Όνομα Οργανισμού

Πολιτική Ασφάλειας Συστημάτων

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Ασφάλειας Συστημάτων |
| **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. Σκοπός 4](#_Toc153449705)

[2. Ασφάλεια Λειτουργικών Συστημάτων 4](#_Toc153449706)

[3. Ασφάλεια Εφαρμογών 5](#_Toc153449707)

[3.1. Κύκλος Ζωής Εφαρμογής 6](#_Toc153449708)

[3.1.1 Σκοπός 6](#_Toc153449713)

[3.1.2 Απαιτήσεις 6](#_Toc153449714)

[3.1.3 Σχεδιασμός 6](#_Toc153449715)

[3.1.4 Μέτρα Εγκατάστασης Εφαρμογών 7](#_Toc153449716)

[3.1.5 Ανάπτυξη και Υλοποίηση 7](#_Toc153449717)

[3.1.6 Δοκιμή και Εγκατάσταση 7](#_Toc153449718)

[3.1.7 Εγχειρίδια Εφαρμογών 8](#_Toc153449719)

[3.1.8 Εκπαίδευση Χρηστών 8](#_Toc153449720)

[3.1.9 Συντήρηση και αξιολόγηση 8](#_Toc153449721)

[3.1.10 Διαδικασία Διαχείρισης Αλλαγών 8](#_Toc153449722)

[3.1.11 Στοιχεία Ενεργητικού 8](#_Toc153449723)

[3.1.12 Μέτρα Διαχείρισης Διαμόρφωσης Εφαρμογών 9](#_Toc153449724)

[3.1.13 Κύκλος Ανάπτυξης Λογισμικού 9](#_Toc153449725)

[3.2. Διαχωρισμός Περιβαλλόντων 10](#_Toc153449726)

[3.3. Ανάθεση Ανάπτυξης σε Τρίτα Μέρη 10](#_Toc153449727)

[3.4. Οδηγίες Ανάπτυξης Λογισμικού 11](#_Toc153449728)

[4. Κακόβουλα Λογισμικά 12](#_Toc153449729)

[4.1. Αντιμετώπιση Κακόβουλων Λογισμικών 12](#_Toc153449730)

[4.2. Βέλτιστες Πρακτικές Αντιμετώπισης Κακόβουλων Λογισμικών 13](#_Toc153449731)

[5. Φορητός Εξοπλισμός 15](#_Toc153449732)

[5.1. Μέτρα ασφαλείας 15](#_Toc153449733)

# Σκοπός

Τα Λειτουργικά Συστήματα και οι Εφαρμογές του [Όνομα Οργανισμού] πρέπει να προστατεύονται κατάλληλα, καθώς αποτελούν αναπόσπαστο στοιχείο για τη εύρυθμη λειτουργία του [Όνομα Οργανισμού].

Σκοπός της Πολιτικής Ασφάλειας Συστημάτων είναι να καθορίζει τις απαιτήσεις και τις τεχνικές για την ασφάλεια των λειτουργικών συστημάτων του [Όνομα Οργανισμού]. Επίσης, περιγράφει τις κατευθυντήριες γραμμές που πρέπει να αναπτυχθούν για την ασφάλεια των εφαρμογών.

