Όνομα Οργανισμού

Πολιτική Ελέγχου Πρόσβασης

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Ελέγχου Πρόσβασης |
| **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](#_Toc158631136)

[2. Πολιτική Ελέγχου Πρόσβασης 4](#_Toc158631137)

[3. Έλεγχος Πρόσβασης 4](#_Toc158631138)

[4. Έλεγχος Πρόσβασης σε Πόρους του [Όνομα Οργανισμού] 5](#_Toc158631139)

[5. Διαχείριση Ταυτότητας και Πρόσβασης Βάσει Ρόλου 6](#_Toc158631140)

[6. Παρακολούθηση και Καταγραφή Ενεργειών (logs) 7](#_Toc158631141)

[7. Έλεγχος Πρόσβασης Δικτύου 8](#_Toc158631142)

[8. Έλεγχος Πρόσβασης Εφαρμογών και Συστημάτων 9](#_Toc158631143)

[9. Έλεγχος Πρόσβασης σε Κτίρια 9](#_Toc158631144)

[10. Διακριτικά Χρηστών 9](#_Toc158631145)

[11. Διαχείριση Κωδικών 11](#_Toc158631146)

[11.1. Κωδικοί Πρόσβασης 12](#_Toc158631147)

[11.2. Βέλτιστες τεχνικές και πρακτικές προστασίας κωδικών 14](#_Toc158631148)

[12. Εξουσιοδότηση Χρηστών 15](#_Toc158631149)

[13. Προνομιακά Δικαιώματα Χρηστών 16](#_Toc158631150)

[14. Λογαριασμοί με αυξημένα δικαιώματα πρόσβασης 17](#_Toc158631151)

[15. Λογαριασμοί εκτός Οργανισμού 17](#_Toc158631152)

[16. Εξωτερική Πρόσβαση σε Πόρους του [Όνομα Οργανισμού] 17](#_Toc158631153)

[17. Απομακρυσμένη Πρόσβαση 18](#_Toc158631154)

[18. Συνδέσεις Τρίτων Μερών 20](#_Toc158631155)

# Σκοπός

Σκοπός της Πολιτικής Ελέγχου Πρόσβασης είναι να καθορίσει τις κατευθυντήριες γραμμές και τεχνικές προκειμένου να διασφαλίζεται η ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών του [Όνομα Οργανισμού] και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση.

# Πολιτική Ελέγχου Πρόσβασης

Σύμφωνα με τον Κανονισμό Κ.Δ.Π. 389/2020 όσον αφορά την καταγραφή των στοιχείων ενεργειακού και την ιδιοκτησία, ο [Όνομα Οργανισμού] οφείλει να διασφαλίσει ότι τα στοιχεία ενεργητικού καταγράφονται σε κατάλογο και ότι η ιδιοκτησία καθορίζεται με σκοπό την επίτευξη της ιχνηλασιμότητας και της ευθύνης για τα στοιχεία, προκειμένου να διασφαλίσει ότι ο οργανισμός έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες) που διατηρεί. . Ο κατάλογος θα πρέπει να προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών και να επιτρέπει στον οργανισμό να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία θα πρέπει να εφαρμόζει και να διατηρεί μέτρα ασφάλειας πληροφοριών.

# Έλεγχος Πρόσβασης

Όλα τα πληροφοριακά συστήματα του [Όνομα Οργανισμού] πρέπει να προστατεύονται με μηχανισμούς «ελέγχου πρόσβασης». Οι εν λόγω μηχανισμοί πρέπει να συμμορφώνονται με τις βασικές αρχές ασφαλούς πρόσβασης (Αυθεντικοποίηση , Εξουσιοδότηση, Καταγραφή). Επιπρόσθετα, όπου είναι εφικτό πρέπει να χρησιμοποιείται τεχνολογία SSO (Single Sign-On).

Ο [Όνομα Οργανισμού] να θέσπιση, εφαρμογή και διατήρηση καταλόγου καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίσει ότι ο οργανισμός έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες, πόρους, δίκτυα και κτίρια) που διατηρεί. Ο κατάλογος θα πρέπει να προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών. Ο κατάλογος θα πρέπει επίσης να επιτρέπει στον οργανισμό να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία θα πρέπει να εφαρμόζει και να διατηρεί μέτρα ασφάλειας πληροφοριών. Πρέπει να γίνεται παρακολούθηση και καταγραφή ενεργειών (logs). Η έκταση της παρακολούθησης και καταγραφής ενεργειών προκύπτει από τα αποτελέσματα σχετικής ανάλυσης διακινδύνευσης που διενεργείται με ευθύνη των ιδιοκτητών πόρων. Τα βασικά χαρακτηριστικά που καθορίζονται είναι: είδος καταγραφής, χρονικό διάστημα διατήρησης, μέσο διατήρησης. Καταγραφή ενεργειών που σχετίζονται με την ασφάλεια είναι ενεργοποιημένη κατ΄ελάχιστο στα κρίσιμα συστήματα. Καταγραφή ενεργειών που σχετίζονται με την ασφάλεια πρέπει να είναι ενεργοποιημένη σε όλα τα συστήματα.

Ο [Όνομα Οργανισμού], πρέπει να παρέχει πρόσβαση στο προσωπικό του, καθώς και ενδέχεται να παρέχει πρόσβαση στους προμηθευτές του, και σε τρίτους που δραστηριοποιούνται εκ μέρους του. Νοείται ότι η πρόσβαση θα πρέπει να παρέχεται μόνο όπου είναι αναγκαία προκειμένου οι πιο πάνω χρήστες να μπορούν να διεκπεραιώσουν τις εργασίες τους.

Ο [Όνομα Οργανισμού] να θεσπίσει, εφαρμόζει και διατηρεί μέτρα διαχείρισης ταυτότητας και πρόσβασης τα οποία εξετάζουν μέτρα πρόσβασης με βάση το ρόλο, με σκοπό 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 θα πρέπει να διασφαλίζει ότι χορηγούνται επαρκείς άδειες σε χρήστες με βάση τις αρμοδιότητες τους που συνδέονται με αντίστοιχους ρόλους. Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να γίνεται σύμφωνα με τις διαδικασίες ασφάλειας των ανθρώπινων πόρων, όπως ορίζεται στο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης είναι ευθυγραμμισμένοι με τους ρόλους και αρμοδιότητες των στελεχών στο πλαίσιο του οργανισμού.

Βασικές αρχές ασφαλούς πρόσβασης:

* **Αυθεντικοποίηση (Authentication):** Η αυθεντικοποίηση είναι η διαδικασία με την οποία ένα πληροφοριακό σύστημα αναγνωρίζει/προσδιορίζει τον αιτητή που αιτείται πρόσβαση σε ένα σύστημα. Ο χρήστης θα πρέπει να αποδείξει ποιος είναι. Στην συνέχεια ο χρήστης παρέχει τα διακριτικά του.
* **Εξουσιοδότηση (Authorization):** Εφόσον τα διακριτικά είναι έγκυρα, το πληροφορικό σύστημα εξουσιοδοτεί το χρήστη με τα ανάλογα δικαιώματα πρόσβασης.
* **Καταγραφή (Accounting/Accountability):** Όλες οι προσβάσεις / εξουσιοδοτήσεις καταγράφονται προκειμένου να υπάρχει ιστορικό για μελλοντική χρήση.

# Έλεγχος Πρόσβασης σε Πόρους του [Όνομα Οργανισμού]

Ο σκοπός της πολιτικής ελέγχου πρόσβασης είναι να διασφαλίσει την ασφαλή πρόσβαση σε πόρους του οργανισμού, περιορίζοντας την πρόσβαση μόνο σε εξουσιοδοτημένα άτομα και ελέγχοντας τη χρήση των πόρων.

**Κατηγορίες Πόρων:**

1. Ηλεκτρονικοί Πόροι:

* Πληροφοριακά Συστήματα.
* Εφαρμογές Λογισμικού.
* Βάσεις Δεδομένων.
* Δικτυακή Υποδομή.

1. Φυσικοί Πόροι:

* Κτίρια και Γραφεία.
* Εξοπλισμός και Υλικά.

