RAAEY
REGULATORY AUTHORITY FOR ENERGY, WASTE & WATER

# Πολιτική Ασφάλειας Πληροφοριών

ΠΟ-00, 01.06.2026

## Στοιχεία Εγγράφου

| | |
|---|---|
| **Τίτλος Εγγράφου** | Πολιτική Ασφάλειας Πληροφοριών |
| **Υπεύθυνη Λειτουργία** | Λειτουργία Ασφάλειας Πληροφοριών |
| **Είδος Εγγράφου** | Πολιτική Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών |
| **Κατηγορία** | Δημόσια Χρήση |
| **Κωδικός/ Έκδοση** | ΠΟ-00 |
| **Ημερομηνία έκδοσης** | 01/06/2026 |

## Πίνακας Ιστορικότητας Μεταβολών Εγγράφου

| Έκδοση | Ημερομηνία | Περιγραφή μεταβολών |
|---|---|---|
| 1.0 | 10/06/2023 | Πρώτη έκδοση |
| 2.0 | 05/05/2025 | Αναθεώρηση σύμφωνα με ISO/IEC 27001:2022 |
| 3.0 | 01/06/2026 | Ετήσια αναθεώρηση |

## Περιεχόμενα


Στοιχεία Εγγράφου ..... 2

Πίνακας Ιστορικότητας Μεταβολών Εγγράφου ..... 2

Περιεχόμενα ..... 3

1. Εισαγωγή ..... 5

1.1 Γενικές Πληροφορίες ..... 5

1.2 Θεσμικό και Εποπτικό Πλαίσιο ..... 6

1.3 Πεδίο Εφαρμογής ..... 6

1.4 Σκοπός και Δήλωση Στόχων ..... 6

1.5 Αρμοδιότητες και έλεγχος ..... 7

1.6 Επισκόπηση, Αναθεώρηση και Τήρηση Αρχείου ..... 8

1.7 Πρόγραμμα μη συμμόρφωσης ..... 8

2. Ορισμοί ..... 8

3. Οργάνωση Ασφάλειας Πληροφοριών ..... 9

3.1 Εσωτερική οργάνωση ..... 9

4. Γενικές Αρχές της Πολιτικής ..... 9

4.1 Ελαχιστοποίηση Κινδύνων ..... 9

4.2 Πρόσβαση όπου απαιτείται ..... 9

4.3 Ακεραιότητα, Εμπιστευτικότητα και Διαθεσιμότητα ..... 10

4.4 Προβλεπόμενη χρήση αγαθών ..... 10

4.5 Περιστατικά Ασφαλείας ..... 10

4.6 Περιστατικά Διαχείρισης Λειτουργικού Κινδύνου ..... 10

4.7 Ενημέρωση Ασφάλειας Πληροφοριών ..... 10

4.8 Μεταβολές ρόλων και Αρμοδιοτήτων ..... 10

4.9 Πρακτικές Ασφαλείας ..... 11

4.10 Ιδιοκτήτες Πληροφοριών ..... 11

5. Ασφάλεια Ανθρώπινου Δυναμικού ..... 11

5.1 Πριν από την Απασχόληση ..... 11

5.2 Κατά τη Διάρκεια της Απασχόλησης ..... 12

5.3 Λήξη ή Μεταβολή Απασχόλησης ..... 12

6. Διαχείριση Αγαθών ..... 13

7. Διαβάθμιση Πληροφοριών ..... 13

8. Έλεγχος Πρόσβασης ..... 13

8.1 Επιχειρησιακή Απαίτηση για τον Έλεγχο της Πρόσβασης ..... 13
8.2 Ευθύνες Χρηστών ..... 14
8.3 Έλεγχος Πρόσβασης σε Λειτουργικά Συστήματα και Εφαρμογές ..... 14
8.4 Φορητά Μέσα Ηλεκτρονικών Υπολογιστών ..... 14
8.5 Φορητές Ιδιωτικές Συσκευές (BYOD) ..... 14
9. Τηλεργασία ..... 15
9.1 Εξοπλισμός ..... 15
9.2 Επικοινωνίες ..... 16
9.3 Λήψη αντιγράφων ασφαλείας στην Τηλεργασία ..... 16
9.4 Καταγγελία σύμβασης ..... 16
10. Πολιτική Κρυπτογραφίας ..... 17
11. Φυσική και Περιβαλλοντική Ασφάλεια ..... 17
11.1 Ασφαλείς Περιοχές ..... 18
11.2 Ασφάλεια Εξοπλισμού ..... 18
12. Ασφάλεια Επιχειρησιακών Λειτουργιών ..... 18
12.1 Λειτουργικές Διαδικασίες ..... 18
13. Ασφάλεια Δικτύων και Επικοινωνιών ..... 19
14. Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων ..... 19
15. Διαχείριση Περιστατικών Ασφάλειας ..... 20
16. Διαχείριση Επιχειρησιακής Συνέχειας ..... 20
17. Λίστα Πολιτικών, Διαδικασιών & Φορμών ..... 20
17.1 Πολιτικές ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
17.2 Διαδικασίες ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
17.3 Φόρμες ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

# 1. Εισαγωγή

## 1.1 Γενικές Πληροφορίες

Η Διοίκηση της ΡΑΑΕΥ αποδεικνύει, μέσω της εφαρμογής των διεργασιών επιχειρησιακής λειτουργίας, ότι οι ανάγκες και οι προσδοκίες της αγοράς που εποπτεύει, καθώς και των καταναλωτών που καλείται να προστατέψει, γίνονται αντιληπτές και μετατρέπονται σε απαιτήσεις που είναι δυνατό να ικανοποιηθούν, τηρουμένων των κατά περίπτωση εφαρμοζόμενων συμβατικών απαιτήσεων.

Η Διοίκηση της ΡΑΑΕΥ αποδεικνύει τη δέσμευσή της όσον αφορά την ικανοποίηση των απαιτήσεων ως Αρχή μέσω:

- της δημιουργίας ενός περιβάλλοντος ευαισθητοποίησης,
- του καθορισμού της πολιτικής για την ασφάλεια πληροφοριών και των αντικειμενικών σκοπών και στόχων ασφάλειας πληροφοριών,
- της διαθεσιμότητας των απαραιτήτων πόρων,
- της κάλυψης των νομικών και κανονιστικών απαιτήσεων,
- της συμμόρφωσης με λοιπούς ισχύοντες κανονισμούς εργασίας.

Η Πολιτική Ασφάλειας Πληροφοριών («Γενική Πολιτική Ασφάλειας» / «Πολιτική») αποτελεί δέσμευση της Διοίκησης της ΡΑΑΕΥ και αποτυπώνεται στην απόφαση Ολομέλειας υπ. αριθμ. 273-2022/17.03.2022 της ΡΑΑΕΥ, με την οποία αποφασίζει:

- Την εφαρμογή προτύπου ασφάλειας ISO 27001:2022 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών» για όλο το φάσμα των δραστηριοτήτων της.
- Δεσμεύεται για την αποτελεσματική διαχείριση ασφάλειας μέσω της επιβολής των πολιτικών ασφάλειας καθώς και την παροχή των κατάλληλων πόρων για την ανάπτυξη, εφαρμογή και συνεχή βελτίωση του ΣΔΑΠ της ΡΑΑΕΥ.
- Διασφαλίζει ότι η συστηματική αναθεώρηση των επιδόσεων του ΣΔΑΠ πραγματοποιείται σε τακτική βάση, ώστε να εξασφαλιστεί ότι οι στόχοι της ασφάλειας των πληροφοριών πληρούνται και οι αδυναμίες και τα προβλήματα ασφάλειας εντοπίζονται από την εσωτερική επιθεώρηση και τις διαδικασίες διαχείρισης ασφάλειας του ΣΔΑΠ. Η ανασκόπηση του ΣΔΑΠ από τη Διοίκηση πραγματοποιείται με διάφορους τρόπους, συμπεριλαμβανομένων τμηματικών και άλλων διοικητικών συνεδριάσεων
- Καθορίζει τους στόχους για την ασφάλεια των πληροφοριών σε ετήσια βάση, σε συνδυασμό με το σχεδιασμό του προϋπολογισμού. Οι στόχοι αυτοί πρέπει να βασίζονται σε μια σαφή κατανόηση των απαιτήσεων της ΡΑΑΕΥ και να ενημερώνονται από την ετήσια Ανασκόπηση Διοίκησης.
- Διασφαλίζει την επανεξέταση σε τακτά χρονικά διαστήματα των πολιτικών, διαδικασιών και των τεχνικών μέτρων προστασίας και ανάλογα με τα αποτελέσματα της Αποτίμησης Επικινδυνότητας και του Σχεδίου Αντιμετώπισης Επικινδυνότητας

## 1.2 Θεσμικό και Εποπτικό Πλαίσιο

Η Πολιτική συμμορφώνεται κατά κύριο λόγο, με την ακόλουθη νομοθεσία:

- Γενικός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 (GDPR), ο ν. 4624/2019, ο ν. 3471/2006 και κάθε άλλη ρύθμιση που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Ο ν. 4727/2020 για την ψηφιακή διακυβέρνηση και τις ηλεκτρονικές επικοινωνίες, καθώς και το κανονιστικό πλαίσιο που διέπει τη λειτουργία της ΡΑΑΕΥ.
- Η νομοθεσία για την ασφάλεια συστημάτων δικτύου και πληροφοριών (ν. 4577/2018, ως εκάστοτε ισχύει, και το πλαίσιο NIS2), όπου εφαρμόζεται στη ΡΑΑΕΥ.
- Το πρότυπο ISO/IEC 27001:2022, του οποίου το Παράρτημα Α (Annex A) περιλαμβάνει 93 ελέγχους ασφάλειας οργανωμένους σε τέσσερις θεματικές ενότητες (Οργανωτικοί, Ανθρώπινου Δυναμικού, Φυσικοί και Τεχνολογικοί έλεγχοι).