# Ασφάλεια Λειτουργικών Συστημάτων

Για την ετοιμασία και διαμόρφωση των λειτουργικών συστημάτων θα πρέπει να καθοριστεί και να ακολουθείται διαδικασία ρύθμισης πρωτότυπων λειτουργικών συστημάτων. H διαδικασία μεταξύ άλλων πρέπει να 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.
* 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 εγκαθίστανται στον [Όνομα Οργανισμού] πρέπει να ακολουθούν την πιο πάνω διαδικασία.
* που βρίσκονται στο εσωτερικό δίκτυο του [Όνομα Οργανισμού], όπου είναι εφικτό, πρέπει να είναι μέλη του Microsoft Domain / Forest,.
	+ Σε αντίθεση τα συστήματα που τοποθετούνται στο DMZ δεν πρέπει να είναι μέλη του Domain / Forest
* πρέπει να είναι συγχρονισμένα σε κεντρικό σύστημα (ntp) για τον ομοιόμορφο καθορισμό της ώρας / ημερομηνίας
* πρέπει vα έχουν τις τελευταίες ενημερώσεις και αναβαθμίσεις
* πρέπει να έχουν μόνο τις εξουσιοδοτημένες, από τον [Όνομα Οργανισμού], εφαρμογές. Οι εν λόγω εφαρμογές πρέπει να είναι ενημερωμένες με τις τελευταίες ενημερώσεις ασφαλείας.
* πρέπει να έχουν απενεργοποιημένους τους προκαθορισμένους λογαριασμούς όπως «administrator», «root», «guest», «default».
* πρέπει να προστατεύονται με κωδικούς ασφάλειας. Οι κωδικοί θα πρέπει να συμμορφώνονται σύμφωνα με την Πολιτική Ελέγχου Πρόσβασης.
* πρέπει να έχουν δίσκους που να είναι κρυπτογραφημένοι σύμφωνα με την Πολιτική Διαχείρισης Στοιχείων Ενεργητικού
* Πρέπει να έχουν απενεργοποιημένες τις υπηρεσίας Bluetooth και WiFi όταν δεν χρειάζονται.
* δεν πρέπει να έχουν λογαριασμούς με αυξημένα δικαιώματα διαχειριστή
* πρέπει να έχουν απενεργοποιημένη την επιλογή εκκίνησης του λειτουργικού συστήματος από εναλλακτικές πήγες εκτός του πρωτεύοντος σκληρού δίσκου.
* πρέπει να έχουν ενεργοποιημένο το χαρακτηριστικό «secure boot»
* πρέπει να υποστηρίζονται και να έχουν ενεργοποιημένο το χαρακτηριστικό «Credential Guard»
* 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 εξουσιοδοτημένοι πρέπει να μπορεί να έχει απομακρυσμένη πρόσβαση.
* πρέπει να έχουν ενεργοποιημένες μόνο τις αναγκαίες υπηρεσίες
* πρέπει να έχουν ενεργοποιημένο το τοπικό Firewall. Μόνο οι αναγκαίες θύρες (ports) πρέπει να είναι ανοικτές.
* πρέπει να μην έχουν κοινούς φακέλους. Σε περίπτωση που υπάρχει ανάγκη για κοινόχρηστους φακέλους τα κατάλληλα δικαιώματα πρόσβασης πρέπει να καθορίζονται.
* πρέπει να έχουν απενεργοποιημένη την αυτόματη εκκίνηση δισκέττας, οπτικού δίσκου, αποσπώμενου μέσου αποθήκευσης.
* υψηλού κινδύνου ή/και φορητός εξοπλισμός πρέπει να υιοθετούν μηχανισμούς κρυπτογράφησης.
* πρέπει να εμφανίζουν μήνυμα, στον χρήστη, κατά τη διάρκεια της διαδικασίας σύνδεσης, το οποίο να υποδεικνύει ότι το συγκεκριμένο σύστημα/ συσκευή/ εφαρμογή ανήκει στον [Όνομα Οργανισμού] και ότι η μη εξουσιοδοτημένη πρόσβαση δεν επιτρέπεται. Ο χρήστης θα μπορεί να ολοκληρώσει την διαδικασία σύνδεσης αφού επιβεβαιώσει ότι κατανοεί το πιο πάνω μήνυμα.
* πρέπει τα μέτρα που θα επιλέγονται και θα εφαρμόζονται για την εγκατάσταση εφαρμογών σε servers να γίνεται με ad-hoc.
* πρέπει όλα τα κρίσιμα στοιχεία ενεργητικού να έχουν ενεργεί παρακολούθηση.
* Πρέπει 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

Οι απαιτήσεις και προδιαγραφές για την ασφάλεια και λειτουργικότητα των εφαρμογών πρέπει να προσδιοριστούν και να τεκμηριωθούν. Οι εφαρμογές που αγοράζονται ή αναπτύσσονται για τον [Όνομα Οργανισμού] πρέπει να πληρούν τις απαιτήσεις και τις προδιαγραφές αυτές.

# Κύκλος Ζωής Εφαρμογής

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) της εφαρμογής. Δικλείδες ασφαλείας όπως κρυπτογράφηση πρέπει να χρησιμοποιούνται. Για κάθε ανάπτυξη 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 . Για περισσότερες πληροφορίες σχετικά με την διαχείριση και προστασία των εφαρμογών ανατρέξτε στην Πολιτική Διαχείρισης Στοιχείων Ενεργητικού.

1.
2.
3. 1.

### 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.

### Απαιτήσεις

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 εφαρμογής πρέπει να συμπεριλαμβάνει την εκπλήρωση των απαιτήσεων της εφαρμογής και το πώς θα υλοποιηθεί. Κατά την διάρκεια του σχεδιασμού θα πρέπει να διενεργεί risk assessment ή threat profiling και σύμφωνα με τα αποτελέσματα θα ενσωματώνει τα κατάλληλα μέτρα ασφαλείας.