Η πολιτική ελέγχου πρόσβασης είναι ένα εκτενές πλαίσιο και πρέπει να προσαρμόζεται συνεχώς για να αντιμετωπίζει νέες προκλήσεις και απειλές. Παρακάτω περιγράφονται κάποιες ευθύνες και διαδικασίες που οφείλει να εφαρμόζει ο [Όνομα Οργανισμού] έτσι ώστε να επιτύχει τον στόχο που καθορίσει η παραπάνω πολιτική.

1. Διαχείριση Πρόσβασης:

* Καθορισμός και διαχείριση των δικαιωμάτων πρόσβασης.
* Κατανομή ρόλων για την αποφυγή παραβιάσεων.

1. Αυθεντικοποίηση:

* Χρήση ασφαλών μεθόδων αυθεντικοποίησης, όπως κωδικοί πρόσβασης, δυναμικά τοκετά και βιομετρικά στοιχεία.

1. Εκχώρηση Δικαιωμάτων:

* Ορισμός δικαιωμάτων πρόσβασης βάσει του ρόλου και της ανάγκης.
* Αναθεώρηση περιοδικών δικαιωμάτων πρόσβασης.
* Ενημέρωση με βάση τις αλλαγές στα καθήκοντα.

1. Πολιτικές Πρόσβασης σε Ευαίσθητα Δεδομένα:

• Εφαρμογή ειδικών πολιτικών για την πρόσβαση σε ευαίσθητα δεδομένα, προστατεύοντας την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών.

1. Καταγραφή Πρόσβασης:

* Πλήρης καταγραφή πρόσβασης για επαλήθευση και ανίχνευση ανωμαλιών.

1. Αντιμετώπιση Παραβάσεων:

* Προσδιορισμός διαδικασίας για την αντιμετώπιση παραβάσεων και πειθαρχικών μέτρων.

1. Παρακολούθηση και Ανίχνευση:

* Αυτόματη παρακολούθηση δραστηριοτήτων και ανίχνευση ασυνήθιστων προτύπων.

1. Εκπαίδευση και Ευαισθητοποίηση:

* Εκπαίδευση του προσωπικού για την ασφαλή χρήση πόρων.
* Ευαισθητοποίηση για τις απειλές ασφαλείας.

1. Αναθεώρηση Πολιτικής:

* Περιοδική αναθεώρηση της πολιτικής για αντιστοίχηση με τις εξελίξεις της τεχνολογίας και τις ανάγκες του οργανισμού.

# Διαχείριση Ταυτότητας και Πρόσβασης Βάσει Ρόλου

Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να γίνεται σύμφωνα με τις διαδικασίες ασφάλειας των ανθρώπινων πόρων, όπως ορίζεται στο [HRS1] του Νόμου Κ.Δ.Π. 389/2020, προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης είναι ευθυγραμμισμένοι με τους ρόλους και αρμοδιότητες των στελεχών στο πλαίσιο του οργανισμού.

Ο [Όνομα Οργανισμού] θα πρέπει να καταρτήσει επαρκή μέτρα για την εξασφάλιση ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, τα οποία έχουν πρόσβαση σε οργανωτικούς πόρους, υποστηρίζουν την πολιτική ασφάλειας πληροφοριών και τους στόχους του [Όνομα Οργανισμού]. Επίσης δημιουργεί σχέδιο για να διασφαλιστεί ότι η ασφάλεια πληροφοριών είναι ενσωματωμένη καθ’ όλη τη διάρκεια του κύκλου ζωής της εργοδότησης (δηλαδή πριν, κατά τη διάρκεια και μετά την εργοδότηση των εργαζομένων) και να καταβάλει κάθε εύλογη προσπάθεια προκειμένου να διασφαλίσει ότι οι εργαζόμενοι κατανοούν τις ευθύνες τους σε σχέση με την ασφάλεια πληροφοριών. Το σχέδιο περιλαμβάνει κατάλληλα μέτρα ασφάλειας πληροφοριών σε κάθε φάση της εργοδότησης, π.χ. έλεγχοι ιστορικού πριν την πρόσληψη, κατάρτιση και ευαισθητοποίηση των εργαζομένων, ενσωμάτωση επαρκών προνοιών στις συμβάσεις εργασίας, κατάρτιση πολιτικής αποδεκτής χρήσης, επιστροφή των συσκευών των εργαζομένων που περιέχουν κρίσιμες πληροφορίες, και αφαίρεση της πρόσβασης σε συστήματα και εφαρμογές.

Παρακάτω αναφέρονται ορισμένες διαδικασίες διαχείρισης ταυτότητας και πρόσβασης, προκειμένου να δοθούν τα τεχνικά και οργανωτικά μέσα για την επιβολή της αρχής του ελάχιστου προνομίου και της διαχείρισης των προνομιούχων χρηστών.

1. Καθορισμός Ρόλων:

• Κάθε χρήστης θα αντιστοιχεί σε συγκεκριμένο ρόλο βάσει των εργασιακών του καθηκόντων.

1. Ανάθεση Δικαιωμάτων βάσει Ρόλου:

• Καθορισμός επαρκών δικαιωμάτων πρόσβασης σε κάθε χρήστη βάσει του ρόλου του, εξασφαλίζοντας την αρχή του ελάχιστου προνομίου.

1. Επαλήθευση Ταυτότητας:

• Χρήση αποτελεσματικών μεθόδων επαλήθευσης ταυτότητας για να εξασφαλιστεί ότι ο κάθε χρήστης συνδέεται σωστά με τον αντίστοιχο ρόλο του.

1. Αναθεώρηση Κανονισμών Πρόσβασης:

• Περιοδική αναθεώρηση των κανόνων πρόσβασης και ενημέρωση ανάλογα με τις αλλαγές στα καθήκοντα και τις ευθύνες των χρηστών.

1. Εκπαίδευση Προσωπικού:

• Εκπαίδευση του προσωπικού σχετικά με τη σημασία της αρχής του ελάχιστου προνομίου και της ορθής χρήσης των δικαιωμάτων πρόσβασης.

1. Παρακολούθηση Δραστηριότητας:

• Σύστημα παρακολούθησης για την επαλήθευση της συμμόρφωσης με τους κανόνες πρόσβασης.

1. Ενσωμάτωση με Διαδικασίες Ασφάλειας Ανθρώπινων Πόρων:

• Συνεργασία με τις διαδικασίες ασφάλειας των ανθρώπινων πόρων για να διασφαλιστεί η αρμονία των ρόλων πρόσβασης με τις επαγγελματικές αρμοδιότητες.

# Παρακολούθηση και Καταγραφή Ενεργειών (logs)

Παρακάτω γίνεται αναφορά στα κριτήρια και τις διαδικασίες παρακολούθησης και καταγραφής ενεργειών (logs) σε σχέση με την ασφάλεια των πληροφοριακών συστημάτων. Ο σκοπός είναι να διασφαλιστεί η ενεργή προστασία των κρίσιμων πληροφοριακών πόρων του [Όνομα Οργανισμού].

1. Είδος Καταγραφής:

• Ορισμός του είδους των ενεργειών που θα καταγράφονται, περιλαμβάνοντας αλλά μη περιοριζόμενο σε προσπάθειες πρόσβασης, αλλαγές στη δομή δεδομένων, και προσπάθειες ανάλυσης διακινδύνευσης.

1. Χρονικό Διάστημα Διατήρησης:

• Καθορισμός του χρονικού διαστήματος για τη διατήρηση των logs, λαμβάνοντας υπόψη τις νομικές απαιτήσεις και τις ανάγκες ανάκτησης δεδομένων.

1. Μέσο Διατήρησης:

• Καθορισμός του μέσου αποθήκευσης για τα logs, με έμφαση στην ασφάλεια και την αποτελεσματική ανάκτηση πληροφοριών.

1. Ενεργοποίηση σε Κρίσιμα Συστήματα:

• Εξασφάλιση πως η καταγραφή ενεργειών είναι ενεργοποιημένη σε όλα τα κρίσιμα πληροφοριακά συστήματα, ώστε να διασφαλίζεται η ενεργή παρακολούθηση.