Για την αποτελεσματική διαχείριση της έκθεσης σε κίνδυνο και της επικινδυνότητας, η παρούσα Πολιτική καλύπτει τις θεματικές ενότητες ασφάλειας πληροφοριών, όπως αυτές αποτυπώνονται στους ελέγχους του Παραρτήματος Α του ISO/IEC 27001:2022 και αναλύονται στις κατευθυντήριες οδηγίες εφαρμογής του ISO/IEC 27002:2022.

## 1.3 Πεδίο Εφαρμογής

Η Πολιτική υιοθετείται και εφαρμόζεται από:

- Τα πρόσωπα που διοικούν την ΡΑΑΕΥ.
- Το σύνολο του προσωπικού της ΡΑΑΕΥ, καθώς και όλους τους δημόσιους και ιδιωτικούς φορείς, εταιρείες και οργανισμούς με τους συνεργάζεται ή συναλλάσσεται η ΡΑΑΕΥ.
- Τα υπόχρεα πρόσωπα δεσμεύονται άμεσα από την Πολιτική που καθιδρύει συγκεκριμένες υποχρεώσεις τους και οφείλουν να τηρούν με κάθε επιμέλεια τα ειδικότερα καθήκοντά τους στο πλαίσιο της οργανικής τους θέσης ή των όρων συνεργασίας τους με την ΡΑΑΕΥ όσον αφορά τους εξωτερικούς συνεργάτες.

## 1.4 Σκοπός και Δήλωση Στόχων

Σκοπός της παρούσας Πολιτικής είναι η διασφάλιση της **εμπιστευτικότητας**, της **ακεραιότητας** και της **διαθεσιμότητας** των πληροφοριών και συστημάτων της ΡΑΑΕΥ, σύμφωνα με την κρισιμότητά τους για την επίτευξη των επιχειρησιακών στόχων, καθώς και της συμμόρφωσής του με το ισχύον νομοθετικό και ρυθμιστικό πλαίσιο.

Η Πολιτική Ασφάλειας αποτελεί το σύνολο, των κανόνων, των διαδικασιών, των ρόλων και των αρμοδιοτήτων για τη διασφάλιση της προστασίας των πληροφοριακών συστημάτων της ΡΑΑΕΥ και την εύρυθμη επιχειρησιακή του συνέχεια.

Βάσει της Πολιτικής Ασφάλειας Πληροφοριών η ΡΑΑΕΥ θεσπίζει Πολιτικές Διαχείρισης της Ασφάλειας Πληροφοριών και εφαρμόζει πιο συγκεκριμένες διαδικασίες ασφάλειας πληροφοριών καθώς και μέτρα ασφάλειας, μεταξύ άλλων για τη μείωση των κινδύνων που μπορεί να εκτεθεί. Στην παρούσα πολιτική περιγράφονται οι βασικές αρχές για τις οποίες καταγράφονται οι εν λόγω διαδικασίες.

## 1.5 Αρμοδιότητες και έλεγχος

1. **ΟΜ** – Ολομέλεια
2. **ΛΕΕ** – Λειτουργία Εσωτερικού Ελέγχου
3. **ΛΚΣ** – Λειτουργία Κανονιστικής Συμμόρφωσης
4. **ΛΑΠ** – Λειτουργία Ασφάλειας Πληροφοριών

| Κατηγορία | Ενέργεια | Εμπλεκόμενα Μέρη | | | |
|---|---|---|---|---|---|
| | | **ΟΜ** | **ΛΕΕ** | **ΛΚΣ** | **ΛΑΠ** |
| **Πολιτική** | Παροχή κατευθυντήριων γραμμών, βασικών αρχών και στόχων διακυβέρνησης | ✓ | | | |
| | Ανάπτυξη / Επικαιροποίηση Πολιτικής | | | | ✓ |
| | Έγκριση Πολιτικής | ✓ | | | |
| | Θεματοφύλακας Πολιτικής | | | ✓ | |
| | Επισκόπηση Πολιτικής | | | | ✓ |
| | Γνωστοποίηση Πολιτικής | | | ✓ | |
| | Διασφάλιση επισκόπησης και επικαιροποίησης Πολιτικής | ✓ | | | |
| | Εποπτεία εφαρμογής Πολιτικής | ✓ | | | |
| **Εφαρμογή, επισκόπηση και έλεγχος** | Παραγωγή Αναφορών | | | | ✓ |
| | Διενέργεια ελέγχου εφαρμογής της εγκεκριμένης Πολιτικής / Επισκόπηση αναφορών | | ✓ | | |

Αναφορικά με τη διασφάλιση, την προστασία και την ενημέρωση σε θέματα δεδομένων προσωπικού χαρακτήρα, αρμόδιος είναι ο Υπεύθυνος Προστασίας Δεδομένων όπως έχει οριστεί από τη ΡΑΑΕΥ. Η Ολομέλεια της ΡΑΑΕΥ διασφαλίζει πως το σύστημα διακυβέρνησης της ΡΑΑΕΥ και ιδίως το σύστημα Διαχείρισης Κινδύνων και Εσωτερικού Ελέγχου, διαχειρίζεται επαρκώς τους κινδύνους ΤΠΕ και ασφάλειας της ΡΑΑΕΥ.

Η Ολομέλεια της ΡΑΑΕΥ διασφαλίζει την επάρκεια του προσωπικού, τόσο σε πληρότητα όσο και ως προς τις δεξιότητες που αυτό διαθέτει.

### 1.6 Επισκόπηση, Αναθεώρηση και Τήρηση Αρχείου

Η παρούσα Πολιτική επισκοπείται ετησίως από τη Λειτουργία Ασφάλειας Πληροφοριών. Αναθεώρηση της Πολιτικής ενδέχεται να πραγματοποιηθεί εκτάκτως όποτε το απαιτούν οι περιστάσεις λόγω μεταβολών είτε στο νομο-κανονιστικό πλαίσιο είτε σε συναφείς πολιτικές και διαδικασίες, έτσι ώστε να ανταποκρίνεται στις εκάστοτε ισχύουσες συνθήκες.

Η Λειτουργία Κανονιστικής Συμμόρφωσης είναι υπεύθυνη για τη διατήρηση σε ηλεκτρονική μορφή των εκδόσεων της Πολιτικής, καθώς και για τη διατήρηση φύλλου παρακολούθησης των τροποποιήσεων της, έτσι ώστε να είναι άμεσα διαθέσιμη και προσβάσιμη στα πρόσωπα που εμπίπτουν σε αυτήν. Η Λειτουργία Ασφάλειας Πληροφοριών είναι υπεύθυνη να γνωστοποιεί στα εμπλεκόμενα μέρη την Πολιτική καθώς και τυχόν τροποποιήσεις αυτής δια της κοινοποιήσεως της μέσω οποιουδήποτε πρόσφορου μέσου, αρκεί να δύναται να αποδεικνύεται η ενημέρωση αυτών.

### 1.7 Πρόγραμμα μη συμμόρφωσης

Σε περίπτωση που οποιοσδήποτε εργαζόμενος της ΡΑΑΕΥ αντιληφθεί πραγματική ή δυνητική μη συμμόρφωση με την παρούσα Πολιτική που θα έχει ως αποτέλεσμα την παραβίαση της εμπιστευτικότητας, της ακεραιότητας ή / και της διαθεσιμότητας των πληροφοριακών συστημάτων και πληροφοριών της ΡΑΑΕΥ, ενημερώνει άμεσα τη Λειτουργία Ασφάλειας Πληροφοριών ή σε περίπτωση απουσίας της τη Γενική Διεύθυνση. Η Λειτουργία αξιολογεί την αναφορά και είτε παρεμβαίνει είτε κοινοποιεί το θέμα στο Δ.Σ., το οποίο αποφαίνεται για την επιβολή τυχόν πειθαρχικών κυρώσεων.

## 2. Ορισμοί

**Πολιτική**: Η Πολιτική Ασφάλειας Πληροφοριών

**ΡΑΑΕΥ**: **ΡΥΘΜΙΣΤΙΚΗ ΑΡΧΗ ΑΠΟΒΛΗΤΩΝ, ΕΝΕΡΓΕΙΑΣ ΚΑΙ ΥΔΑΤΩΝ**

**ΤΠΕ**: Τεχνολογίες Πληροφοριών και Επικοινωνίας

**Πληροφοριακό Σύστημα**: είναι ένα οργανωμένο σύνολο που αποτελείται από πέντε στοιχεία: ανθρώπους, υλικό, λογισμικό, διαδικασίες και δεδομένα, τα οποία αλληλοεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση πληροφορίας για την υποστήριξη ανθρώπινων δραστηριοτήτων, στο πλαίσιο ενός οργανισμού.

**Ακεραιότητα**: Η διασφάλιση της ακρίβειας και της πληρότητας της πληροφορίας.

**Διαθεσιμότητα**: Η διασφάλιση της διαθεσιμότητας της πληροφορίας και των πληροφοριακών πόρων στη διάθεση των χρηστών όποτε αυτό απαιτείται.

**Εμπιστευτικότητα**: Η διασφάλιση ότι πληροφορίες δε θα αποκαλύπτονται (δημοσιοποιούνται) σε μη εξουσιοδοτημένα πρόσωπα, φορείς, διαδικασίες ή συστήματα.

# 3. Οργάνωση Ασφάλειας Πληροφοριών

## 3.1 Εσωτερική οργάνωση

Η ΡΑΑΕΥ τηρεί ένα πλαίσιο ασφάλειας πληροφοριακών συστημάτων και πληροφοριών προκειμένου να διαχειρίζεται αποτελεσματικότερα την ασφάλειά τους. Το πλαίσιο ασφάλειας εναρμονίζεται πλήρως, τόσο με την φύση των πληροφοριακών αγαθών και των επιχειρησιακών απαιτήσεων της ΡΑΑΕΥ, όσο και με την πολυπλοκότητα των δραστηριοτήτων που καλείται να διαχειριστεί Η ΡΑΑΕΥ.