Το risk assessment και το threat profiling είναι σημαντικά στοιχεία της διαδικασίας ανάπτυξης λογισμικού. Συγκεκριμένα το risk assessment (αξιολόγηση κινδύνων) αφορά:

• Αναγνώριση και καταγραφή δυνητικών κινδύνων για το λογισμικό.

• Καθορισμός της πιθανότητας εκδήλωσης κάθε κινδύνου και του αντίκτυπου του στο σύστημα.

• Κατάταξη των κινδύνων με βάση τη σοβαρότητά τους.

Ενώ το threat profiling (καθορισμός απειλών) την:

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

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

### Μέτρα Εγκατάστασης Εφαρμογών

Πριν από την εγκατάσταση των εφαρμογών, γίνεται λεπτομερής ανάλυση των απαιτήσεών τους, λαμβάνοντας υπόψη τη λειτουργία τους, τις ανάγκες ασφαλείας και τους ενδεχόμενους κινδύνους [AS1].

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 [AS1].

### Ανάπτυξη και Υλοποίηση

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

### 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. Αυτό σημαίνει ότι αφαιρούνται ή αντικαθίστανται τα στοιχεία που μπορούν να οδηγήσουν στην αναγνώριση του ατόμου.
2. Περιορισμός Πρόσβασης: Ορισμένα άτομα ή ομάδες εργασίας μπορεί να χρειάζονται πρόσβαση σε ευαίσθητα δεδομένα για τις δοκιμές. Πρέπει να επιβάλλονται περιορισμοί πρόσβασης, και μόνο τα απαραίτητα άτομα θα πρέπει να έχουν πρόσβαση.
3. 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.
4. Εφαρμογή Απαγορευτικών Κανόνων: Οι κανόνες και οι πολιτικές που απαγορεύουν τη χρήση πραγματικών ευαίσθητων πληροφοριών για τις δοκιμές πρέπει να εφαρμόζονται αυστηρά.
5. 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 οργανισμός μπορεί να διασφαλίσει ότι οι δοκιμές γίνονται με ασφάλεια και χωρίς την παραβίαση της ανωνυμίας ή της ευαισθησίας των πληροφοριών.

### Εγχειρίδια Εφαρμογών

Εγχειρίδια χρήσης και ιστορικού της εφαρμογής πρέπει να συντάσσονται και να επικαιροποιούνται.

### Εκπαίδευση Χρηστών

Οι χρήστες της εφαρμογής πρέπει να εκπαιδεύονται από το Τμήμα Ανθρώπινου Δυναμικού σε συνεργασία με τον ιδιοκτήτη της εφαρμογής.

### Συντήρηση και αξιολόγηση

Η εφαρμογή πρέπει να συντηρείται και να αξιολογείται σε τακτά χρονικά διαστήματα.

### Διαδικασία Διαχείρισης Αλλαγών

Εφαρμόζονται κατάλληλα μέτρα ασφαλείας όπως:

• Εφαρμογή μέτρων ασφαλείας που αντιμετωπίζουν τους αναγνωρισμένους κινδύνους και απειλές.

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

Και ο έλεγχος του λογισμικού πραγματοποιείται μέσα από την διαδικασία διαχείρισης αλλαγών [CM1]:

• 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.

### Στοιχεία Ενεργητικού

Ο [Όνομα Οργανισμού] θα πρέπει να εξασφαλίσει επαρκή μέτρα στο πλαίσιο της εξωτερικής πρόσβασης σε οργανωτικούς πόρους. Να διασφαλίζει τη δυνατότητα απομακρυσμένης πρόσβασης στο δίκτυο με τη χρήση εικονικών ιδιωτικών δικτύων (VPN) και την πρόσβαση σε εξ αποστάσεως εφαρμογές μέσω της χρήσης εξωτερικών εφαρμογών διεπαφών. Οφείλει να εφαρμόσει επαρκή μέτρα διαχείρισης ταυτότητας και πρόσβασης και τον ειδικό έλεγχο πρόσβασης βάσει ρόλου [ΑΜ2].

Χρειάζεται να καταρτισθεί κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού και να γίνει καταγραφή των εξαρτήσεων και αλληλεξαρτήσεων μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο θα πραγματοποιηθεί η εκτίμηση κινδύνου [RM2].