1. Ενεργοποίηση σε Όλα τα Συστήματα:

• Η καταγραφή ενεργειών που σχετίζονται με την ασφάλεια πρέπει να είναι ενεργοποιημένη σε όλα τα συστήματα, προκειμένου να διατηρείται ολοκληρωμένη επισκόπηση των δραστηριοτήτων.

1. Ανάλυση Διακινδύνευσης:

• Πραγματοποίηση ανάλυσης διακινδύνευσης για την προσδιορισμό των ενεργειών που απαιτούν ειδική παρακολούθηση.

# Έλεγχος Πρόσβασης Δικτύου

1. Όλες οι απομακρυσμένες συνδέσεις για συντήρηση, υποστήριξη κλπ., θα πρέπει να ασφαλίζονται και να ελέγχονται. Οι συνδέσεις θα πρέπει να απενεργοποιούνται μετά την χρήση τους.
2. Όλες οι απομακρυσμένες προσβάσεις θα πρέπει να αυθεντικοποιούνται με σύστημα αυθεντικοποίησης δύο παραγόντων.
3. Όλα τα εξωτερικά αιτήματα για πρόσβαση στα συστήματα, δίκτυα ή εφαρμογές του Οργανισμού θα πρέπει να εγκρίνονται από τον Υπεύθυνο Ασφάλειας Πληροφοριών και τον Διευθυντή Πληροφορικής.
4. Όλοι οι χρήστες που έχουν απομακρυσμένη πρόσβαση στα συστήματα, δίκτυα ή εφαρμογές του Οργανισμού (π.χ. μέσω σύνδεσης VPN) θα πρέπει να συμμορφώνονται με όλες τις ενότητες των Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων και θα πρέπει να τους παρέχεται πρόσβαση μέσω αυθεντικοποίησης δύο παραγόντων.
5. Τα ασύρματα δίκτυα θα πρέπει να εγκρίνονται, αυθεντικοποιούνται, κρυπτογραφούνται και επιτρέπονται μόνο σε εγκεκριμένες τοποθεσίες.
6. Το περιβάλλον παραγωγής θα πρέπει να διαχωρίζεται από το περιβάλλον δοκιμής, χρησιμοποιώντας κατάλληλο μηχανισμούς διαχωρισμού με τη χρήση τείχους προστασίας (firewall segmentation).
7. Η σύνδεση/ πρόσβαση μεταξύ τμημάτων διαχωρισμένων δικτύων, θα πρέπει να ελέγχεται κατάλληλα.
8. Η πρόσβαση σε κοινόχρηστους φακέλους, θα εξουσιοδοτείται μόνο σε περιοσμένους χρήστες, για συγκεκριμένους επιχειρησιακούς σκοπούς.
9. Για την υποστήριξη της ακεραιότητας των αρχείων καταγραφής, θα πρέπει να συγχρονίζεται το ρολόι δικτύου με όλες τις συσκευές του δικτύου, συσκευές ασφάλειας, τους σταθερούς υπολογιστές (desktops) και τους διακομιστές.
10. Όλα τα δικαιώματα πρόσβασης στο δίκτυο θα αναθεωρούνται περιοδικά (π.χ. κάθε έξι (6) μήνες).
11. Θα υπάρχουν και θα συντηρούνται αρχεία καταγραφής πρόσβασης χρηστών.

# Έλεγχος Πρόσβασης Εφαρμογών και Συστημάτων

1. Η πρόσβαση σε πηγαίο κώδικα προγράμματος και παρεμφερή αγαθά, θα πρέπει να ελέγχεται αυστηρά.
2. Η πρόσβαση σε εφαρμογές θα αντικατοπτρίζει τις απαιτήσεις κάθε επιχειρησιακής εφαρμογής και δεν θα πρέπει να αντικρούεται με τα προκαθορισμένα δικαιώματα πρόσβασης του χρήστη.
3. Τα δικαιώματα πρόσβασης χρήστη θα πρέπει να ελέγχονται π.χ. Ανάγνωση, Εγγραφή, Διαγραφή και Εκτέλεση.
4. Θα υπάρχουν και θα συντηρούνται αρχεία καταγραφής πρόσβασης χρηστών.

# Έλεγχος Πρόσβασης σε Κτίρια

1. Διαχείριση Πρόσβασης:

* Καθορισμός και διαχείριση των εξουσιοδοτήσεων πρόσβασης.
* Κατανομή ρόλων για την καλύτερη διαχείριση.

1. Αυθεντικοποίηση:

* Χρήση ασφαλών μεθόδων αυθεντικοποίησης, όπως κάρτες πρόσβασης, κωδικοί ή βιομετρικά στοιχεία.

1. Φυσική Ασφάλεια:

* Έλεγχος πρόσβασης σε εισόδους και ευαίσθητες περιοχές.
* Χρήση συστημάτων κλειδώματος και ασφαλείας.

1. Παρακολούθηση Πρόσβασης:

* Καταγραφή χρηστών που εισέρχονται και εξέρχονται από τα κτίρια.
* Συνεχείς ελέγχοι παραβίασης πολιτικής πρόσβασης.

1. Διαχείριση Κινδύνων:

* Αξιολόγηση και διαχείριση κινδύνων που σχετίζονται με την πρόσβαση.
* Εφαρμογή μέτρων για τη μείωση κινδύνων.

# Διακριτικά Χρηστών

Προκειμένου να επιτυγχάνεται η αυθεντικοποίηση των χρηστών στα πληροφορικά συστήματα, ο [Όνομα Οργανισμού] πρέπει να παρέχει διακριτικά στους χρήστες. Υπάρχουν τριών ειδών διακριτικά, «κάτι που έχει», «κάτι που είναι», «κάτι που γνωρίζει» ο χρήστης. Για παράδειγμα μπορεί να είναι usernames/passwords, κάρτες πρόσβασης, έξυπνες κάρτες, security tokens, βιομετρικά στοιχεία, PINs κλπ., ή και συνδυασμός.