Η ΡΑΑΕΥ διατηρεί κατάλληλο διοικητικό σχήμα το οποίο:

- Εξασφαλίζει ότι Η ΡΑΑΕΥ διαθέτει τους απαραίτητους πόρους για την αποτελεσματική εφαρμογή της Πολιτικής
- Αναθέτει τους ρόλους και τις αρμοδιότητες σε σχέση με την ασφάλεια πληροφοριών
- Συντονίζει την υλοποίηση του προγράμματος της ασφάλειας πληροφοριών στην ΡΑΑΕΥ
- Διασφαλίζει ότι οι στόχοι της Πολιτικής είναι ευθυγραμμισμένοι με τους γενικότερους στόχους της ΡΑΑΕΥ.
- Η καθιέρωση και η επιτυχής εφαρμογή της Πολιτικής απαιτούν τη συνεργασία όλων όσοι εμπλέκονται στην επίτευξη των επιχειρησιακών στόχων της ΡΑΑΕΥ: της Διοίκησης, των στελεχών, των χρηστών, των προμηθευτών, των αναδόχων, των επισκεπτών και των τρίτων συνεργαζόμενων φορέων.
- Η ΡΑΑΕΥ θα τηρεί σαφώς καθορισμένους ρόλους και αρμοδιότητες για το σύνολο των στελεχών, υπαλλήλων, συνεργατών και τρίτων μερών, σύμφωνα με την «Πολιτική Οργάνωσης Ασφάλειας Πληροφοριακών Συστημάτων & Πληροφοριών».

# 4. Γενικές Αρχές της Πολιτικής

## 4.1 Ελαχιστοποίηση Κινδύνων

Η ασφάλεια των πληροφοριών και πληροφοριακών συστημάτων της ΡΑΑΕΥ αποτελεί στρατηγικής σημασίας στόχο και υποχρέωσή της. Η ΡΑΑΕΥ εφαρμόζει μια πολιτική μέσω της οποίας είναι σε θέση να επιβλέπει και να ελέγχει την ασφάλεια των πληροφοριακών του αγαθών ώστε να είναι σε θέση να ελαχιστοποιεί τους κινδύνους και τις πιθανές επιπτώσεις τους.

## 4.2 Πρόσβαση όπου απαιτείται

Τα πληροφοριακά συστήματα της ΡΑΑΕΥ, καθώς και οι πληροφορίες σε φυσική / έντυπη μορφή, αποτελούν απαραίτητους πόρους για την επίτευξη των επιχειρησιακών της στόχων. Η ΡΑΑΕΥ παρέχει πρόσβαση στις πληροφορίες του μόνο στα άτομα που απαιτούνται για την επίτευξη των επιχειρησιακών του στόχων («need to know» principle).

## 4.3 Ακεραιότητα, Εμπιστευτικότητα και Διαθεσιμότητα

Τα πληροφοριακά συστήματα, καθώς και οι πληροφορίες της ΡΑΑΕΥ διαχειρίζονται και χρησιμοποιούνται κατάλληλα, ώστε να διασφαλίζεται η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητά τους.

## 4.4 Προβλεπόμενη χρήση αγαθών

Τα πληροφοριακά συστήματα και οι πληροφορίες αποτελούν αγαθό της ΡΑΑΕΥ και μπορούν να χρησιμοποιηθούν μόνο για την επίτευξη των επιχειρησιακών στόχων της. Η χρήση τους από το προσωπικό της ΡΑΑΕΥ ή τρίτους με σκοπό την αποκόμιση προσωπικού κέρδους, τη διεξαγωγή επιχειρηματικών δραστηριοτήτων εκτός αυτών της ΡΑΑΕΥ ή με σκοπό να διαπράξουν αξιόποινες πράξεις δεν επιτρέπεται. Για περισσότερες πληροφορίες δείτε «Πολιτική Αποδεκτής Διαχείρισης Αγαθών».

## 4.5 Περιστατικά Ασφαλείας

Πληροφορίες μη κατηγοριοποιημένες ως «Δημόσιες» πρέπει να προστατεύονται και δεν πρέπει να δημοσιοποιούνται χωρίς την κατάλληλη έγκριση. Μη εξουσιοδοτημένη πρόσβαση, διαχείριση, δημοσιοποίηση ή αναπαραγωγή και μετάδοση αυτών των πληροφοριών διακυβεύει την ασφάλεια της ΡΑΑΕΥ, αποτελεί «Περιστατικό Ασφάλειας».

## 4.6 Περιστατικά Διαχείρισης Λειτουργικού Κινδύνου

Η ασφάλεια πληροφοριών αποτελεί ένα ζήτημα διαχείρισης λειτουργικού κινδύνου. Σε όλες τις Διευθύνσεις και τα Τμήματα της ΡΑΑΕΥ εφαρμόζονται βέλτιστες πρακτικές (σύμφωνα με τη «Πολιτική Αποδεκτής Διαχείρισης Αγαθών») και δικλείδες ασφάλειας προς ελαχιστοποίηση των κινδύνων.

## 4.7 Ενημέρωση Ασφάλειας Πληροφοριών

Περιστατικά ασφάλειας πρέπει να αναφέρονται άμεσα αρχικά στον Υπεύθυνο της Λειτουργίας Ασφάλειας Πληροφοριών, η οποία είναι αρμόδια να αξιολογήσει τη σοβαρότητα και να λάβει τα κατάλληλα μέτρα και εν συνεχεία στον Υπεύθυνο Διαχείρισης Κινδύνων και στο Τμήμα Μηχανογράφησης.

## 4.8 Μεταβολές ρόλων και Αρμοδιοτήτων

Όλες οι Διευθύνσεις / Τμήματα της ΡΑΑΕΥ παρέχουν άμεση ενημέρωση στους διαχειριστές συστημάτων και στη Λειτουργία Ασφάλειας Πληροφοριών αναφορικά με μεταβολές στην εργασιακή θέση, το ρόλο και τις αρμοδιότητες μέσα στην ΡΑΑΕΥ (μεταθέσεις, αποχωρήσεις, προσλήψεις, έναρξη συνεργασίας κ.λπ.) των υπάλληλων, συνεργατών ή τρίτων, οι οποίες χρήζουν απόδοσης ή μεταβολής δικαιωμάτων πρόσβασης στα πληροφοριακά συστήματα της ΡΑΑΕΥ.

### 4.9 Πρακτικές Ασφαλείας

Ο Υπεύθυνος Μηχανογράφησης και η Λειτουργία Ασφάλειας Πληροφοριών είναι αρμόδιοι να δημιουργούν και να προάγουν κατάλληλες πρακτικές ασφάλειας (security practices) στο σύνολο της ΡΑΑΕΥ, συμπεριλαμβανομένων:

- Ενημερώσεων σε υφιστάμενο και νέο προσωπικό
- Προγραμμάτων ενίσχυσης της κουλτούρας κινδύνων / ευαισθητοποίησης Ασφάλειας Πληροφοριών (Information Security Awareness)

### 4.10 Ιδιοκτήτες Πληροφοριών

Η ΡΑΑΕΥ προσδιορίζει εγγράφως όλους τους «ιδιοκτήτες πληροφοριών» για το σύνολο των Πληροφοριακών συστημάτων και κατηγοριών πληροφοριών.

## 5. Ασφάλεια Ανθρώπινου Δυναμικού

Η ΡΑΑΕΥ εξασφαλίζει ότι όλοι οι χρήστες (υπάλληλοι, ανάδοχοι, τρίτοι) κατανοούν τις ευθύνες τους σχετικά με την ασφάλεια πληροφοριών και ότι είναι κατάλληλοι για τους ρόλους για τους οποίους έχουν επιλεγεί. Η πολιτική ασφάλειας ανθρώπινου δυναμικού έχει ως σκοπό την ελαχιστοποίηση των κινδύνων από ανθρώπινο λάθος, κλοπή και σκόπιμο ή ακούσιο κακό χειρισμό των πληροφοριακών αγαθών της ΡΑΑΕΥ, καθώς επίσης την ενσωμάτωση της ασφάλειας πληροφοριών στις περιγραφές εργασίας και τις διαδικασίες πρόσληψης προσωπικού.

### 5.1 Πριν από την Απασχόληση

Η ΡΑΑΕΥ λαμβάνει μέριμνα ώστε να ελαχιστοποιείται η πιθανότητα πρόσληψης προσωπικού που μπορεί να τον θέσει σε κίνδυνο, όπου αυτό είναι εφικτό και σύμφωνα με το υφιστάμενο νομικό και κανονιστικό πλαίσιο. Ιδιαίτερη μέριμνα θα λαμβάνεται για προσλήψεις που αφορούν καίριες θέσεις της ΡΑΑΕΥ, συμπεριλαμβανομένων αυτών που σχετίζονται με την επεξεργασία ευαίσθητων δεδομένων.

**Πολιτική Επιλογής Προσωπικού (Personnel Screening Policy)**

Η ΡΑΑΕΥ θα διεξάγει ελέγχους επαλήθευσης των στοιχείων όλων των υποψηφίων και ειδικότερα σε επιλογή προσωπικού σε θέσεις οι οποίες έχουν σαν προϋπόθεση αυξημένες απαιτήσεις ασφάλειας, σύμφωνα με τους σχετικούς νόμους και κανονισμούς, εφόσον αυτό κρίνεται απαραίτητο. Για τη διασφάλιση της ακεραιότητας και εμπιστευτικότητας των εταιρικών δεδομένων, το προσωπικό της ΡΑΑΕΥ που θα εμπλέκεται σε επεξεργασία προσωπικών δεδομένων και ευαίσθητων εταιρικών πληροφοριών, θα πρέπει να διαθέτει επάρκεια γνώσεων και κατάρτιση στο χειρισμό αντίστοιχου τύπου δεδομένων. Τα δεδομένα των υποψηφίων υπαλλήλων που συλλέγονται θα πρέπει να περιορίζονται στα απολύτως αναγκαία. Τα παραπάνω ισχύουν επίσης για έκτακτο προσωπικό καθώς και για τους εξωτερικούς συνεργάτες της ΡΑΑΕΥ. Ιδιαίτερα για προσωπικό το οποίο επιλέγεται με τη βοήθεια κάποιου γραφείου ευρέσεως στελεχών ή ανήκει σε τρίτες εταιρίες (outsourced), οι ευθύνες τους έναντι της ΡΑΑΕΥ θα πρέπει να είναι ξεκάθαρες.