### Μέτρα Διαχείρισης Διαμόρφωσης Εφαρμογών

Ο [Όνομα Οργανισμού] έχει θεσπίσει μέτρα διαχείρισης της διαμόρφωσης εφαρμογών προκειμένου να προληφθεί η μη επιτρεπόμενη και κακόβουλη εγκατάσταση, διαμόρφωση ή τροποποίηση εφαρμογών και λογισμικού σε οργανωτικά στοιχεία και συσκευές. Αυτό το μέτρο είναι σημαντικό για τη διασφάλιση της ασφάλειας του οργανισμού και την προστασία από ανεπιθύμητη εισβολή και τροποποίηση των εφαρμογών και του λογισμικού.

Τέτοια μέτρα περιλαμβάνουν τη χρήση υπογεγραμμένων εφαρμογών, περιοδικούς ελέγχους κατά την εγκατάσταση και τη χρήση λογισμικού, καθώς και την παρακολούθηση ενημερώσεων ασφαλείας. Επιπλέον, υιοθετείται πολιτική αρχειοθέτησης για την αποθήκευση παλαιότερων εκδόσεων εφαρμογών, προκειμένου να διευκολυνθεί η επαναφορά σε προηγούμενες καταστάσεις σε περίπτωση ανωμαλίας.

### Κύκλος Ανάπτυξης Λογισμικού

Για κάθε στοιχείο λογισμικού θα πρέπει να προσδιοριστούν οι ρόλοι για τους οποίους απαιτείται πρόσβαση καθώς και το επίπεδο πρόσβασης, επαληθεύοντας την αυθεντικότητα και εξουσιοδότηση χρηστών, με βάση το ελάχιστο προνόμιο και τους οργανωτικούς ρόλους και αρμοδιότητες. Η θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης ταυτότητας και πρόσβασης σκοπέυουν να παρέχουν τεχνικά και οργανωτικά μέσα για την επιβολή της αρχής του ελάχιστου προνομίου και να διαχειρίζονται αντίστοιχα τους προνομιούχους χρήστες. Ο έλεγχος πρόσβασης βάσει ρόλου διασφαλίζει ότι χορηγούνται επαρκείς άδειες σε χρήστες με βάση τις αρμοδιότητες τους που συνδέονται με αντίστοιχους ρόλους [ΙΑΜ1].

Σύμφωνα με τον Κανονισμό 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. Το 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 το SDLC είναι σχεδιασμένο για να εξασφαλίζει την ποιότητα, την ασφάλεια, και τη συντηρησιμότητα του λογισμικού κατά τη διάρκεια όλου του κύκλου ζωής του.

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.

# Διαχωρισμός Περιβαλλόντων

Ο διαχωρισμός των περιβαλλόντων ανάπτυξης λογισμικού από το επιχειρησιακό 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 λογισμικού συνήθως γίνεται σε ένα περιβάλλον ανάπτυξης, ενώ η παραγωγή λειτουργεί σε ένα διαφορετικό περιβάλλον. Αυτός ο διαχωρισμός εξασφαλίζει ότι τυχόν σφάλματα ή προβλήματα που μπορεί να προκύψουν κατά την ανάπτυξη δεν επηρεάζουν τον παραγωγικό κώδικα.
2. Χρήση Αντιγράφων Βάσεων Δεδομένων: Συχνά, κατά τη διάρκεια της ανάπτυξης, χρησιμοποιούνται αντίγραφα των βάσεων δεδομένων. Είναι σημαντικό να ελέγχεται προσεκτικά η χρήση αυτών των δεδομένων και να μην επηρεάζεται η παραγωγική βάση δεδομένων.
3. Έλεγχος Πρόσβασης: Η πρόσβαση στο περιβάλλον παραγωγής πρέπει να περιορίζεται μόνο σε αυτούς που την χρειάζονται. Ορισμένοι εργαζόμενοι μπορεί να έχουν πρόσβαση στο περιβάλλον ανάπτυξης, αλλά αυτό δεν σημαίνει ότι πρέπει να έχουν πρόσβαση και στο περιβάλλον παραγωγής.
4. Καθαρισμός Δεδομένων: Κατά τη μετάβαση από το περιβάλλον ανάπτυξης στο περιβάλλον παραγωγής, πρέπει να διασφαλιστεί ότι τα δεδομένα είναι καθαρά και δεν υπάρχουν δεδομένα που δεν πρέπει να υπάρχουν στο περιβάλλον παραγωγής.
5. Κανόνες Εφαρμογής: Θα πρέπει να υπάρχουν σαφείς κανόνες και διαδικασίες για το πώς γίνεται η μετάβαση από το περιβάλλον ανάπτυξης 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.