* Τα διακριτικά κάθε χρήστη πρέπει να είναι μοναδικά, προκειμένου να επιτυγχάνεται η μη αποποίηση της ευθύνης.
* Τα μη ονομαστικά διακριτικά απαγορεύονται. Για παράδειγμα το κάθε διακριτικό πρέπει να ταυτίζεται μόνο με ένα συγκεκριμένο φυσικό πρόσωπο/χρήστη. Όταν αυτό δεν είναι εφικτό, τα πληροφοριακά συστήματα πρέπει να υποστηρίζονται με λογισμικό το οποίο έχει την δυνατότητα της εξακρίβωσης της ταυτότητας του χρήστη που χρησιμοποιεί τον μη ονομαστικό λογαριασμό. Για παράδειγμα (Observe IT, CyberArk, Microsoft PAM) .
* Η δημιουργία και η χρησιμοποίηση κοινών λογαριασμών σε πληροφοριακά συστήματα απαγορεύεται. Όταν αυτό δεν είναι εφικτό, τα πληροφοριακά συστήματα πρέπει να υποστηρίζονται με λογισμικό το οποίο έχει την δυνατότητα της εξακρίβωσης της ταυτότητας του χρήστη που χρησιμοποιεί τον κοινό λογαριασμό. Για παράδειγμα (Observe IT, CyberArk, Microsoft PAM).
  + Νοείται ότι κατά την αποχώρηση / μετακίνηση ενός από τους χρήστες του κοινού λογαριασμού, ο κωδικός πρόσβασης πρέπει άμεσα να αλλάζει.
* Πρέπει να τηρείται αρχείο όλων των διακριτικών των χρηστών. Το εν λόγω αρχείο θα πρέπει να είναι κρυπτογραφημένο και να περιλαμβάνει τουλάχιστον τα ακόλουθα:
  + την αντιστοιχία χρήστη / διακριτικού.
  + το πρόσωπο που το ενέκρινε.
  + την ημερομηνία της δημιουργίας του διακριτικού.
  + τα δικαιώματα πρόσβασης του κάθε διακριτικού
  + κατά πόσο το διακριτικό βρίσκεται σε ισχύ.
* Σε συστήματα που η αυθεντικοποίηση επιτυγχάνεται με το username/password, πρέπει να συμμορφώνονται σύμφωνα με την παρούσα Πολιτική.
* Σε συστήματα που η αυθεντικοποίηση επιτυγχάνεται με το username/password, σε περιπτώσεις όπου οποιοδήποτε από τα πεδία (username/ password) είναι λανθασμένο, το σύστημα δεν πρέπει να ενημερώνει τον χρήστη σε πιο πεδίο υπάρχει λάθος.
* Σε περιπτώσεις όπου συμβαίνουν επαναλαμβανόμενες αποτυχημένες προσπάθειες πρόσβασης ο λογαριασμός του χρήστη πρέπει να κλειδώνεται ή να αναστέλλεται ή να απενεργοποιείται.
* Σε κρίσιμα συστήματα ή σε συστήματα που περιέχουν κρίσιμα δεδομένα ή σε συστήματα που είναι προσβάσιμα από το διαδίκτυο πρέπει να χρησιμοποιείται συνδυασμός διακριτικών, πιστοποίηση διπλής συνιστώσας και ισχυρής ταυτοποίησης. Το ίδιο θα πρέπει να ισχύει και για τις περιπτώσεις απομακρυσμένης πρόσβασης.
* Η αυθεντικοποίηση στα συστήματα του [Όνομα Οργανισμού] δεν πρέπει να είναι εφικτή σε μη εργάσιμες ώρες και αργίες. Για παράδειγμα, η πρόσβαση στις εγκαταστάσεις του [Όνομα Οργανισμού] σε μη εργάσιμες ώρες, θα πρέπει να απαγορεύεται. Επιπρόσθετα η αυθεντικοποίηση στα συστήματα του [Όνομα Οργανισμού] δεν θα πρέπει να επιτυγχάνεται από χρήστες οι οποίοι απουσιάζουν με άδεια. Για παράδειγμα οι λογαριασμοί των χρηστών πρέπει να είναι απενεργοποιημένοι. Αυτό γίνεται για μείωση κακόβουλων δραστηριοτήτων στα συστήματα / κτήρια του [Όνομα Οργανισμού] σε περίπτωση που τα διακριτικά ενός εργαζομένου κλαπούν. Με αυτό τον τρόπο, η πρόσβαση στα συστήματα / κτήρια του οργανισμού παρέχεται μόνο με την παρουσία και την αυθεντικοποίηση του εργαζομένου. Σημειώνεται ότι κάποιες εξαιρέσεις μπορεί να υπάρχουν, οι οποίες θα πρέπει να εγκρίνονται από τον εκάστοτε ιδιοκτήτη του συστήματος. Νοείται ότι όλες οι εξαιρέσεις θα πρέπει να καταγράφονται σε σχετικό μητρώο.

# Διαχείριση Κωδικών

H σωστή στρατηγική για τη δημιουργία, και διαχείριση κωδικών πρόσβασης μειώνει σημαντικά τον κίνδυνο σπασίματος, υποκλοπής, υπολογισμού κωδικών ούτως ώστε η μη εξουσιοδοτημένη πρόσβαση να αποτρέπεται.

* Όλα τα πληροφοριακά συστήματα πρέπει να προστατεύονται με κωδικό πρόσβασης.
  + Περαιτέρω, όλα τα κρίσιμα πληροφορικά συστήματα ή συστήματα που είναι προσβάσιμα από το διαδίκτυο (Internet Facing Application) ή συστήματα που υποστηρίζουν απομακρυσμένη πρόσβαση πρέπει να υποστηρίζονται με πιστοποίηση διπλής συνιστώσας (Multifactor Authentication) και Ισχυρής Αυθεντικοποίησης (strong authentication).
* Οι προκαθορισμένοι / εξ ορισμού (default) κωδικοί πρόσβασης των συστημάτων πρέπει να αλλάζουν (συμπεριλαμβανομένων και των κωδικών που προεπιλέγονται από τον κατασκευαστή ή/και τον προμηθευτή των συστημάτων).
  + Σε όλα τα λειτουργικά συστήματα οι τοπικοί προκαθορισμένοι λογαριασμοί όπως «administrator», «root», «guest», «default», πρέπει να μετονομάζονται. Σε περίπτωση που προκαθορισμένος λογαριασμός δεν μπορεί να απενεργοποιηθεί πρέπει να μετονομαστεί.
  + Στα λειτουργικά συστήματα Microsoft Windows, ο τοπικός λογαριασμός διαχειριστή, πρέπει να μετονομάζεται. Επιπρόσθετα, οι κωδικοί των εν λόγω λογαριασμών πρέπει να τυγχάνουν διαχείρισης (αλλάζονται σύμφωνα με την παρόν Πολιτική) και νοείται ότι οι εν λόγω λογαριασμοί πρέπει να έχουν διαφορετικό κωδικό οι οποίοι πρέπει να δημιουργούνται τυχαία. Νοείται ότι πρέπει να αποθηκεύονται σε κρυπτογραφημένη μορφή.
* Τα χαρακτηριστικό που επιτρέπει τον καθορισμό «Hints» για τους κωδικούς πρέπει να απενεργοποιείται.
* Όλα τα συστήματα (τύπου workstation) τα οποία δεν χρησιμοποιούνται πέραν των 15 (δεκαπέντε) λεπτών πρέπει να κλειδώνονται αυτόματα (password protected screen saver).
* Όλοι οι εξυπηρετητές που δεν χρησιμοποιούνται πέραν των 5 (πέντε) λεπτών πρέπει να κλειδώνονται αυτόματα (password protected screen saver).
* Όλες οι αδρανείς συνδέσεις (inactive sessions) πέραν των 15 λεπτών πρέπει να τερματίζονται αυτόματα (auto logout).
* Η χρήση των κοινών λογαριασμών (shared accounts) πρέπει να περιορίζεται στο ελάχιστο δυνατό.
  + Η χρήση κοινών λογαριασμών για την καθημερινή διεκπεραίωση εργασιών απαγορεύεται.
  + Η χρήση κοινών λογαριασμών επιτρέπεται μόνο σε περιπτώσεις όπου δεν υπάρχει άλλος εναλλακτικός τρόπος για τη διεκπεραίωση των εργασιών και μετά από σχετική έγκριση.
  + Όπου χρησιμοποιείται κοινός λογαριασμός, η πρόσβαση στα πληροφοριακά συστήματα πρέπει να προστατεύεται με λογισμικό το οποίο έχει την δυνατότητα εξακρίβωσης της ταυτότητας του χρήστη που χρησιμοποιεί τον κοινό λογαριασμό. Για παράδειγμα (Observe IT, CyberArk, Microsoft PAM).
  + Όπου χρησιμοποιείται κοινός λογαριασμός, νοείται ότι κατά την αποχώρηση / μετακίνηση ενός από τους χρήστες του κοινού λογαριασμού, ο κωδικός πρόσβασης πρέπει άμεσα να αλλάζει.
* Όπου χρησιμοποιείται το δικτυακό πρωτόκολλο SNMP, δεν πρέπει να ορίζονται οι προκαθορισμένοι κωδικοί «public», «private» και «system», ενώ ταυτόχρονα πρέπει να είναι διαφορετικοί από τους κωδικούς που χρησιμοποιούνται για τη διαδραστική επικοινωνία με τη συσκευή. Όπου είναι δυνατό πρέπει να χρησιμοποιείται η έκδοση SNMPv3 που υποστηρίζει κρυπτογράφηση και αυθεντικοποίηση.
* Απαγορεύεται η καταγραφή των κωδικών πρόσβασης σε αρχεία για διασύνδεση συστημάτων, σε μη κρυπτογραφημένη μορφή. Οι κωδικοί πρόσβασης πρέπει να προστατεύονται με την εφαρμογή βέλτιστων τεχνικών και πρακτικών προστασίας κωδικών πρόσβασης.
* Απαγορεύεται η χρήση κωδικών μέσω μη κρυπτογραφημένων καναλιών επικοινωνίας (π.χ. http, ftp, telnet κτλ.)
* Σε περίπτωση παραβίασης ή υποψίας παραβίασης ενός κωδικού χρήστη ή συστήματος, πρέπει να εφαρμόζονται οι διαδικασίες που διέπουν την Πολιτική Διαχείρισης Περιστατικών Ασφαλείας. Ο [Όνομα Οργανισμού] διατηρεί το δικαίωμα να διεξάγει ελέγχους στους κωδικούς πρόσβασης.