**Όροι και Συνθήκες Απασχόλησης (Terms and conditions of employment)**

Η ΡΑΑΕΥ μέσω του Τμήματος Ανθρωπίνου Δυναμικού, μεριμνά ώστε κάθε νέος εργαζόμενος να ενημερώνεται για τις ευθύνες και τις αρμοδιότητές του σχετικά με την ασφάλεια πληροφοριών, οι οποίες θα προβλέπονται και από τη σύμβαση εργασίας. Ειδικότερα εξωτερικοί συνεργάτες οι οποίοι απασχολούνται σε θέσεις που τους παρέχουν πρόσβαση σε διαβαθμισμένες πληροφορίες, θα υπογράφουν σχετική συμφωνία εμπιστευτικότητας και μη δημοσιοποίησης πληροφοριών κατά την ανάληψη των καθηκόντων τους. Οι συμφωνίες εμπιστευτικότητας θα εξετάζονται και θα αναθεωρούνται όταν υπάρχουν μεταβολές σε συμβάσεις ή συμβόλαια με υπαλλήλους ή τρίτα μέρη.

## 5.2 Κατά τη Διάρκεια της Απασχόλησης

Όλοι όσοι εργάζονται στην ΡΑΑΕΥ θα εφαρμόζουν τις πολιτικές και τις διαδικασίες ασφάλειας και θα τους γίνονται περιοδικές υπενθυμίσεις σχετικά με τις υποχρεώσεις που απορρέουν από την Πολιτική . Η Διοίκηση εξασφαλίζει ότι το σύνολο του προσωπικού της ΡΑΑΕΥ, καθώς και τρίτα μέρη κατά περίπτωση, θα λαμβάνουν κατάλληλη ενημέρωση για την Πολιτική Ασφαλείας και τις σχετικές με αυτή διαδικασίες. Στο πλαίσιο αυτό θα εφαρμόζεται ένα περιοδικό πρόγραμμα αύξησης της επίγνωσης κίνδυνων (awareness campaign) του προσωπικού του προσαρμοσμένο στις ανάγκες της ΡΑΑΕΥ.

Σε όλο το νέο προσωπικό της ΡΑΑΕΥ υποχρεωτικά θα γίνεται τεκμηριωμένη ενημέρωση / εκπαίδευση σε θέματα ασφάλειας πληροφοριών κατά την περίοδο της ένταξης / προσαρμογής τους στο εργασιακό περιβάλλον της ΡΑΑΕΥ, πριν αποκτήσουν πρόσβαση σε προσωπικά και ευαίσθητα δεδομένα, απόρρητες πληροφορίες ή πληροφοριακά συστήματα.

## 5.3 Λήξη ή Μεταβολή Απασχόλησης

Σε περίπτωση μεταβολής της θέσης κάποιου εργαζομένου, οι ανάγκες του σε θέματα ασφάλειας πληροφοριών θα επαναξιολογούνται και εάν κρίνεται απαραίτητο, θα του παρέχεται η ανάλογη ενημέρωση.

Κατά τη διαδικασία λήξης της εργασιακής σχέσης με την ΡΑΑΕΥ, όλοι οι χρήστες (υπάλληλοι, ανάδοχοι, τρίτοι) των πληροφοριακών συστημάτων θα επιστρέφουν τον εξοπλισμό (φορητοί υπολογιστές, φωτογραφικές μηχανές, κ.λπ.) που τους παρασχέθηκε για την εκπλήρωση των εργασιών τους, όπως περιγράφεται στη «Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας». Επιπλέον θα επιστρέφεται στην ΡΑΑΕΥ οποιοσδήποτε άλλος πληροφοριακός πόρος τους έχει παρασχεθεί, όπως για παράδειγμα εγχειρίδια και πληροφορίες που βρίσκονται αποθηκευμένες σε ηλεκτρονικά μέσα κλπ.

Σε περιπτώσεις που υπάλληλοι, ανάδοχοι, τρίτοι, χρησιμοποιούν δικό τους εξοπλισμό, θα πρέπει να διασφαλίζεται ότι τυχόν ευαίσθητες πληροφορίες της ΡΑΑΕΥ που είναι αποθηκευμένες στον εν λόγω εξοπλισμό θα διαγράφονται.

Τα δικαιώματα πρόσβασης του προσωπικού στα πληροφοριακά συστήματα της ΡΑΑΕΥ, όπως και τα δικαιώματα φυσικής πρόσβασης στις εγκαταστάσεις της ΡΑΑΕΥ θα αλλάζουν ή θα καταργούνται με μέριμνα του Υπεύθυνου Μηχανογράφησης, όταν η εργασιακή σχέση του ατόμου αυτού παύει ή μεταβάλλεται αντίστοιχα. Στις περιπτώσεις λήξης της εργασιακής σχέσης, οι εργαζόμενοι θα

επιστρέφουν στη ΡΑΑΕΥ τις ειδικές κάρτες που τους είχαν δοθεί για την πρόσβαση στα γραφεία της ΡΑΑΕΥ, όπως περιγράφεται στη «Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας».

Συμφωνίες εμπιστευτικότητας και μη δημοσιοποίησης ευαίσθητων πληροφοριών που εξακολουθούν να ισχύουν μετά την λήξη της απασχόλησης θα καθορίζονται, θα επικοινωνούνται στον υπάλληλο και θα πρέπει να εφαρμόζονται.

## 6. Διαχείριση Αγαθών

Στην «Πολιτική Αποδεκτής Διαχείρισης Αγαθών» προβλέπεται πως Η ΡΑΑΕΥ, για κάθε ένα από τα πληροφοριακά αγαθά της, προσδιορίζει «Ιδιοκτήτες» και αναπτύσσει τα κατάλληλα μέτρα για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, τροποποίησης και καταστροφής τους, αποσκοπώντας στη διατήρηση ενός κατάλληλου επιπέδου προστασίας τους.

## 7. Διαβάθμιση Πληροφοριών

Σύμφωνα με την «Πολιτική Διαβάθμισης Πληροφοριών», οι πληροφορίες της ΡΑΑΕΥ διαβαθμίζονται με κριτήριο το βαθμό ευαισθησίας τους, τις συνέπειες από πιθανή απώλειά τους ή από πιθανή απώλεια της εμπιστευτικότητας τους, καθώς και σύμφωνα με τις υποχρεώσεις που Η ΡΑΑΕΥ φέρει απέναντι στη νομοθεσία στην οποία υπόκειται.

## 8. Έλεγχος Πρόσβασης

Η πρόσβαση στα Πληροφοριακά Συστήματα της ΡΑΑΕΥ είναι περιορισμένη και ελεγχόμενη σύμφωνα με την «Πολιτική Ελέγχου Πρόσβασης», έτσι ώστε να διασφαλίζεται πως μόνο εξουσιοδοτημένοι και ταυτοποιημένοι χρήστες έχουν δικαιώματα πρόσβασης στους πόρους και τις πληροφορίες της ΡΑΑΕΥ.

### 8.1 Επιχειρησιακή Απαίτηση για τον Έλεγχο της Πρόσβασης

Πριν από την παραχώρηση πρόσβασης σε οποιοδήποτε πληροφοριακό πόρο εξετάζεται η επιχειρησιακή αναγκαιότητα ώστε να διασφαλίζεται η ασφάλεια των πληροφοριών της ΡΑΑΕΥ. Εφαρμόζεται πολιτική ελέγχου πρόσβασης, σύμφωνα με τις επιχειρησιακές απαιτήσεις της ΡΑΑΕΥ.

Η πρόσβαση στα πληροφοριακά συστήματα πρέπει να διασφαλίζεται από μέτρα ταυτοποίησης του χρήστη και καθορισμού του επιπέδου πρόσβασής του. Η πρόσβαση στα πληροφοριακά συστήματα πρέπει να είναι επαρκής αλλά ποτέ μεγαλύτερη των απαιτήσεων των χρηστών για την εκπλήρωση του επιχειρησιακού τους ρόλου και έργου.

**Διαχείριση Πρόσβασης Χρηστών**

Όλα τα τμήματα πρέπει να εφαρμόζουν τυποποιημένη διαδικασία, με την οποία καταγράφονται οι απαιτούμενες μεταβολές και αναφέρονται στον Διευθυντή Πληροφορικής, ώστε τα δικαιώματα των χρηστών να μεταβάλλονται ή να καταργούνται άμεσα. Η απόδοση των δικαιωμάτων πρέπει να βασίζεται στην αρχή των ελάχιστων προνομίων.

## 8.2 Ευθύνες Χρηστών

Όλοι οι χρήστες των πληροφοριακών συστημάτων πρέπει να ακολουθούν πρακτικές ασφάλειας καθορισμένες από την ΡΑΑΕΥ που αφορούν στην επιλογή και στη χρήση των κωδικών πρόσβασης. Όλοι οι χρήστες της ΡΑΑΕΥ λαμβάνουν τα απαραίτητα μέτρα για την προστασία των πληροφοριών και του πληροφοριακού εξοπλισμού που βρίσκονται στον χώρο εργασίας τους.