# 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. Αυτό μπορεί να περιλαμβάνει πτυχές όπως η προστασία των δεδομένων, η αντιμετώπιση των απειλών ασφαλείας και η συμμόρφωση με τυχόν κανονιστικά πρότυπα.
2. Ζητούνται εγγυήσεις από τον ανάδοχο ή τον προμηθευτή του λογισμικού ότι οι προδιαγραφές ασφαλείας πληρούνται. Αυτές οι εγγυήσεις μπορεί να περιλαμβάνουν διαδικασίες δοκιμής, αναφορές ασφαλείας, και άλλες εγγυήσεις για την ορθή λειτουργία του λογισμικού.
3. Διασφαλίζεται ότι όλες οι απαιτούμενες εγγυήσεις και διαβεβαιώσεις καλύπτονται πριν από την αποδοχή ή την εκτέλεση των εφαρμογών. Αυτό περιλαμβάνει επαρκείς διαδικασίες ελέγχου και επαλήθευσης.

# Οδηγίες Ανάπτυξης Λογισμικού

Ο [Όνομα Οργανισμού] θα πρέπει να δημιουργήσει μια σειρά από οδηγίες (υποχρεωτικής εφαρμογής) για την ασφαλή ανάπτυξη λογισμικού. Για τη δημιουργία ασφαλών οδηγιών ανάπτυξης λογισμικού, ο οργανισμός μπορεί να ακολουθήσει τα παρακάτω βήματα:

Καθορισμός Στόχων και Πολιτικών:

• Καθορισμός των αναμενόμενων επιδόσεων και των στόχων ασφαλείας.

• Διατύπωση πολιτικών ασφαλείας που θα καθοδηγούν την ανάπτυξη.

Έρευνα Καλών Πρακτικών:

• Ερευνα βέλτιστων πρακτικών στον κλάδο και συγκριτική ανάλυση.

Καθορισμός Απαιτήσεων Ασφαλείας:

• Καθορισμός απαιτήσεων ασφαλείας για κάθε στάδιο της διαδικασίας ανάπτυξης.

Δημιουργία Οδηγιών Ανάπτυξης:

• Διαμόρφωση οδηγιών που καλύπτουν συγκεκριμένα θέματα όπως η εισαγωγή δεδομένων, ο χειρισμός σφαλμάτων, και η αντιμετώπιση ευπάθειών.

Συμμόρφωση με Διεθνείς Προτύπους:

• Ενσωμάτωση προτύπων ασφαλείας όπως ISO 27001 στις οδηγίες.

Εκπαίδευση Προσωπικού:

• Παροχή εκπαίδευσης στους προγραμματιστές για τη σωστή υλοποίηση των οδηγιών.

Ενσωμάτωση στη Διαδικασία Ανάπτυξης Λογισμικού:

• Ενσωμάτωση των οδηγιών στη διαδικασία ανάπτυξης λογισμικού, ώστε να είναι μέρος της καθημερινής εργασίας.

Αξιολόγηση και Ενημέρωση:

• Αξιολόγηση των οδηγιών σε τακτική βάση και ενημέρωσή τους σύμφωνα με νέες απαιτήσεις και απειλές.

Παρακολούθηση Συμμόρφωσης:

• Παρακολούθηση της συμμόρφωσης με τις οδηγίες και λήψη μέτρων για την αντιμετώπιση τυχόν παραβιάσεων.

Ενίσχυση Πολιτικής:

• Ενίσχυση της πολιτικής σε περίπτωση νέων επιθέσεων ή ευπαθειών.