# Κωδικοί Πρόσβασης

Οι κωδικοί που εκδίδονται, τόσο για νέους λογαριασμούς χρηστών, όσο και για την επανέκδοση κωδικών για τους υφιστάμενους λογαριασμούς χρηστών πρέπει να δημιουργούνται τυχαία (randomly generated), να είναι μιας χρήσης και να έχουν χρονική διάρκεια όχι περισσότερο από 7 ημέρες.

* **Password history**: Οι κωδικοί πρόσβασης πρέπει να είναι διαφορετικοί από τους **Χ**, τουλάχιστο, τελευταίους κωδικούς του χρήστη
* **Maximum password age**: Ο μέγιστος χρόνος ζωής ενός κωδικού δεν πρέπει να υπερβαίνει τις **Χ** μέρες. Με τη λήξη της χρονικής αυτής διάρκειας, η αλλαγή του κωδικού πρέπει να είναι υποχρεωτική.
* **Password age (for System, Service Accounts and Admin Accounts)**: Σημειώνεται ότι για τους λογαριασμούς υπηρεσιών (system, service accounts) και των λογαριασμών με αυξημένα δικαιώματα πρόσβασης (privileged accounts), ο μέγιστος χρόνος ζωής ενός κωδικού δεν πρέπει να υπερβαίνει τις **Χ** μέρες.
* **Minimum password age**: Ο ελάχιστος χρόνος ζωής ενός κωδικού πρέπει να είναι **1** (μια) μέρα.
* **Minimum password length**: Οι κωδικοί πρόσβασης πρέπει να είναι το ελάχιστο **10** (δέκα) χαρακτήρες.
* **Maximum password length (for System, Service and Admin Accounts)**: Σημειώνεται ότι για τους λογαριασμούς υπηρεσιών (system, service accounts) και των λογαριασμών με αυξημένα δικαιώματα πρόσβασης (privileged accounts), οι κωδικοί πρόσβασης πρέπει να είναι το ελάχιστο **15** (δεκαπέντε) χαρακτήρες.
* **Password Complexity**: Οι κωδικοί πρόσβαση πρέπει να περιλαμβάνουν τουλάχιστο 3 (τρεις) από τους 4 (τέσσερεις) διαφορετικούς τύπους χαρακτήρων. Τύποι χαρακτήρων είναι
  + τα κεφαλαία, [Α B C D E F … Z],
  + πεζά γράμματα [a b c d e f … z],
  + αριθμοί [0 1 2 3 4 5 6 7 8 9],
  + ειδικοί χαρακτήρες [ ( ) ` ~ ! @ # $ % ^ & \* - + = | \ { } [ ] : ; " ' < > . ? / ) ],
* **Password Illegal Patterns**: Οι κωδικοί πρόσβασης δεν πρέπει είναι όμοιοι με τους λογαριασμούς των χρηστών (user name) και δεν πρέπει να είναι κοινές λέξεις (από λεξικό) ούτε πρέπει να βασίζονται σε προσωπικές πληροφορίες του χρήστη (π.χ. ονόματα οικογένειας, μάρκα αυτοκινήτου, ομάδα κτλ.). Επιπρόσθετα οι κωδικοί πρόσβασης δεν πρέπει να είναι χαρακτήρες σε σειρά (π.χ. 12345, 54321, qwerty, abcdef κτλ.).
* **Password encryption**: Οι κωδικοί πρόσβασης δεν πρέπει να αποθηκεύονται σε μορφή απλού κειμένου (Plain Text) ή/και χρησιμοποιώντας αδύνατους μηχανισμούς κρυπτογράφησης. Επιπρόσθετα όπου αποθηκεύονται κρυπτογραφημένοι κωδικοί πρόσβασης, οι εν λόγω κωδικοί δεν πρέπει να μπορούν να ανακτηθούν (disable store passwords using reversible encryption).
* Lockout threshold: Ο λογαριασμός πρόσβασης πρέπει να κλειδώνεται αυτόματα στις 5 (πέντε) ανεπιτυχείς προσπάθειες εισαγωγής του κωδικού ασφαλείας
  + Lockout counter: Ο αριθμός των λεπτών που πρέπει να παρέλθουν από τη στιγμή που ένας χρήστης αποτυγχάνει να συνδεθεί πριν επαναφερθεί ο μετρητής αποτυχημένης προσπάθειας σύνδεσης σε 0, πρέπει να είναι 30 λεπτά.
  + Lockout duration: Ο κλειδωμένος λογαριασμός πρόσβασης συνιστάται να ξεκλειδώνεται από εξουσιοδοτημένο διαχειριστή του συστήματος
* **Dormant Accounts**: Οι ανενεργοί λογαριασμοί πρέπει να απενεργοποιούνται και τα δικαιώματα πρόσβασης τους να αναιρούνται. Ανενεργός λογαριασμός είναι ο λογαριασμός ο οποίος δεν έχει συνδεθεί στο σύστημα για περισσότερες από τις ημέρες που προσδιορίζονται στο «Maximum password age», δηλαδή Χ ημέρες.

Επιπρόσθετα για την αυθεντικοποίηση των χρηστών σε κρίσιμα συστήματα ή σε συστήματα που είναι προσβάσιμα από το διαδίκτυο πρέπει να χρησιμοποιείται πιστοποίηση διπλής συνιστώσας και Ισχυρή Αυθεντικοποίηση. Πιστοποίηση διπλής συνιστώσας και Ισχυρή Αυθεντικοποίηση πρέπει να τηρείται κατά την απομακρυσμένη πρόσβαση των συστημάτων. Νοείται ότι οι κωδικοί μιας χρήσης (One Time Password - Token), πρέπει να δημιουργούνται τυχαία.

* **One Time Password - Validity Period**: Ο μέγιστος χρόνος ζωής του κωδικού μιας χρήσης (OTP) δεν πρέπει να υπερβαίνει τα **Χ** λεπτά.
* **One Time Password - Lockout Threshold**: Ο λογαριασμός πρέπει να κλειδώνεται αυτόματα στις **Χ** ανεπιτυχείς προσπάθειες εισαγωγής του OTP.
* **One Time Password - Lockout counter**: Ο αριθμός των λεπτών που πρέπει να παρέλθουν από τη στιγμή που ένας χρήστης αποτυγχάνει να συνδεθεί πριν επαναφερθεί ο μετρητής αποτυχημένης προσπάθειας σύνδεσης σε 0, πρέπει να είναι **Χ** λεπτά.
* **One Time Password - Lockout duration**: Ο κλειδωμένος λογαριασμός πρόσβασης συνιστάται να ξεκλειδώνεται από εξουσιοδοτημένο διαχειριστή του συστήματος.
* **One Time Password - Password Complexity**: Οι κωδικοί πρόσβαση πρέπει να περιλαμβάνουν τουλάχιστο 2 (δύο) από τους 4 (τέσσερεις) διαφορετικούς τύπους χαρακτήρων. Τύποι χαρακτήρων είναι:
  + τα κεφαλαία, [Α B C D E F … Z],
  + πεζά γράμματα [a b c d e f … z],
  + αριθμοί [0 1 2 3 4 5 6 7 8 9],
  + ειδικοί χαρακτήρες [ ( ) ` ~ ! @ # $ % ^ & \* - + = | \ { } [ ] : ; " ' < > . ? / ) ],

