβάλλον παραγωγής, πρέπει να διασφαλίζεται ότι τα δεδομένα είναι καθαρά απαλλαγμένα από δεδομένα που δεν έπρεπε να υπάρχουν σε αυτό και λανθασμένα μεταφέρθηκαν από το περιβάλλον ανάπτυξης.
4. Κανόνες Εφαρμογής: Θα πρέπει να υπάρχει καταγραμμένη διαδικασίας μεταφοράς κώδικα και δεδομένων από το περιβάλλον ανάπτυξης, ελέγχου στο περιβάλλον παραγωγής.

Αυτά τα μέτρα βοηθούν στο να διατηρείται η ασφάλεια και η σταθερότητα των παραγωγικών συστημάτων, ενώ παράλληλα επιτρέπεται η αποτελεσματική ανάπτυξη και δοκιμή του λογισμικού.

## Δοκιμή και Εγκατάσταση

Δοκιμές για τη λειτουργικότητα και ασφάλεια της εφαρμογής πρέπει να γίνουν πριν την εγκατάσταση της εφαρμογής. Αν η εφαρμογή αποτύχει στις δοκιμές αυτές, η εφαρμογή πρέπει να επιστρέψει στην αρχική φάση του κύκλου ζωής. Οποιαδήποτε δεδομένα χρησιμοποιούνται για τη διενέργεια δοκιμών θα πρέπει να είναι ανώνυμα και να μην συνδέονται με εμπιστευτικές και ευαίσθητες πληροφορίες.

Για να διασφαλίσει ο οργανισμός την ανωνυμία και την προστασία των ευαίσθητων πληροφοριών κατά τη διενέργεια δοκιμών, μπορεί να λάβει τα παρακάτω μέτρα:

1. Ανωνυμοποίηση Δεδομένων: Τα προσωπικά δεδομένα που χρησιμοποιούνται για τις δοκιμές πρέπει να υποβληθούν σε ανωνυμοποίηση (Data Masking & Anonymization). Με αυτή τη πρακτική, αφαιρούνται ή αντικαθίστανται τα στοιχεία που μπορούν να οδηγήσουν στην αναγνώριση του ατόμου.
2. Χρήση Δοκιμαστικών Βάσεων Δεδομένων: Μπορεί να χρησιμοποιηθούν ειδικές δοκιμαστικές βάσεις δεδομένων που περιλαμβάνουν ψευδή ή ανωνυμοποιημένα δεδομένα για τις δοκιμές, αντί να χρησιμοποιούνται πραγματικά δεδομένα πελατών ή χρηστών.
3. Περιορισμός Πρόσβασης: Πρέπει να επιβάλλονται περιορισμοί πρόσβασης, και μόνο τα απαραίτητα άτομα θα πρέπει να έχουν πρόσβαση ακόμα και σε ευαίσθητα δεδομένα για τις δοκιμές
4. Εκπαίδευση Προσωπικού: Το προσωπικό που εμπλέκεται στις δοκιμές πρέπει να είναι εκπαιδευμένο σχετικά με τη σημασία της προστασίας της ανωνυμίας και της ευαισθησίας των δεδομένων.

Με αυτά τα μέτρα, ο [Όνομα Οργανισμός] διασφαλίζει ότι οι δοκιμές γίνονται με ασφάλεια και περιορίζει τυχόν παραβίαση της ανωνυμίας των πληροφοριών.

## Μέτρα Εγκατάστασης Εφαρμογών

Πριν από την εγκατάσταση των εφαρμογών, γίνεται λεπτομερής ανάλυση των απαιτήσεων τους, λαμβάνοντας υπόψη τη λειτουργία τους, τις ανάγκες ασφαλείας και τους ενδεχόμενους κινδύνους σύμφωνα με το [AS1] της Απόφασης Κ.Δ.Π 389/2020.

Ορίζονται και ανατίθενται συγκεκριμένα δικαιώματα πρόσβασης στους χρήστες, με βάση την αρχή των λιγότερων προνομίων (principle of least privilege). Κατά την εγκατάσταση, εφαρμόζονται τεχνικές όπως η χρήση υπογεγραμμένων εφαρμογών, κρυπτογραφημένων συνδέσεων, και ελεγχόμενων περιβαλλόντων εκτέλεσης.

Κατά τη διάρκεια της λειτουργίας, οι εφαρμογές υπόκεινται σε συνεχή παρακολούθηση με τη χρήση συστημάτων ανίχνευσης και απεικόνισης συμπεριφοράς και συστημάτων παρακολούθησης αποστολής καταγραφικών αρχείων. Επιπλέον, τα κρίσιμα συστήματα διαθέτουν προηγμένα μέτρα τροποποίησης των ρυθμίσεων ασφαλείας, όπως αυτόματες ενημερώσεις και συχνούς ελέγχους ευπάθειας σύμφωνα με το [AS1] της Απόφασης Κ.Δ.Π 389/2020.

## Εγχειρίδια Εφαρμογών

Θα πρέπει να ετοιμάζονται εγχειρίδια χρήσης της εφαρμογής τα οποία να επικαιροποιούνται και να παραμένουν πάντοτε ενημερωμένα.

## Εκπαίδευση Χρηστών

Ο ιδιοκτήτης της εκάστοτε εφαρμογής θα πρέπει να εξασφαλίζει ότι, οι τελικοί χρήστες της εφαρμογής είναι επαρκώς εκπαιδευμένοι πριν την έναρξη χρήσης της Συντήρηση και αξιολόγηση.