# Κακόβουλα Λογισμικά

# Αντιμετώπιση Κακόβουλων Λογισμικών

* Ο [Όνομα Οργανισμού] πρέπει να προστατεύεται από συστήματα περιμετρικής ασφάλειας. (*βλέπε Πολιτική Ασφάλειας* *Δικτύου).*
* Ο [Όνομα Οργανισμού] πρέπει να έχει εγκαταστήσει και να χρησιμοποιεί λογισμικό για την προστασία από κακόβουλο λογισμικό/κώδικα σε όλες της συσκευές τελικού σημείου.
* Ο [Όνομα Οργανισμού] πρέπει να τηρεί μέτρα διαχείρισης της διαμόρφωσης εφαρμογών με σκοπό την πρόληψη της μη επιτρεπόμενης και κακόβουλης εγκατάστασης, της διαμόρφωσης ή της τροποποίησης εφαρμογών και του λογισμικού σε οργανωτικά στοιχεία και συσκευές.
* Ο [Όνομα Οργανισμού] πρέπει να προωθεί τους εργαζομένους του να εκπαιδεύονται σε θέματα κυβερνοασφάλειας και συγκεκριμένα σε κοινωνικές επιθέσεις και κακόβουλα λογισμικά. Για περισσότερες πληροφορίες σχετικά με την εκπαίδευση εργαζομένων, ανατρέξτε στο Πλάνο Εκπαιδεύσεων Ευαισθητοποίησης.
* Τα λειτουργικά συστήματα και τα λογισμικά του [Όνομα Οργανισμού] πρέπει να έχουν εγκατεστημένες τις τελευταίες ενημερωμένες εκδόσεις
* Ο [Όνομα Οργανισμού] πρέπει να υποστηρίζεται από κεντρικό σύστημα αντιμετώπισης και παρακολούθησης κακόβουλων λογισμικών.
	+ Επίσης πρέπει να παρακολουθούνται και να εντοπίζονται οι περιπτώσεις όπου το λογισμικό αντιμετώπισης κακόβουλων λογισμικών στα Λειτουργικά Συστήματα δεν είναι εγκατεστημένο ή δεν είναι ενημερωμένο ή δεν έχει επικοινωνία με τον κεντρικό σύστημα αντιμετώπισης και παρακολούθησης κακόβουλων λογισμικών
* Πρόσβαση στο κεντρικό σύστημα αντιμετώπισης κακόβουλων λογισμικών πρέπει να έχει μόνο εξουσιοδοτημένο προσωπικό.
* Οποιεσδήποτε ρυθμίσεις αντιμετώπισης κακόβουλων λογισμικών πρέπει να γίνονται στο κεντρικό σύστημα αντιμετώπισης κακόβουλων λογισμικών με μορφή κανόνων και πολιτικών.
* Το κεντρικό σύστημα αντιμετώπισης κακόβουλων λογισμικών πρέπει να ενημερώνεται **τουλάχιστο 2 (δυο) φορές** την μέρα με την πιο πρόσφατη έκδοση ορισμών ιών (virus definitions).
* Όλα τα πληροφοριακά συστήματα πρέπει να έχουν εγκατεστημένο, και ενημερωμένο λογισμικό αντιμετώπισης κακόβουλων λογισμικών. Αυτό πρέπει να είναι συνδεδεμένο με το κεντρικό σύστημα αντιμετώπισης κακόβουλων λογισμικών και να ενημερώνεται **2 (δυο) φορές τη ημέρα**.
* Το εν λόγω λογισμικό αντιμετώπισης κακόβουλων λογισμικών όπου είναι εφικτό πρέπει να είναι προ εγκατεστημένο στο προκαθορισμένο λειτουργικό σύστημα.
* Η εγκατάσταση του λογισμικού αντιμετώπισης κακόβουλων λογισμικών πρέπει να γίνεται μόνο από εξουσιοδοτημένο προσωπικό.
* Απαγορεύεται η εγκατάσταση ανεπίσημου ή/και μη εξουσιοδοτημένου λογισμικού αντιμετώπισης κακόβουλων λογισμικών.
* Η απενεργοποίηση του λογισμικού αντιμετώπισης κακόβουλων λογισμικών δεν πρέπει να είναι δυνατή από τους χρήστες ή και τους διαχειριστές.
* Στις περιπτώσεις ανίχνευσης κακόβουλου λογισμικού σε πληροφοριακό σύστημα, το σύστημα αυτό πρέπει να αποσυνδέεται από το δίκτυο μέχρι το κακόβουλο λογισμικό να διαγραφεί.
* Πλήρης έλεγχος (full scan) κακόβουλων λογισμικών πρέπει να γίνεται **εβδομαδιαία** σε ώρες μη αιχμής.
* Το λογισμικό αντιμετώπισης κακόβουλων λογισμικών πρέπει να παρέχει προστασία σε πραγματικό χρόνο. Με την ανίχνευση κακόβουλου λογισμικού, το κακόβουλο λογισμικό πρέπει να «τίθεται σε καραντίνα» ή/και να διαγράφεται αυτόματα.
* Το λογισμικό αντιμετώπισης κακόβουλων λογισμικών πρέπει να ελέγχει όλα τα εισερχόμενα και εξερχόμενα αρχεία των ηλεκτρονικών μηνυμάτων.
* Το λογισμικό αντιμετώπισης κακόβουλων λογισμικών πρέπει να ελέγχει οποιαδήποτε αρχεία που προέρχονται από εξωτερικές πηγές.
* Απαγορεύεται η δημιουργία ή/και διανομή κακόβουλων λογισμικών στα πληροφοριακά συστήματα του [Όνομα Οργανισμού].
* Εξοπλισμός που δεν ανήκει στον [Όνομα Οργανισμού] δεν πρέπει να χρησιμοποιείται (π.χ. προσωπικοί φορητοί υπολογιστές)
* Συνδέσεις επικοινωνίας μέσω ιδεατών ιδιωτικών δικτύων (VPN) πρέπει να παρεμποδίζονται
* Φορητοί υπολογιστές (τρίτων, επισκεπτών), όπου ο έλεγχος για κακόβουλα λογισμικά δεν είναι εφικτός, δεν πρέπει να συνδέονται στο δίκτυο του [Όνομα Οργανισμού]. Μπορούν να συνδέονται σε ένα ιδεατό τοπικό δίκτυο (“guest” VLAN) (βλέπε *Πολιτική Ασφάλειας Δικτύου*).
* Τα πληροφοριακά συστήματα πρέπει να προστατεύονται εφαρμόζοντας τις βέλτιστες πρακτικές αντιμετώπισης κακόβουλων λογισμικών.