# Βέλτιστες τεχνικές και πρακτικές προστασίας κωδικών

* Η χρήση ενός ισχυρού κωδικού πρόσβασης και η συχνή αλλαγή του, είναι από τις πιο σημαντικές ενέργειες που προτείνονται προκειμένου να προστατέψετε τους λογαριασμούς σας από τους κακόβουλους χρήστες.
* Κρατήστε όλους τους κωδικούς πρόσβασης σας μυστικούς.
* Μη χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης παντού.
* Λειτουργός του [Όνομα Οργανισμού] δεν πρόκειται ΠΟΤΕ να σας ζητήσει οποιοδήποτε κωδικό πρόσβασης.
  + Οι κωδικοί δεν πρέπει να αποκαλύπτονται σε ΚΑΝΕΝΑ (προϊστάμενο, συνάδελφο, διαχειριστή συστημάτων, φίλους κ.τ.λ.).σε περίπτωση που οποιοσδήποτε σας ζητήσει να του πείτε το κωδικό πρόσβασης σας, αναφέρτε το αμέσως στον Υπεύθυνο Ασφαλείας.
* Οι κωδικοί πρόσβασης πρέπει να είναι μεταξύ 10 (δέκα) και 127 (εκατό είκοσι επτά) χαρακτήρων και να περιλαμβάνει τουλάχιστο 3 (τρεις) από τους 4 (τέσσερεις) διαφορετικούς τύπους χαρακτήρων. Τύποι χαρακτήρων είναι
  + τα κεφαλαία, [Α B C D E F … Z],
  + πεζά γράμματα [a b c d e f … z],
  + αριθμοί [0 1 2 3 4 5 6 7 8 9],
  + ειδικοί χαρακτήρες [ ( ) ` ~ ! @ # $ % ^ & \* - + = | \ { } [ ] : ; " ' < > . ? / ) ],
* Οι κωδικοί πρόσβασης που παρέχονται από τους διαχειριστές, προμηθευτές και τους κατασκευαστές των συστημάτων πρέπει άμεσα να αλλάζονται.
* Οι κωδικοί πρόσβασης δεν πρέπει να καταγράφονται ή να αποθηκεύονται εκτός αν χρησιμοποιούνται ισχυροί μηχανισμοί για την προστασία τους.
* Οι κωδικοί πρόσβασης δεν πρέπει να είναι όμοιοι με τους λογαριασμούς των χρηστών (user name).
* Οι κωδικοί πρόσβασης δεν πρέπει να είναι κοινές λέξεις (από λεξικό) ούτε πρέπει να βασίζονται σε προσωπικές πληροφορίες του χρήστη (π.χ. ονόματα οικογένειας, μάρκα αυτοκινήτου, ομάδα κλπ.).
* Οι κωδικοί πρόσβασης δεν πρέπει να είναι χαρακτήρες σε σειρά (π.χ. 12345, 54321, qwerty, abcde, κλπ.)
* Το "Remember Password" χαρακτηριστικό των εφαρμογών (Internet Explorer, Firefox, Google Chrome κλπ.) πρέπει να είναι απενεργοποιημένο.
* Όπου είναι εφικτό ή όπου κρίνεται αναγκαίο, να γίνεται χρήση τεχνολογίας two factor authentication με το συνδυασμό κωδικών πρόσβασης, έξυπνων καρτών (smart cards) ή/και βιομετρικών.

# Εξουσιοδότηση Χρηστών

Όλα τα δικαιώματα πρόσβασης, πρέπει να καθορίζονται σύμφωνα με τις πιο κάτω αρχές:

* «Αρχή των ελάχιστων προνομίων» (principle of least privilege)
* «Αρχή της ανάγκης γνώσης» (principle of need to know)

Τα δικαιώματα πρόσβασης των χρηστών πρέπει να είναι προκαθορισμένα, σύμφωνα με τις θέσεις και τα καθήκοντα εργασίας του [Όνομα Οργανισμού] όπως αυτές καθορίζονται από τη Διεύθυνση του [Όνομα Οργανισμού]. Επιπρόσθετα, τα εν λόγω δικαιώματα, πρέπει να εγκρίνονται από τον επικεφαλής της εκάστοτε υπηρεσιακής μονάδας, με βάση τα ακόλουθα:

* Λόγοι για την πρόσβαση στο συγκεκριμένο σύστημα.
* Διαχωρισμός των καθηκόντων.
* Το επίπεδο πρόσβασης που απαιτείται.
* Προκειμένου να δοθεί εξουσιοδότηση για περαιτέρω δικαιώματα πρόσβασης σε ένα χρήστη πέραν των προκαθορισμένων, σχετική αίτηση θα πρέπει να συμπληρώνεται.
* Σε περιπτώσεις πρόσβασης στα συστήματα του [Όνομα Οργανισμού] από εξωτερικούς συνεργάτες/τρίτα μέρη, η έγκριση παροχής πρόσβασης, πρέπει να καταγράφεται και να παρέχεται από τον υπεύθυνο του εκάστοτε συστήματος.
* Οι υπεύθυνοι ανάπτυξης *εφαρμογών* καθώς και το τεχνικό προσωπικό δεν πρέπει να έχουν πρόσβαση στα συστήματα και τα αντίστοιχα δεδομένα παραγωγής, εκτός εάν υπάρχει συγκεκριμένος λόγος.
* Θα πρέπει να διατηρούνται αρχεία όλων των δικαιωμάτων πρόσβασης είτε είναι σε ισχύ είτε όχι.
* Οι ανενεργοί (**καθορίστε χρόνο σε ημέρες**) λογαριασμοί θα πρέπει αυτόματα να απενεργοποιούνται και τα δικαιώματα πρόσβασης τους να αναιρούνται.
* Οι απενεργοποιημένοι λογαριασμοί δεν πρέπει να διαγράφονται.
  + Σε περίπτωση που οι απενεργοποιημένοι λογαριασμοί περιέχουν Δεδομένα Προσωπικού Χαρακτήρα πρέπει να τυγχάνουν χειρισμού όπως προβλέπεται από την εκάστοτε νομοθεσία
* Τα δικαιώματα πρόσβασης θα πρέπει να αναιρούνται σε περιπτώσεις όπου οι χρήστες βρίσκονται με άδεια ή/και με άδεια ασθένειας.
* Τα δικαιώματα πρόσβασης θα πρέπει να αναιρούνται σε περιπτώσεις όπου οι χρήστες δεν δραστηριοποιούνται πλέον για τον [Όνομα Οργανισμού].
* Τα δικαιώματα πρόσβασης θα πρέπει να αναιρούνται κατά τη διάρκεια των μη εργάσιμων ωρών και αργιών.
* Τα δικαιώματα πρόσβασης θα πρέπει να ελέγχονται και να αναθεωρούνται ανά τακτά (**καθορίστε χρόνο σε μήνες**) χρονικά διαστήματα από την Μονάδα Εσωτερικού Ελέγχου.
* Σε περιπτώσεις κατάχρησης των εν λόγω δικαιωμάτων πρόσβασης, ο Επιχειρησιακός Ιδιοκτήτης του συστήματος και η Μονάδα Εσωτερικού Ελέγχου έχουν το δικαίωμα να ανακαλέσουν τα εν λόγω δικαιώματα πρόσβασης.

Για περισσότερες πληροφορίες βλέπε Πολιτική Ανθρώπινου Δυναμικού.

# Προνομιακά Δικαιώματα Χρηστών

Σύμφωνα με τον Νόμο Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] θεσπίζει μέτρα για τη διασφάλιση της ορθής διαχείρισης των προνομιούχων χρηστών, και ενεργοποίηση τους μόνο όταν χρειάζεται. Ο [Όνομα Οργανισμού] ελέγχει εάν στους χρήστες δεν χορηγούνται προνομιακά δικαιώματα εξ ορισμού και ότι τα συστήματα και οι εφαρμογές δεν λειτουργούν εξ ορισμού με προνομιακά δικαιώματα χρήστη, προκειμένου να μετριάζεται ο κίνδυνος της κλιμάκωσης προνομίων και να διασφαλίζεται η προστασία των προνομιακών δικαιωμάτων των χρηστών από κακόβουλες πράξεις ή από άλλες αρνητικές συμπεριφορές ή προθέσεις.

1. Κριτήρια Χορήγησης Προνομιακών Δικαιωμάτων:

• Η πρόσβαση με προνομιακά δικαιώματα χορηγείται μόνο όταν υπάρχει αποδεδειγμένη ανάγκη (need to use basis) και με βάση συγκεκριμένα γεγονότα (event by event basis).