## 8.3 Έλεγχος Πρόσβασης σε Λειτουργικά Συστήματα και Εφαρμογές

Σε όλους τους χρήστες παρέχεται ένα μοναδικής ταυτότητας αναγνωριστικό χρήστη (user ID) για προσωπική τους χρήση, ενώ η πρόσβαση στα λειτουργικά συστήματα ελέγχεται μέσω μιας ασφαλούς διαδικασίας σύνδεσης, η οποία περιλαμβάνει κατ' ελάχιστον τη χρήση ισχυρού κωδικού πρόσβασης.

Οι κωδικοί πρόσβασης είναι αυστηρώς προσωπικοί και δεν κοινοποιούνται ή αποκαλύπτονται. Για την καλύτερη προστασία των κρίσιμων εφαρμογών, οι ανενεργές συνδέσεις διακόπτονται μετά από μια καθορισμένη περίοδο αδράνειας.

## 8.4 Φορητά Μέσα Ηλεκτρονικών Υπολογιστών

Η χρήση φορητών ηλεκτρονικών υπολογιστών απαιτεί έγκριση από τον Διευθυντή Πληροφορικής και τον αρμόδιο Διευθυντή ή Προϊστάμενο. Η χρήση αποσπώμενων αποθηκευτικών μέσων (USB Flash drives, External Disks κ.λπ.) περιορίζεται μέσω σχετικού μηχανισμού και επιτρέπεται όπου απαιτείται για την εκπλήρωση των επιχειρησιακών αναγκών.

## 8.5 Φορητές Ιδιωτικές Συσκευές (BYOD)

Ως φορητές, ιδιωτικές συσκευές θεωρούνται, μεταξύ άλλων, οι εξής:

- Συσκευές Tablet
- Έξυπνα κινητά (smartphones)
- Φορητοί υπολογιστές (laptop)
- Φορέσιμες έξυπνες συσκευές (wearables π.χ. έξυπνα ρολόγια, έξυπνα γυαλιά, κλπ.)

Η παραχώρηση άδειας στον εργαζόμενο, ώστε να κάνει χρήση δικών του συσκευών για επαγγελματικούς σκοπούς μπορεί να οδηγήσει στην ανάγκη υλοποίησης πρόσθετων ελέγχων και μέτρων προστασίας στις συσκευές αυτές, πέραν εκείνων που λαμβάνονται για μια απλή συσκευή προσωπικής χρήσης. Συνηθισμένα προβλήματα σε σχέση με τη χρήση φορητών, ιδιωτικών συσκευών περιλαμβάνουν:

- Χρήση της συσκευής από άλλα μέλη της οικογένειας του υπαλλήλου.
- Προεπιλεγμένη αποθήκευση των δεδομένων σε εγκαταστάσεις Νεφοϋπολογιστικής (Cloud).
- Αυξημένη έκθεση σε κίνδυνο πιθανής απώλειας (πχ. χρήστη σε καφετέρια κλπ.)
- Πρόσβαση σε δικτυακούς τόπους που δεν πληρούν την *Πολιτική Αποδεκτή Χρήσης Διαδικτύου* της ΡΑΑΕΥ.
- Σύνδεση σε μη ασφαλή δίκτυα.

- Έλλειψη προστασίας από ιούς και έλλειψη ενημέρωσης αντιικού λογισμικού.
- Εγκατάσταση δυνητικά κακόβουλων εφαρμογών στη συσκευή (συχνά χωρίς να γνωρίζει ο χρήστης ότι είναι κακόβουλες).

Τα θέματα αυτά πρέπει να λαμβάνονται υπόψη κατά την αξιολόγηση της καταλληλόλητας οποιασδήποτε τέτοιας συσκευής, πριν καταστεί ικανή για τήρηση δεδομένων που ανήκουν στη ΡΑΑΕΥ.

## 9. Τηλεργασία

Μια σύμβαση τηλεργασίας είναι μια συμφωνία μεταξύ της ΡΑΑΕΥ και του εργαζομένου. Αφορά συνθήκες, κατά τις οποίες ο εργαζόμενος εργάζεται σε χώρους εκτός της ΡΑΑΕΥ, είτε αυτό είναι ένα σπίτι ή άλλος τύπος εγχώριας κατοικίας.

Η τηλεργασία στη ΡΑΑΕΥ επιτρέπεται μόνο κατ' εξαίρεση και εφόσον κριθεί απολύτως αναγκαίο από τη Διοίκηση, ύστερα από έγκριση του Υπευθύνου Ασφάλειας Πληροφοριών και τήρηση των μέτρων ασφάλειας που ορίζονται στην παρούσα ενότητα. Η ΡΑΑΕΥ δύναται να απασχολεί εξειδικευμένο και έμπειρο προσωπικό υπό συνθήκες τηλεργασίας, όποτε το κρίνει σκόπιμο και υπό τις προϋποθέσεις που τίθενται κατωτέρω.

Η συγκεκριμένη πολιτική καθορίζει τα βασικά ζητήματα ασφάλειας πληροφοριών που πρέπει να εξετάζονται για κάθε συμφωνία μιας σύμβασης τηλεργασίας. Διασφαλίζει ότι όλα τα αναγκαία ζητήματα αντιμετωπίζονται και ότι τα πληροφοριακά αγαθά της ΡΑΑΕΥ προστατεύονται.

Η παρούσα πολιτική δεν ασχολείται με τις πτυχές του ανθρώπινου δυναμικού της τηλεργασίας, όπως η υγεία, η ασφάλεια, η παρακολούθηση των απουσιών, η απόδοση στην εργασία και άλλα παρόμοια συμβατικά θέματα. Τέτοια θέματα εμπίπτουν στις αρμοδιότητες του τμήματος Ανθρώπινου Δυναμικού και πρέπει να έχουν αποφασιστεί, πριν από την έναρξη της σύμβασης τηλεργασίας.

### 9.1 Εξοπλισμός

- Για τους σκοπούς της τηλεργασίας και για την απομακρυσμένη πρόσβαση στα επιχειρησιακά δίκτυα της ΡΑΑΕΥ, μπορεί να χρησιμοποιηθεί μόνο ο εξοπλισμός που παρέχεται από τη ΡΑΑΕΥ. Ιδιωτικές συσκευές του εργαζομένου, όπως φορητοί υπολογιστές ή tablet/smartphones δεν πρέπει να χρησιμοποιούνται για το σκοπό αυτό, εκτός και αν υπάρχει σχετική έγκριση από τον *Υπεύθυνο Ασφάλειας*.
- Σύμφωνα με τις απαιτήσεις, στον τηλεργαζόμενο μπορεί να παρέχεται ένας φορητός ή σταθερός υπολογιστής με πληκτρολόγιο και ποντίκι. Ο εξοπλισμός παραμένει ιδιοκτησία της ΡΑΑΕΥ ακόμη και μετά τη λήξη της συνεργασίας με τον υπάλληλο.
- Οι *Διαχειριστές Συστημάτων* της ΡΑΑΕΥ είναι αρμόδιοι για την ρύθμιση του αναγκαίου εξοπλισμού, για κάθε ξεχωριστή περίπτωση τηλε-εργασίας.
- Όπου είναι εφικτό, η απομακρυσμένη θέση τηλεργασίας πρέπει να εποπτεύεται και να γίνεται εκτίμηση του κινδύνου της, πριν αποφασιστούν τα μέτρα ασφάλειας που πρέπει να χρησιμοποιηθούν.
- Κάθε τηλεργαζόμενος πρέπει να έχει ενημερωθεί για τους κινδύνους της τηλεργασίας και να έχει εκπαιδευτεί κατάλληλα στους τρόπους αντιμετώπισής τους.

- Ο τηλεργαζόμενος πρέπει να αποδέχεται πως αντιλαμβάνεται τους κινδύνους, τα δικαιώματα και τις υποχρεώσεις του ως προς τον ρόλο που του ανατίθεται και να υπογράφει σχετική υπεύθυνη δήλωση.
- Ο τηλεργαζόμενος είναι υπεύθυνος, ώστε να διασφαλίζει πως κανένας δεν έχει πρόσβαση στο τερματικό εργασίας του.
- Ο τηλεργαζόμενος είναι υπεύθυνος για τυχόν πληροφορίες της ΡΑΑΕΥ, που μπορεί διαρρεύσουν, ως αποτέλεσμα δικής του αμέλειας (πχ. αν ξεχάσει έγγραφα στο χώρο τηλε-εργασίας).
- Ο εξοπλισμός τηλεργασίας πρέπει να ασφαλίζεται κατάλληλα, κάθε φορά που ο τηλεργαζόμενος διακόπτει την εργασία του (πχ. χρήση λουκέτων, ειδικών φοριαμών κλπ.).
- Μετά την εφαρμογή όλων των προαπαιτούμενων μέτρων ασφαλείας στην απομακρυσμένη τοποθεσία τηλεργασίας, η αυθεντικοποίηση του τηλεργαζόμενου ακολουθεί την ίδια διαδικασία που ακολουθούν και οι υπάλληλοι τοπικά στα γραφεία της ΡΑΑΕΥ.

## 9.2 Επικοινωνίες

Εκτός από τον εξοπλισμό (και όταν αυτό καθίσταται δυνατό), ο τηλεργαζόμενος πρέπει να είναι εφοδιασμένος με μια ξεχωριστή σύνδεση επικοινωνιών που δεν συνδέεται με κανέναν τρόπο με τα ήδη υφιστάμενα εθνικά ευρυζωνικά δίκτυα ή κάτι παρόμοιο. Αυτό γίνεται για να εξασφαλιστεί ότι:

- Η απόδοση του δικτύου δεν θα πρέπει να επηρεάζεται από άλλες δραστηριότητες στο σπίτι.
- Η δυνατότητα σύνδεσης άλλων συσκευών σε αυτή τη σύνδεση, μπορεί να προληφθεί μέσω της προστασίας των κλειδιών δικτύου κλπ.

Κάθε απομακρυσμένη σύνδεση τηλεργασίας πρέπει να τερματίζεται αμέσως μόλις διακόπτεται η εργασία του τηλεργαζόμενου.