# Βέλτιστες Πρακτικές Αντιμετώπισης Κακόβουλων Λογισμικών

* Ο [Όνομα Οργανισμού] υλοποιεί προστασία τόσο σε επίπεδο συσκευής όσο και σε επίπεδο δικτύου και σε επίπεδο συστημάτων(firewall, proxy κλπ) όπου θα διενεργείται από ειδικό εξουσιοδοτημένο προσωπικό.
* Ο [Όνομα Οργανισμού] υλοποιεί εκπαίδευση σε θέματα που σχετίζονται με την προστασία από τεχνικές επίθεσης, phishing&social engineering, malware.
* Εγκαταστήστε λογισμικό για την προστασία από κακόβουλο λογισμικό/κώδικα σε όλες της συσκευές τελικού σημείου..
	+ Το λογισμικό θα διενεργεί αυτόματη σάρωση σε οποιοδήποτε εισερχόμενο.
	+ Το λογισμικό θα διενεργεί σάρωση και θα μπλοκάρει συνημμένα ηλεκτρονικών επικοινωνιών που περιέχουν κακόβουλο κώδικα ή τύπους αρχείων που ενέχουν αυξημένο κίνδυνο.
	+ Το λογισμικό θα διενεργεί τακτικούς ελέγχους στα σημεία αποθήκευσης πληροφοριών για την αναγνώριση αρχείων ή άλλων στοιχείων που σχετίζονται με κακόβουλο κώδικα.
	+ Το λογισμικό δεν θα επιτρέπει την αυτόματη έναρξη λογισμικών από διάφορα μέσα.
	+ Το λογισμικό θα ειδοποιεί τον χρήστη σε περίπτωση αναγνώρισης κάποιας απειλής.
	+ Το λογισμικό αυτόματα θα διενεργεί ενέργειες για την διαγραφή ή απομόνωση της απειλής.
	+ Το λογισμικό αυτόματα θα διενεργεί ενημερώσεις τόσο των υπογραφών όσο και της λειτουργικότητας.
	+ Διατηρείτε πάντα το λογισμικό αντιμετώπισης κακόβουλων λογισμικών ενημερωμένο και μην το απενεργοποιείτε.
	+ Βεβαιωθείτε ότι είναι πάντα σε λειτουργία.
* Αποφύγετε την χρήση μη πιστοποιημένων, άγνωστων ή ύποπτων ιστοσελίδων (όπου είναι εφικτό θα πρέπει να παρεμποδίζονται από το κεντρικό σύστημα).
* Αποφύγετε την εγκατάσταση και την χρήση μη πιστοποιημένων, άγνωστων ή ύποπτων λογισμικών (όπου είναι εφικτό θα πρέπει να παρεμποδίζονται από το κεντρικό σύστημα ).
* Όπου είναι επιτρεπτή η χρήση οπτικών δίσκων ή αποσπώμενων μέσων αποθήκευσης, αυτά πρέπει να ελέγχονται από το λογισμικό κακόβουλων λογισμικών πριν χρησιμοποιηθούν.
* Προσέξετε οποιαδήποτε συνημμένα αρχεία σας έχουν αποσταλεί μέσω ηλεκτρονικού ταχυδρομείου, ειδικά εάν δεν γνωρίζετε τον αποστολέα. Να είστε καχύποπτοι και να αποφύγετε:
	+ Το άνοιγμα αρχείων από άγνωστους αποστολείς.
	+ Το άνοιγμα αρχείων, των οποίων η λήψη δεν αναμένεται, από γνωστούς αποστολείς.
	+ Το άνοιγμα αρχείων, των οποίων η επέκταση τους μπορεί να προσδιορίζει αρχείο το οποίο περιέχει κακόβουλο κώδικα. Οι πιο διαδεδομένες επεκτάσεις είναι (EXE, COM, PIF, SCR, VBS, SHS, CHM BAT)
	+ Το άνοιγμα αρχείων, των οποίων έχουν περισσότερα από μια επέκταση (filetype) από έναν τύπο π.χ. (document.doc.vbs, picture.jpg.bat).
* Εφεδρικά αντίγραφα συνιστάται να τηρούνται σε τακτά χρονικά διαστήματα, ανάλογα με την κρισιμότητα της πληροφορίας.