1. Έγκριση Υπεύθυνου:

• Ο χορηγός προνομιακών δικαιωμάτων πρέπει να είναι υπεύθυνος, εξουσιοδοτημένο πρόσωπο που κατανοεί τις επιπτώσεις της πρόσβασης και της χρήσης με προνομιακά δικαιώματα.

1. Διαδικασία Αξιολόγησης Ανάγκης:

• Καθορισμός συγκεκριμένων κριτηρίων για την ανάλυση της ανάγκης προνομιακής πρόσβασης, ώστε να διασφαλίζεται ότι η πρόσβαση χορηγείται μόνο σε περιπτώσεις πραγματικής ανάγκης.

1. Εκδήλωση Συγκεκριμένων Συμβάντων:

• Η πρόσβαση με προνομιακά δικαιώματα πρέπει να συνδέεται με συγκεκριμένα συμβάντα (events) και να χορηγείται μόνο κατά τη διάρκεια αυτών των συμβάντων.

1. Εγγραφή και Επίβλεψη:

• Καταγραφή όλων των περιπτώσεων προνομιακής πρόσβασης, συμπεριλαμβανομένων των συγκεκριμένων γεγονότων που δικαιολογούν την πρόσβαση.

1. Αναθεώρηση και Ανακατανομή:

• Περιοδική αναθεώρηση των προνομιακών δικαιωμάτων, με τυχόν ανακατανομή ή ανάκληση ανάλογα με τις εξελίξεις και τις ανάγκες.

# Λογαριασμοί με αυξημένα δικαιώματα πρόσβασης

Η χρήση των λογαριασμών με αυξημένα δικαιώματα πρόσβασης για την εκτέλεση καθημερινών εργασιών από τους διαχειριστές των συστημάτων, απαγορεύεται. Ο κάθε διαχειριστής πρέπει να έχει τον δικό του ονομαστικό λογαριασμό ως απλός χρήστης προκειμένου να διεκπεραιώνει τις καθημερινές του εργασίες. Όσον αφορά τη διαχείριση των εξυπηρετητών και των εφαρμογών, ο κάθε διαχειριστής πρέπει να έχει ξεχωριστό ονομαστικό λογαριασμό τον οποίο να χρησιμοποιεί μόνο όταν αυτό είναι αναγκαίο για τη πρόσβαση και διαχείριση των εξυπηρετητών και εφαρμογών.

Όλες οι προσβάσεις σε πληροφοριακά συστήματα και πληροφορίες πρέπει να καταγράφονται και να αρχειοθετούνται (ηλεκτρονικά). Επιπλέον, όλες οι ενέργειες των διαχειριστών καθώς και οι οποιεσδήποτε άλλες συνδέσεις των χρηστών στα πιο κάτω συστήματα πρέπει να οπτικογραφούνται, με τη βοήθεια εξειδικευμένου μηχανισμού ελέγχου/λογισμικού. (π.χ. Observe IT, CyberArk, Centrify, Balabit):

* Συστήματα που έχουν διαβαθμιστεί ως Κρίσιμης σημασίας
* Συστήματα που διαχειρίζονται ή/και περιέχουν ή/και επεξεργάζονται εμπιστευτικής φύσεως πληροφορίες (όπως προσωπικά δεδομένα, τραπεζικά δεδομένα)
* Συστήματα που περιέχουν κοινοχρήστους λογαριασμούς
* Συστήματα που είναι εγκατεστημένα στις De-Militarized Zones (DMZs)
* Συστήματα που είναι προσβάσιμα από εξωτερικούς συνεργάτες

# Λογαριασμοί εκτός Οργανισμού

Σε περιπτώσεις όπου απαιτούνται εταιρικοί λογαριασμοί σε πλατφόρμες και εφαρμογές εκτός του [Όνομα Οργανισμού] για τη δημιουργία τους, πρέπει να καθοριστεί και να ακολουθείται διαδικασία. Η διαδικασία μεταξύ άλλων πρέπει να περιλαμβάνει:

* Την καταγραφή σε μητρώο που να περιέχει τους λογαριασμούς, τους εξουσιοδοτημένους χρήστες και τους λόγους που απαιτούνται/χρησιμοποιούνται
* Τον καθορισμό δύο λειτουργών ως διαχειριστές (ένας υπεύθυνος και ένας αντικαταστάτης).
* Την αναθεώρηση των λειτουργών και την αλλαγή του κωδικού πρόσβασης σε περιπτώσεις αποχώρησης/μετακίνησης προσωπικού.
* Την απενεργοποίηση του λογαριασμού όταν δεν είναι πλέον απαραίτητος
* Την αναφορά οποιοδήποτε περιστατικού (δραστηριότητα ή ανησυχία ή υποψία) μπορεί να βλάψει έμμεσα ή άμεσα την ασφάλεια των πληροφοριακών συστημάτων ή/και των πληροφοριών του [Όνομα Οργανισμού].

Σημειώνεται ότι, θα πρέπει να γίνεται χρήση Πιστοποίησης Διπλής Συνιστώσας και ο κωδικός πρόσβασης πρέπει να αλλάζεται σε ετήσια βάση.

# Εξωτερική Πρόσβαση σε Πόρους του [Όνομα Οργανισμού]

Σύμφωνα με τον Νόμο Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] οφείλει να εξασφαλίσει επαρκή μέτρα ελέγχου πρόσβασης στο πλαίσιο της εξωτερικής πρόσβασης σε οργανωτικούς πόρους. Ο [Όνομα Οργανισμού] θα πρέπει 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. Παρακάτω αναφέρονται διαδικασίες για τη χορήγηση εξωτερικής πρόσβασης και την τήρηση καταλόγου των εξωτερικών προσβάσεων.

1. Έγκριση Εξωτερικής Πρόσβασης:

• Η εξωτερική πρόσβαση σε πόρους του οργανισμού χορηγείται μόνο μετά από έγκριση από εξουσιοδοτημένο υπεύθυνο.

1. Διαδικασία Χορήγησης Πρόσβασης:

• Οι εξωτερικές προσβάσεις χορηγούνται μετά από σχετική αίτηση, η οποία πρέπει να περιλαμβάνει τους λόγους της πρόσβασης και τα αναγκαία μέτρα ασφαλείας που λαμβάνονται.

1. Καταγραφή Εξωτερικών Προσβάσεων:

• Ο εξουσιοδοτημένος υπεύθυνος διατηρεί λίστα με όλες τις εξωτερικές προσβάσεις που έχουν χορηγηθεί, συμπεριλαμβάνοντας τα συστήματα που επηρεάζονται και την ημερομηνία χορήγησης.

1. Διάρκεια Χορήγησης Πρόσβασης:

• Καθορισμός της περιόδου για την οποία ισχύει η εξωτερική πρόσβαση, με δυνατότητα ανανέωσης μετά από νέα έγκριση.

1. Μέτρα Ασφαλείας:

• Καθορισμός των μέτρων ασφαλείας που πρέπει να τηρούνται κατά τη διάρκεια της εξωτερικής πρόσβασης, περιλαμβανομένων της κρυπτογράφησης και της διαχείρισης δικαιωμάτων.

1. Ενημέρωση Συστημάτων Ασφαλείας:

• Οποιαδήποτε αλλαγή στην εξωτερική πρόσβαση πρέπει να αντικατοπτρίζεται άμεσα στα συστήματα ασφαλείας του οργανισμού.

# Απομακρυσμένη Πρόσβαση

Οι απομακρυσμένες προσβάσεις (Remote Access) στο δίκτυο, στα πληροφοριακά συστήματα και στις πληροφορίες του [Όνομα Οργανισμού], θα πρέπει (όπου είναι δυνατό), να αποφεύγονται. Η εξουσιοδότηση χρήσης για την απομακρυσμένη πρόσβαση στο δίκτυο, στα πληροφοριακά συστήματα και στις πληροφορίες του [Όνομα Οργανισμού], θα πρέπει να παραχωρείται μόνο σε εξαίρετες/μεμονωμένες περιπτώσεις, όπου δεν υπάρχει άλλος, εναλλακτικός τρόπος, προκειμένου ο χρήστης να μπορεί να διεκπεραιώσει τις εργασίες του.