## 9.3 Λήψη αντιγράφων ασφαλείας στην Τηλεργασία

- Όπου είναι δυνατόν, τα δεδομένα δεν πρέπει να αποθηκεύονται στον υπολογιστή του τηλεργαζόμενου. Σε περίπτωση που αυτό είναι αναπόφευκτο, είναι ευθύνη του τηλεργαζόμενου να διασφαλίσει ότι τα αντίγραφα ασφαλείας θα αποθηκεύονται για όσο το δυνατόν μικρότερο χρονικό διάστημα εκτός του εταιρικού δικτύου και θα μεταφέρονται το συντομότερο δυνατόν στο επιχειρησιακό δίκτυο της ΡΑΑΕΥ.
- Δεν πρέπει να αποθηκεύετε τα μη κρυπτογραφημένα αντίγραφα ασφαλείας σε άλλες υπηρεσίες υπολογιστικού νέφους (cloud services) πλην αυτών που έχει ορίσει ο *Διαχειριστής του Συστήματος*.

## 9.4 Καταγγελία σύμβασης

- Σε περίπτωση που η σύμβαση τηλεργασίας τερματιστεί για οποιονδήποτε λόγο, όλος ο εξοπλισμός που παρέχεται ως μέρος της σύμβασης πρέπει να επιστραφεί στον *Υπεύθυνο Ασφάλειας* και στη *Διεύθυνση Πληροφορικής* το συντομότερο δυνατόν.

## 10. Πολιτική Κρυπτογραφίας

Η ΡΑΑΕΥ, όπου είναι τεχνικά εφικτό δύναται να εφαρμόζει πολιτική για τη χρήση κρυπτογραφικών μέτρων για την προστασία των κρίσιμων πληροφοριών της. Κρυπτογραφικές μέθοδοι χρησιμοποιούνται στους κωδικούς πρόσβασης για τη διαχείριση των κρίσιμων συστημάτων και των λογαριασμών της ΡΑΑΕΥ όταν αυτοί αποθηκεύονται ή μεταφέρονται μέσω του δικτύου. Επιπλέον, φορητά αποθηκευτικά μέσα που περιέχουν πληροφορίες της ΡΑΑΕΥ προστατεύονται με τους κατάλληλους κρυπτογραφικούς μηχανισμούς.

Η κρυπτογράφηση πρέπει να εφαρμόζεται για τα ευαίσθητα περιουσιακά στοιχεία πληροφοριών, τόσο κατά τη μεταφορά όσο και κατά την ηρεμία, με βάση την αξιολόγηση των κινδύνων και των νομικών/κανονιστικών απαιτήσεων.

Οι αλγόριθμοι κρυπτογράφησης και τα μήκη κλειδιών πρέπει να επιλέγονται με βάση τις βέλτιστες πρακτικές του κλάδου και τη συμμόρφωση με τα ισχύοντα πρότυπα.

Ισχυρή κρυπτογράφηση πρέπει να χρησιμοποιείται για ασύρματες επικοινωνίες, απομακρυσμένη πρόσβαση και κάθε άλλη ευαίσθητη μετάδοση δεδομένων.

Εφαρμόζεται κρυπτογράφηση σε όλες τις συσκευές ακόμα και στην τηλεργασία, με σκοπό την προστασία των διαβαθμισμένων πληροφοριών, εάν η συσκευή παρέχεται με κρυπτογράφηση, τότε δεν πρέπει να την απενεργοποιήσετε.

Όταν οι πληροφορίες πρόκειται να μεταφερθούν μέσω ενός δημόσιου δικτύου, όπως το Διαδίκτυο, τότε πρέπει να χρησιμοποιείται ισχυρή κρυπτογράφηση μέσω SSL, για τη διασφάλιση της εμπιστευτικότητας των δεδομένων που διαβιβάζονται. Συγκεκριμένα, πρέπει να εγκατασταθούν έμπιστα πιστοποιητικά στους δικτυακούς ιστότοπους της ΡΑΑΕΥ με μέγεθος κλειδιού τουλάχιστον 2048 bits.

Επίσης, όλες οι συσκευές Bluetooth πρέπει να χρησιμοποιούν Secure Simple Pairing με ενεργοποιημένη την κρυπτογράφηση.

**Πάροχοι υπηρεσιών κρυπτογράφησης:**

Κατά την πρόσληψη τρίτων παρόχων κρυπτογραφικών υπηρεσιών, ο οργανισμός πρέπει να διασφαλίζει ότι αυτοί τηρούν τις βέλτιστες πρακτικές του κλάδου, διαθέτουν σχετικές πιστοποιήσεις και συμμορφώνονται με τις νομικές και κανονιστικές απαιτήσεις.

Οι συμβάσεις ή οι συμφωνίες με τους παρόχους κρυπτογραφικών υπηρεσιών πρέπει να καθορίζουν σαφώς τους ρόλους, τις αρμοδιότητες και τις απαιτήσεις ασφαλείας.

## 11. Φυσική και Περιβαλλοντική Ασφάλεια

Όλα τα μέλη του προσωπικού πρέπει να εφαρμόζουν τις πολιτικές και τις διαδικασίες ασφάλειας της ΡΑΑΕΥ που αφορούν στη φυσική και περιβαλλοντική προστασία των πληροφοριακών της αγαθών, έτσι ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση, καθώς και η καταστροφή και η επέμβαση στις εγκαταστάσεις και τις πληροφορίες του.

### 11.1 Ασφαλείς Περιοχές

Η ΡΑΑΕΥ εφαρμόζει όλα τα απαραίτητα μέτρα προκείμενου να διασφαλίσει ότι οι περιοχές που περιέχουν πληροφορίες και συστήματα επεξεργασίας πληροφοριών προστατεύονται επαρκώς.

Παράλληλα λαμβάνονται κατάλληλα μέτρα έτσι ώστε να εξασφαλίζεται η φυσική προστασία της ΡΑΑΕΥ αναφορικά με όλες τις μορφές φυσικής ή προκαλούμενης από τον άνθρωπο καταστροφής (π.χ. φωτιές, πλημμύρες, εκρήξεις κ.λπ.).

### 11.2 Ασφάλεια Εξοπλισμού

Οι Διευθύνσεις / Τμήματα της ΡΑΑΕΥ καθίστανται υπεύθυνοι για την εφαρμογή μέτρων που αφορούν στη φυσική ασφάλεια των προσωπικών υπολογιστών και των πληροφοριακών αγαθών στο χώρο ευθύνης τους, συμπεριλαμβανομένων μέτρων για την αποφυγή περιστατικών κλοπής, βανδαλισμού ή καταστροφής εξοπλισμού και αποθηκευτικών μέσων.

## 12. Ασφάλεια Επιχειρησιακών Λειτουργιών

### 12.1 Λειτουργικές Διαδικασίες

Όλες οι αρμοδιότητες και διαδικασίες για τη διαχείριση και τη λειτουργία όλων των εγκαταστάσεων επεξεργασίας πληροφοριών, συμπεριλαμβανομένων των διαδικασιών απόκρισης και αντιμετώπισης περιστατικών ασφάλειας, καταγράφονται. Πρόσβαση σε κρίσιμα πληροφοριακά συστήματα και δεδομένα παρέχεται μόνο εφόσον πιστοποιείται η αντίστοιχη ανάγκη. Εφαρμόζεται καταμερισμός αρμοδιοτήτων, όπου είναι εφικτό, προς αποφυγή ή ελαχιστοποίηση των κινδύνων από σκόπιμη κακή χρήση των συστημάτων ή από αμέλεια.

Για την προστασία των λειτουργικών διαδικασιών της ΡΑΑΕΥ πρέπει να εφαρμόζονται τα παρακάτω:

**Προστασία από Κακόβουλο Λογισμικό:** Λογισμικό ανίχνευσης ιών χρησιμοποιείται σε όλους τους σταθμούς εργασίας, εξυπηρετητές και φορητούς υπολογιστές σύμφωνα με την «Πολιτική Ασφάλειας Λειτουργιών».

**Αντίγραφα Ασφάλειας:** Αντίγραφα ασφάλειας Πληροφοριών και λογισμικού λαμβάνονται σε τακτά χρονικά διαστήματα σύμφωνα με την «Πολιτική Αντιγράφων Ασφαλείας».

**Έλεγχος:** Ακολουθούνται διαδικασίες για την παρακολούθηση της χρήσης των συστημάτων της ΡΑΑΕΥ, ενώ στο μέτρο που είναι δυνατό και τεχνικά εφικτό, οι δραστηριότητες όλων των χρηστών της ΡΑΑΕΥ θα καταγράφονται και θα ελέγχονται σε τακτά χρονικά διαστήματα. Τα συστήματα καταγραφής και οι καταγεγραμμένες πληροφορίες θα προστατεύονται επαρκώς από τους κινδύνους της μη εξουσιοδοτημένης πρόσβασης και τροποποίησης ή καταστροφής τους.

**Έλεγχος Νέου Λογισμικού:** Για την ανάπτυξη και την εγκατάσταση νέων εφαρμογών, ο αρμόδιος Υπεύθυνος Έργου θα τεκμηριώνει τις απαιτήσεις ασφάλειας της ΡΑΑΕΥ και θα τις ανασκοπούν ο Υπεύθυνος Μηχανογράφησης σε συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφοριών, κατά τη διάρκεια της φάσης ανάλυσης απαιτήσεων του έργου.

**Διαχείριση Τεχνικών Ευπαθειών:** Ο Υπεύθυνος Μηχανογράφησης της ΡΑΑΕΥ πρέπει να εφαρμόζει τις ενημερώσεις ή διορθώσεις ασφάλειας έγκαιρα και σύμφωνα με όσα αναφέρονται στη «Πολιτική Ασφάλειας Λειτουργιών».