Η εφαρμογή πρέπει να συντηρείται και να αξιολογείται σε τακτά χρονικά διαστήματα μέσω συμφωνιών επιπέδου υπηρεσιών (SLAs).

## Διαδικασία Διαχείρισης Αλλαγών

Για κάθε αλλαγή της εφαρμογής, εφαρμόζονται κατάλληλα μέτρα ασφαλείας όπως:

• υλοποίηση μέτρων ασφαλείας για αντιμετώπιση αναγνωρισμένων κινδύνων και απειλών.

• Χρήση αντιμέτρων όπως κρυπτογράφηση, ανίχνευση εισβολών, περιορισμός πρόσβασης, και άλλα.

Και ο έλεγχος του λογισμικού πραγματοποιείται μέσα από την διαδικασία διαχείρισης αλλαγών σύμφωνα με το [CM1] της Απόφασης Κ.Δ.Π 389/2020:

• Οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών

• Επιβεβαίωση ότι κάθε νέα έκδοση λογισμικού είναι συμβατή με τα μέτρα ασφαλείας που έχουν ληφθεί.

• Αξιολόγηση κινδύνων στο πλαίσιο αιτημάτων αλλαγών και σχεδιασμός αλλαγών λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας.

Ο [Όνομα Οργανισμού] πρέπει να εξετάσει το ενδεχόμενο εφαρμογής, τουλάχιστον, μιας αξιολόγησης κινδύνου στο αρχικό στάδιο του έργου, διενέργειας δοκιμών ασφάλειας και εξέτασης κώδικα στα στάδια ανάπτυξης του έργου, και διενέργεια αξιολόγησης ασφάλειας και ασφαλούς διαμόρφωσης στην παράδοση του έργου. Διασφαλίζει ότι τα δεδομένα που χρησιμοποιούνται για τη διενέργεια δοκιμών είναι ανώνυμα και δεν συνδέονται με εμπιστευτικές και ευαίσθητες πληροφορίες στο πλαίσιο αναπτυξιακών δραστηριοτήτων.

# Ανάθεση Ανάπτυξης σε Τρίτα Μέρη

Σε περίπτωση που ο [Όνομα Οργανισμού] αναθέσει την ανάπτυξη εφαρμογών σε τρίτα μέρη για λογαριασμό του οφείλει να αναφέρει τη σημασία του να υπάρχουν ακριβείς προδιαγραφές ασφαλείας, εγγυήσεις και διαβεβαιώσεις για τις εφαρμογές που αναπτύσσονται από τρίτα μέρη ή χρησιμοποιούνται από οργανισμούς. Συγκεκριμένα θα πρέπει να:

1. Οριστούν οι ακριβείς προδιαγραφές ασφαλείας που οι εφαρμογές πρέπει να πληρούν στο έγγραφο απαιτήσεων (request for proposal - RFP). Μεταξύ άλλων, δύναται να περιλαμβάνει πτυχές όπως η προστασία των δεδομένων, η αντιμετώπιση των απειλών ασφαλείας και η συμμόρφωση με τυχόν κανονιστικά πρότυπα.
2. Ζητούνται εκ των προτέρων εγγυήσεις και διαβεβαιώσεις από τον ανάδοχο ή τον προμηθευτή της εφαρμογής ότι οι προδιαγραφές ασφαλείας πληρούνται. Αυτές οι εγγυήσεις μπορεί να περιλαμβάνουν διαδικασίες δοκιμής της εφαρμογής, αναφορές ασφαλείας, και άλλες εγγυήσεις για την ορθή λειτουργία της.

# Αναθεώρηση

H Πολιτική για την Ασφάλεια Συστημάτων και Εφαρμογών θα πρέπει να επανεξετάζεται και να επικαιροποιείται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] ή άλλων αναγκών όπως όταν υπάρχουν σημαντικές αλλαγές στην υποδομή ή τις εφαρμογές (π.χ. εφαρμογή νέων συστημάτων ή παροπλισμός παλαιών εφαρμογών με την ολοκλήρωση του κύκλου ζωής τους.)

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Ασφάλεια Συστημάτων | SS1 | Καταπολέμηση κακόβουλου λογισμικού | Να διασφαλιστεί ότι δεν θα επηρεαστούν οργανωτικοί πόροι από κακόβουλο λογισμικό και κώδικα. |
| Ασφάλεια Συστημάτων | SS2 | Θωράκιση συστημάτων και συσκευών και βασικές απαιτήσεις ασφάλειας | Να ελαχιστοποιηθεί, στο μέτρο του δυνατού, η επιφάνεια επίθεσης των συστημάτων πληροφοριών, μέσω της μείωσης της λειτουργικότητας και των χαρακτηριστικών τους. |
| Ασφάλεια Συστημάτων | SS3 | Ασφάλεια κινητών συσκευών | Να εξασφαλιστεί η κατάλληλη ασφάλεια των κινητών συσκευών που έχουν πρόσβαση σε οργανωτικούς πόρους. |
| Ασφάλεια Συστημάτων | SS4 | Διαχείριση διαμόρφωσης εφαρμογών | Να διασφαλιστεί η κατάλληλη διαχείριση των εφαρμογών που χρησιμοποιούνται για την πρόσβαση ή επεξεργασία οργανωτικών πόρων. |
| Ασφάλεια Εφαρμογών | AS1 | Ασφαλής κύκλος ζωής ανάπτυξης λογισμικού | Να διασφαλιστούν επαρκή μέτρα ασφάλειας στο πλαίσιο των δραστηριοτήτων ανάπτυξης λογισμικού που αναπτύσσει ο οργανισμός |