# Φορητός Εξοπλισμός

Ο φορητός εξοπλισμός διατρέχει μεγάλο κίνδυνο καθώς μπορεί να μετακινείται εκτός των εγκαταστάσεων του [Όνομα Οργανισμού] και ως εκ τούτου να απολεσθεί ή/και να καταστραφεί ή/και να κλαπεί. Καθώς ο κίνδυνος είναι μεγάλος, τόσο ο εξοπλισμός όσο και το περιεχόμενο του, πρέπει να προστατευτούν σε οποιαδήποτε περίπτωση χρειαστεί αλλαγή κάποια συσκευή μόνο εξουσιοδοτημένα άτομα μπορούν να υλοποιήσουν την αλλαγή. Οι πληροφορίες που είναι αποθηκευμένες σε αυτό πρέπει να μείνουν ακέραιες, εμπιστευτικές και διαθέσιμες για τους εξουσιοδοτημένους χρήστες.

# Μέτρα ασφαλείας

* 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 φορητός εξοπλισμός που παραδίδεται σε εξουσιοδοτημένο χρήστη θα πρέπει να επιστραφεί σε περίπτωση τερματισμού απασχόλησης ή δεν είναι πλέον απαραίτητος για την άσκηση των καθηκόντων απασχόλησης.
* 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.
* 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 [Όνομα Οργανισμού] διατηρεί το δικαίωμα κατάσχεσης του φορητού εξοπλισμού, σε περίπτωση εξουσιοδοτημένης έρευνας, σε περίπτωση κακόβουλης ενέργειας (κατάχρηση δικαιωμάτων, διαρροής πληροφοριών κλπ.).
* Όλος ο φορητός εξοπλισμός θα πρέπει να είναι μέλος του Domain
* Ο φορητός εξοπλισμός πρέπει να προστατεύεται από κωδικό ασφαλείας (βλέπε Πολιτική Ελέγχου Πρόσβασης)
* Ο φορητός εξοπλισμός πρέπει να κλειδώνεται αυτόματα όταν δεν χρησιμοποιείται **πέραν των 15 λεπτών**.
* Ο φορητός εξοπλισμός πρέπει να προστατεύεται από λογισμικό αντιμετώπισης κακόβουλων λογισμικών (βλέπε Πολιτική Διαχείρισης Στοιχείων Ενεργητικού).
* 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.
* Ο φορητός εξοπλισμός πρέπει πάντα να είναι κρυπτογραφημένος (βλέπε Πολιτική Διαχείρισης Στοιχείων Ενεργητικού).
* Η αποθήκευση ευαίσθητων πληροφοριών πρέπει να αποφεύγεται στις φορητές συσκευές. Σε τέτοια περίπτωση η πληροφορία ή/και ο σκληρός δίσκος πρέπει να κρυπτογραφείται
* Ο χρήστης του φορητού εξοπλισμού είναι υπεύθυνος για την ακεραιότητα και τη διαθεσιμότητα της πληροφορίας.
* Περιττές αποθηκευμένες πληροφορίες στο φορητό εξοπλισμό, πρέπει να διαγράφονται.
* Ο φορητός εξοπλισμός δεν πρέπει να μένει ποτέ αφύλακτος, ιδιαίτερα εάν ο φορητός εξοπλισμός περιέχει ευαίσθητα δεδομένα ή πληροφορίες (βλέπε Πολιτική Αποδεκτής Χρήσης).
* Ο φορητός εξοπλισμός πρέπει να κλειδώνεται (π.χ. με κλειδαριές lockdown cable) ή να τοποθετείται σε ασφαλισμένα ντουλάπια.
* Σε περίπτωση κλοπής ή απώλειας του φορητού εξοπλισμού πρέπει να ενημερώνεται ο άμεσα προϊστάμενος του χρήστη, και ο/η Λειτουργός Ασφάλειας Πληροφοριών.
* Ο [Όνομα Οργανισμού] πρέπει να είναι σε θέση να διαγράφει τα δεδομένα που είναι αποθηκευμένα στο φορητό εξοπλισμό απομακρυσμένα (remote wiping).