**Έλεγχος των Πληροφοριακών Συστημάτων:** Οι απαιτήσεις και διαδικασίες ελέγχου των πληροφοριακών συστημάτων πρέπει να σχεδιάζονται προσεκτικά με σκοπό να ελαχιστοποιηθεί ο κίνδυνος διατάραξης της ομαλής λειτουργίας των πληροφοριακών συστημάτων της ΡΑΑΕΥ.

## 13. Ασφάλεια Δικτύων και Επικοινωνιών

Τα δίκτυα της ΡΑΑΕΥ διαχειρίζονται και ελέγχονται, προκειμένου να εξασφαλίζεται η επαρκής προστασία από απειλές και η διατήρηση της ασφάλειας των συστημάτων, των εφαρμογών και των πληροφοριών που χρησιμοποιούν.

Η Μηχανογράφηση της ΡΑΑΕΥ διασφαλίζει την αξιοπιστία και τη λειτουργικότητα της δικτυακής υποδομής , τη δυνατότητα εύκολης πρόσβασης των χρηστών στους πληροφοριακούς πόρους και την προστασία της εμπιστευτικότητας και της ακεραιότητας των πληροφοριών της ΡΑΑΕΥ.

Όλες οι συνδέσεις δικτύων της ΡΑΑΕΥ, είτε μισθωμένες από τρίτους, είτε ιδιόκτητες, είτε δημόσιες προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, Η ΡΑΑΕΥ λαμβάνει τα κατάλληλα μέτρα για την προστασία της μετάδοσης των πληροφοριών και των μηνυμάτων της όπως ορίζεται στην «Πολιτική Ασφάλειας Δικτύων και Επικοινωνιών».

## 14. Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων

Για την ανάπτυξη και συντήρηση των Πληροφοριακών Συστημάτων της ΡΑΑΕΥ λαμβάνονται υπόψη τα παρακάτω:

**Απαιτήσεις Ασφάλειας Πληροφοριακών Συστημάτων:** Πριν από την ανάπτυξη νέων πληροφοριακών συστημάτων ή την προσθήκη νέων λειτουργιών στα υπάρχοντα, πραγματοποιείται **εκτίμηση κινδύνου** ώστε οι απαιτήσεις ασφάλειας να συμπεριλαμβάνονται στο σχεδιασμό των νέων πληροφοριακών συστημάτων.

Η ανάπτυξη των νέων πληροφοριακών συστημάτων πραγματοποιείται σε ασφαλές / δοκιμαστικό περιβάλλον που δεν επηρεάζει τα παραγωγικά συστήματα. Η συγκεκριμένη διαδικασία εφαρμόζεται σε όλο τον κύκλο ζωής ενός συστήματος.

Στις κρίσιμες εφαρμογές της ΡΑΑΕΥ ενσωματώνονται έλεγχοι επικύρωσης όπου υποστηρίζεται και είναι τεχνικά εφικτό, έτσι ώστε να είναι δυνατό να ανιχνεύονται οποιεσδήποτε ενέργειες τροποποίησης ή καταστροφής πληροφοριών που μπορεί να προκληθούν από λάθη ή σκόπιμες ενέργειες.

**Ασφάλεια στις Διαδικασίες Ανάπτυξης και Υποστήριξης:** Η ΡΑΑΕΥ εφαρμόζει μια επίσημη διαδικασία ελέγχου αλλαγών και δοκιμαστικών ελέγχων όπως ορίζεται στη «Πολιτική Ανάπτυξης και Συντήρησης Πληροφοριακών Συστημάτων». Έτσι διασφαλίζεται ότι δεν υπάρχουν επιπτώσεις στις λειτουργίες ή την ασφάλεια των συστημάτων της ΡΑΑΕΥ από αλλαγές σε νέα / υπό υλοποίηση κρίσιμα πληροφοριακά συστήματα.

**Διαχείριση Τεχνικών Ευπαθειών:** Η ΡΑΑΕΥ στο πλαίσιο ενημέρωσης από τους προμηθευτές σχετικά με τις τεχνικές ευπάθειες των πληροφοριακών του συστημάτων λαμβάνει πληροφορίες, έτσι ώστε να προβαίνει άμεσα στην αντιμετώπιση των σχετικών κινδύνων.

## 15. Διαχείριση Περιστατικών Ασφάλειας

Η ΡΑΑΕΥ εφαρμόζει αναλυτική διαδικασία (βλέπε «Διαδικασία Διαχείρισης Περιστατικών») κατά την οποία τα περιστατικά ασφάλειας καταγράφονται, κατηγοριοποιούνται με κριτήριο τις πιθανές επιπτώσεις στη λειτουργία της ΡΑΑΕΥ και θα αποφασίζεται ο κατάλληλος τρόπος αντιμετώπισής τους.

**Αναφορά Περιστατικών Ασφάλειας:** Όλοι οι υπάλληλοι, οι ανάδοχοι και τα τρίτα μέρη που χρησιμοποιούν τα πληροφοριακά συστήματα και τις υπηρεσίες της ΡΑΑΕΥ, πρέπει να αναφέρουν άμεσα στη Λειτουργία Ασφάλειας Πληροφοριών και στο Τμήμα Μηχανογράφησης, περιστατικά που αφορούν στην ασφάλεια των πληροφοριών της ΡΑΑΕΥ.

**Διαχείριση Περιστατικών Ασφάλειας και Βελτιώσεων:** Η ΡΑΑΕΥ στο πλαίσιο της διαχείρισης περιστατικών ασφάλειας εφαρμόζει κατάλληλες πολιτικές και διαδικασίες, έτσι ώστε να εξασφαλίζεται η έγκαιρη, μεθοδική και αποτελεσματική αντιμετώπιση των περιστατικών ασφαλείας.

## 16. Διαχείριση Επιχειρησιακής Συνέχειας

Στο πλαίσιο της πολιτικής ασφάλειας της ΡΑΑΕΥ τηρείται και εφαρμόζεται πολιτική και αναλυτικές διαδικασίες αναφορικά με τη δημιουργία, την εφαρμογή, την ενημέρωση και την παρακολούθηση του «Σχεδίου Επιχειρησιακής Συνέχειας», ώστε να εξασφαλίζεται η ελάχιστη δυνατή διακοπή στις λειτουργίες της ΡΑΑΕΥ σε περιπτώσεις φυσικών καταστροφών ή διακοπής της λειτουργίας σημαντικών πληροφοριακών του πόρων.

Η Λειτουργία Ασφάλειας Πληροφοριών και οι ιδιοκτήτες πληροφοριών θα εξετάζουν σε τακτά χρονικά διαστήματα την ετοιμότητα της ΡΑΑΕΥ να εφαρμόσει το Σχέδιο Επιχειρησιακής Συνέχειας. Το Σχέδιο αυτό πρέπει να εξασφαλίζει ότι οι πληροφορίες θα είναι διαθέσιμες όποτε αυτές ζητηθούν από εξουσιοδοτημένους χρήστες. Τα συστήματα αντιγράφων ασφάλειας ελέγχονται σε προκαθορισμένα διαστήματα, ούτως ώστε να ελαχιστοποιείται ο κίνδυνος αδυναμίας ανάκτησης κρίσιμων δεδομένων.

## 17. Λίστα Πολιτικών, Διαδικασιών & Φορμών

Η ΡΑΑΕΥ έχει τεκμηριώσει και διατηρεί όλες τις απαιτούμενες, από το πρότυπο ISO 27001 πολιτικές, διαδικασίες και φόρμες του ΙΣΜΣ.

Η λίστα με τις πολιτικές και διαδικασίες ασφάλειας αποτυπώνονται στους παρακάτω πίνακες.

### Πίνακας Πολιτικών

| Κωδικός | Όνομα Πολιτικής |
|---|---|

| | |
|---|---|
| ΜΑ-00 | Εγχειρίδιο Ασφάλειας Πληροφοριών |
| ΠΟ-00 | Πολιτική Ασφάλειας Πληροφοριών |
| ΠΟ-01 | Πολιτική Αποδεκτής Διαχείρισης Αγαθών |
| ΠΟ-02 | Πολιτική Διαχείρισης Αλλαγών |
| ΠΟ-03 | Πολιτική Διαβάθμισης Πληροφοριών |
| ΠΟ-04 | Πολιτική Διαχείρισης Επιχειρησιακής Συνέχειας |
| ΠΟ-05 | Πολιτική Διαχείρισης Προμηθευτών |
| ΠΟ-06 | Πολιτική Ελέγχου Πρόσβασης |
| ΠΟ-07 | Πολιτική Ανάπτυξης και Συντήρησης Πληροφοριακών Συστημάτων |
| ΠΟ-08 | Πολιτική Ασφάλειας Λειτουργιών |
| ΠΟ-09 | Πολιτική Οργάνωσης Ασφάλειας Πληροφοριών |
| ΠΟ-10 | Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας |
| ΠΟ-11 | Πολιτική Ασφάλειας Δικτύων και Επικοινωνιών |
| ΠΟ-12 | Πολιτική Αντιγράφων Ασφαλείας |
| ΠΟ-13 | Πολιτική Συμμόρφωσης |
| ΠΟ-14 | Πολιτική Υπηρεσιών Υπολογιστικού Νέφους |
| ΠΟ-15 | Πολιτική Διαχείρισης Περιστατικών Ασφάλειας |
| ΠΟ-16 | Πολιτική Κρυπτογραφίας |
| ΠΟ-17 | Πολιτική Ασφάλειας Ανθρώπινου Δυναμικού |

## Πίνακας Διαδικασιών

| Κωδικός | Όνομα Διαδικασίας |
|---|---|
| ΔΙ-1 | Διαδικασία Εκτίμησης Κινδύνου |
| ΔΙ-2 | Διαδικασία Εσωτερικού Ελέγχου |
| ΔΙ-3 | Διαδικασία Καταστροφής Μέσων Αποθήκευσης |
| ΔΙ-4 | Διαδικασία Διαχείρισης Αφαιρούμενων Μέσων Αποθήκευσης |
| ΔΙ-5 | Διαδικασία Ασφαλούς Ανάπτυξης Συστημάτων |

| | |
|---|---|
| ΔΙ-6 | Διαδικασία Λήψης Αντιγράφων Ασφάλειας |
| ΔΙ-7 | Διαδικασία Συνεχούς Βελτίωσης και Στόχων |
| ΔΙ-8 | Διαδικασία Λειτουργίας Διαχείρισης Συστημάτων |
| ΔΙ-9 | Διαδικασία Μεταφοράς Πληροφοριακού Εξοπλισμού |
| ΔΙ-10 | Εκπαιδευτικό Υλικό |
| ΔΙ-11 | Δοκιμές Παρείσδυσης |
| ΔΙ-12 | Σχέδιο Επιχειρησιακής Συνέχειας (BCP) |
| ΔΙ-13 | Διαδικασία Διορθωτικών και Προληπτικών Ενεργειών |
| ΔΙ-14 | Διαδικασία Ελέγχου Εγγράφων |
| ΔΙ-15 | Διαδικασία Ελέγχου Αρχείων |
| ΔΙ-16 | Διαδικασία Διαχείρισης Περιστατικών |
| ΔΙ-17 | Διαδικασία Ανασκόπησης Διοίκησης |
| ΔΙ-18 | Διαδικασία Διαχείρισης Αλλαγών |
| ΔΙ-19 | Διαδικασία Πρόσβασης Χρηστών |
| ΔΙ-20 | Πειθαρχική Διαδικασία |
| ΔΙ-21 | Διαδικασία για την Πληροφόρηση Απειλών (Threat Intelligence) |
| ΔΙ-22 | Διαδικασία Επιτήρησης Φυσικής Ασφάλειας |
| ΔΙ-23 | Διαδικασία Διαχείρισης Ασφαλών Παραμετροποιήσεων |
| ΔΙ-24 | Διαδικασία Διαγραφής Πληροφοριών |
| ΔΙ-25 | Διαδικασία Ψευδωνυμοποίησης και Απόκρυψης Δεδομένων |
| ΔΙ-26 | Διαδικασία Αποτροπής Διαρροής Πληροφοριών |
| ΔΙ-27 | Διαδικασία Επίβλεψης Δραστηριοτήτων |
| ΔΙ-28 | Διαδικασία Προστασίας Διαδικτυακής Πρόσβασης |
| ΔΙ-29 | Διαδικασία Ασφάλειας Υπολογιστικού Νέφους |
| ΔΙ-30 | Διαδικασία Ελέγχου Πρόσβασης |
| ΔΙ-31 | Διαδικασία Κρυπτογραφίας |
| ΔΙ-32 | Διαδικασία Διαχείρισης Προμηθευτών και Τρίτων Μερών |

## Πίνακας φορμών και λοιπών αρχείων

| Κωδικός | Όνομα Φόρμας / Σχέδιου / Αρχείου |
|---|---|
| ΔΓ-2-1 | Διάγραμμα Μέθοδος Διεξαγωγής Εσωτερικών Ελέγχων |
| ΕΚ-2-1 | Έκθεση Εσωτερικού Ελέγχου |
| ΛΙ-2-1 | Λίστα Ελέγχου Εσωτερικού Ελέγχου |
| ΠΛ-2-1 | Πλάνο Εσωτερικών Ελέγχων |
| ΑΡ-3-1 | Αρχείο Καταγραφής Μέσων Αποθήκευσης προς καταστροφή |
| ΔΓ-3-1 | Διάγραμμα Διαδικασία Καταστροφής Μέσων Αποθήκευσης |
| ΦΟ-4-1 | Φόρμα Αίτησης Χρήσης Αφαιρούμενου Μέσου |
| ΔΓ-5-1 | Διάγραμμα Διαδικασία Ασφαλούς Ανάπτυξης Συστημάτων |
| ΔΓ-6-1 | Διάγραμμα Διαδικασία Λήψης Αντιγράφων Ασφάλειας |
| ΑΡ-7-1 | Καταγραφή ΜΣ |
| ΑΡ-7-2 | Στόχοι Ασφάλειας |
| ΑΡ-7-3 | Εσωτερική Επιθεώρηση (12/6/2023) |
| ΕΚ-7-1 | Εσωτερική Επιθεώρηση (2024) |
| ΕΚ-7-2 | Εσωτερική Επιθεώρηση (2025) |
| ΠΡ-7-1 | Πρακτικά Συμβουλίου |
| ΑΡ-10-1 | Training - Security Management ISO 27001 |
| ΑΡ-10-2 | Training - Security Policies ISO 27001 |
| ΑΡ-10-3 | Training - Security Procedures ISO 27001 |
| ΑΡ-10-4 | Εκπαίδευση Υπευθύνου ΣΔΑΠ, Ομάδας Ασφάλειας & εμπλεκόμενων |
| ΑΡ-11-1 | RAE Internal ptrpt |
| ΑΡ-11-2 | RAE External ptrpt |
| ΑΡ-11-3 | server ip |
| ΑΡ-12-1 | Διαδικασία χειρισμού συμβάντων |
| ΑΡ-12-2 | Αποκατάσταση των λειτουργιών |
| ΑΡ-12-3 | Ενημερώσεις εντός εργάσιμων ωρών |
| ΑΡ-12-4 | Ενημερώσεις σε μη εργάσιμες ώρες |
| ΑΡ-12-5 | Διασφάλιση ακεραιότητας συναλλαγών και εγγράφων |
| ΣΧ-12-1 | Σχέδιο Επιχειρησιακής Συνέχειας |
| ΣΧ-12-2 | Σχέδιο επανεκκίνησης |

| | |
|---|---|
| ΦΟ-13-1 | Φόρμα Διορθωτικών Προληπτικών Ενεργειών |
| ΑΡ-14-1 | Αρχείο Ελεγχόμενων Εγγράφων ΣΔΑΠ |
| ΔΓ-14-1 | Διάγραμμα Αλλαγής Εγγράφων |
| ΔΓ-14-2 | Διάγραμμα Μέθοδος ελέγχων του ΣΔΑΠ |
| ΔΓ-14-3 | Διάγραμμα Δημιουργίας Εγγράφων |
| ΦΟ-14-1 | Φόρμα Αίτησης Αλλαγών Εγγράφου |
| ΔΓ-15-1 | Διάγραμμα Διαδικασία Ελέγχου Αρχείων |
| ΑΡ-16-1 | Αρχείο Περιστατικών Αδυναμιών Ασφάλειας Πληροφοριών |
| ΔΓ-16-1 | Διάγραμμα Διαδικασία Διαχείρισης Περιστατικών |
| ΦΟ-16-1 | Φόρμα Αναφοράς Περιστατικού Αδυναμίας Ασφάλειας |
| ΦΟ-16-2 | Φόρμα Καταγραφής Περιστατικών Αδυναμιών Ασφάλειας |
| ΔΓ-17-1 | Διάγραμμα Διαδικασία Ανασκόπησης Διοίκησης |
| ΠΡ-17-1 | Πρακτικό Συνεδρίασης Ανασκόπησης Διοίκησης |
| ΣΧ-17-1 | Σχέδιο Δράσης |
| ΦΟ-17-1 | Φόρμα Πρακτικών Συνεδριάσεων Ανασκόπησης Διοίκησης |
| ΑΡ-18-1 | Αρχείο Αιτημάτων Αλλαγών |
| ΔΓ-18-1 | Διάγραμμα Διαδικασία Διαχείρισης Αλλαγών |
| ΦΟ-18-1 | Φόρμα Αίτησης Αλλαγών |
| ΦΟ-18-2 | Φόρμα Αίτησης Αλλαγών Business Cards |
| ΦΟ-18-3 | Φόρμα Αίτησης Αλλαγών Conference System |
| ΦΟ-18-4 | Φόρμα Αίτησης Αλλαγών HRNET |
| ΦΟ-18-5 | Φόρμα Αίτησης προμήθειας laptop |
| ΦΟ-18-6 | Φόρμα Αίτησης Αλλαγών Printers |
| ΦΟ-18-7 | Φόρμα Αίτησης Αλλαγών IP τηλ. συσκευών |
| ΑΡ-19-1 | Διαδικασία αξιολόγησης φορητών ιδιωτικών συσκευών |
| ΔΓ-19-1 | Διάγραμμα Ανασκόπηση Δικαιωμάτων Πρόσβασης |
| ΔΓ-19-2 | Διάγραμμα Τροποποίηση Δικαιωμάτων Πρόσβασης |
| ΔΓ-19-3 | Διάγραμμα Εγγραφή Χρήστη |
| ΔΓ-19-4 | Διάγραμμα Διαγραφή Λογαριασμού Χρήστη |
| ΔΓ-19-5 | Διάγραμμα Αρχικοποίηση Κωδικού Πρόσβασης |
| ΔΓ-20-1 | Διάγραμμα Πειθαρχική Διαδικασία |
| ΑΡ-30-1 | Αρχείο Χρέωσης Αγαθών εκτός ΡΑΑΕΥ |
| ΑΡ-30-2 | Αρχείο αιτήσεων υπηρεσιών |
| ΑΡ-30-3 | Αρχείο Δικαιωμάτων Πρόσβασης |
| ΑΡ-30-4 | Μητρώο server ip (asset registry) 2026 |

| | |
|---|---|
| ΑΡ-30-5 | Asset registry ΡΑΑΕΥ 2026 |
| ΦΟ-30-1 | Φόρμα Δικαιωμάτων Πρόσβασης |
| ΦΟ-30-2 | Φόρμα Χρέωσης Αγαθών |
| ΦΟ-30-3 | Φόρμα Χρέωσης Αγαθών εκτός ΡΑΑΕΥ |
| ΦΟ-30-4 | Φόρμα Αίτησης Υπηρεσίας |
| ΑΡ-32 | ΜΗΤΡΩΟ ΑΝΑΔΟΧΩΝ-ΠΡΟΜΗΘΕΥΤΩΝ -2020-2026 |