Οι απομακρυσμένες προσβάσεις, όπου είναι εφικτό, πρέπει να διενεργούνται μέσω της χρήσης απομονωμένου εικονικού περιβάλλοντος (Υποδομή εικονικής επιφάνειας εργασίας (Virtual Desktop Infrastructure (VDI)), SandBox και τεχνολογίας streaming), ούτως ώστε να αποτρέπεται η μεταφορά, επεξεργασία και αποθήκευση εταιρικών δεδομένων στο μηχανογραφικό εξοπλισμό που χρησιμοποιείται ως μέσο σύνδεσης.

* Όλες οι απομακρυσμένες συνδέσεις, θα πρέπει να διεξάγονται χρησιμοποιώντας ισχυρούς μηχανισμούς και τεχνολογίες κρυπτογράφησης. (π.χ. VPN, βλέπε Πολιτική Ασφάλειας Δικτύου)
* Η έναρξη μιας απομακρυσμένης πρόσβασης, καθώς και η πρόσβαση στο δίκτυο, στα συστήματα και στις πληροφορίες του Οργανισμού, θα πρέπει να προστατεύεται μέσω πιστοποίησης διπλής συνιστώσας, ισχυρής ταυτοποίησης και αυθεντικοποίησης των χρηστών. Πιο συγκεκριμένα, η αυθεντικοποίηση των χρηστών θα πρέπει να επιτυγχάνεται χρησιμοποιώντας τουλάχιστο τα πιο κάτω:
  + Συνδυασμό διακριτικών, πιστοποίηση διπλής συνιστώσας (two-factor authentication).
  + Χρήση κωδικών πρόσβασης μιας χρήσης (OTP) και προκαθορισμένης χρονικής διάρκειας.
  + Oι κωδικοί πρόσβασης θα πρέπει να συμμορφώνονται σύμφωνα με τις κατευθυντήριες γραμμές σωστής χρήσης κωδικών.
* Όλα τα διακριτικά των χρηστών, τα οποία χρησιμοποιούνται για την αυθεντικοποίηση τους στο δίκτυο, στα συστήματα και στις πληροφορίες του Οργανισμού, θα πρέπει να είναι ατομικά/ονομαστικά και να προσδιορίζουν τον εν λόγω χρήστη. Επιπρόσθετα, οι κωδικοί πρόσβασης θα πρέπει να παραμένουν μυστικοί.
* Η εξουσιοδότηση για την απομακρυσμένη πρόσβαση, θα πρέπει να απαγορεύεται για τους πιο κάτω τύπους λογαριασμών:
  + κοινόχρηστους ή/και μη ονομαστικούς λογαριασμούς.
  + βοηθητικούς λογαριασμούς.
  + λογαριασμούς με αυξημένα δικαιώματα πρόσβασης. Όπου απαιτείται απομακρυσμένη πρόσβαση για τους διαχειριστές των συστημάτων η σύνδεση πρέπει να επιτυγχάνεται με τους απλούς λογαριασμούς των χρηστών.
  + λογαριασμούς υπηρεσιών (service accounts).
  + εποχιακούς ή/και προσωρινούς λογαριασμούς χρηστών.
* Όπως αναφέρεται και πιο πάνω, μόνο εξουσιοδοτημένοι χρήστες θα πρέπει να έχουν δικαίωμα απομακρυσμένης πρόσβασης στο δίκτυο, στα πληροφοριακά συστήματα και στις πληροφορίες του [Όνομα Οργανισμού]. Οι εν λόγω χρήστες θα πρέπει να συμμορφώνονται με το Πολιτική Αποδεκτής Χρήσης καθώς και γενικότερα με τις Πολιτικές σχετικά με την Ασφάλεια Πληροφοριών.
  + Όλα τα δικαιώματα πρόσβασης, θα πρέπει να καθορίζονται σύμφωνα με τις ευθύνες και τα καθήκοντα του κάθε χρήστη.
  + Επιπρόσθετα, όλα τα δικαιώματα πρόσβασης, θα πρέπει να καθορίζονται σύμφωνα με τις πιο κάτω αρχές:
    - «αρχή των ελάχιστων προνομίων» (principle of least privilege)
    - «αρχή της ανάγκης γνώσης» (principle of need to know)
* Όλες οι απομακρυσμένες συνδέσεις (επιτυχείς ή/και ανεπιτυχείς) θα πρέπει να παρακολουθούνται και να καταγράφοντα.
* Όλες οι απομακρυσμένες συνδέσεις θα πρέπει να τυγχάνουν οπτικογράφησης, με την βοήθεια εξειδικευμένου λογισμικού.
* Στις περιπτώσεις όπου οι αδρανείς συνδέσεις ξεπερνούν τα 15 λεπτά θα πρέπει αυτόματα να ενεργοποιείται η λειτουργία προφύλαξης οθόνης (password protected screen saver).
* Όταν δεν απαιτείται πλέον, ή με την λήξη της εξουσιοδότησης, ή με τον τερματισμό της απασχόλησης του χρήστη, η εξουσιοδότηση απομακρυσμένης πρόσβασης καθώς και τα δικαιώματα πρόσβασης θα πρέπει άμεσα να αναιρούνται.
* Νοείται ότι, οι πληροφορίες που δημιουργούνται ή/και διακινούνται ή/και αποθηκεύονται για λογαριασμό του Οργανισμού σε ιδιόκτητο μηχανογραφικό εξοπλισμό αποτελούν ιδιοκτησία του [Όνομα Οργανισμού].
* Το μέγεθος των πληροφοριών του Οργανισμού που μεταφέρονται μέσω της απομακρυσμένης πρόσβασης δεν θα πρέπει να ξεπερνά τα 100 Mb εβδομαδιαία ανά χρήστη.

# Συνδέσεις Τρίτων Μερών

* Οι απομακρυσμένες συνδέσεις από τρίτους στο δίκτυο του [Όνομα Οργανισμού] θα πρέπει, όπου είναι δυνατό, να αποφεύγονται.
* Η οποιαδήποτε σύνδεση με τη μηχανογραφική υποδομή του Οργανισμού πρέπει να τυγχάνει ελέγχου και εξουσιοδότησης από τον Υπεύθυνο Ασφάλειας Πληροφοριών.
* Οι τρίτοι (π.χ. εταιρίες) πρέπει έχουν συμφωνήσει και υπογράψει σχετική συμφωνία Τρίτων Μερών και εμπιστευτικότητας, προκειμένου να εγκριθεί η σύνδεση. Σε περίπτωση επεξεργασίας προσωπικών δεδομένων θα πρέπει να υπογραφεί και το Data Processing Agreement.
* Τα δικαιώματα πρόσβασης πρέπει να καθοριστούν πριν την υπογραφή της συμφωνίας.
* Στις περιπτώσεις σύνδεσης τρίτων στο δίκτυο του Οργανισμού θα πρέπει να υπάρχουν μηχανισμοί ασφαλούς μετάδοσης των δεδομένων μεταξύ του [Όνομα Οργανισμού] και των Τρίτων Μερών. (βλέπε Πολιτική Ασφάλειας Δικτύου) καθώς και μηχανισμοί παρακολούθησης όλων των ενεργειών από τα τρίτα μέρη.
* Τα Τρίτα Μέρη πρέπει να χειρίζονται τις πληροφορίες του Οργανισμού όπως καθορίζεται στην Πολιτική Διαχείρισης Στοιχείων Ενεργητικού*.*
* Τα Τρίτα Μέρη πρέπει να καθορίσουν ένα πρόσωπο που θα είναι ο υπεύθυνος επικοινωνίας, για τη σύνδεση τους με του [Όνομα Οργανισμού]. Στην περίπτωση που ο υπεύθυνος επικοινωνίας αλλάξει, ο [Όνομα Οργανισμού] θα πρέπει να ενημερωθεί άμεσα.
* Όταν δεν απαιτείται πλέον ή με τον τερματισμό της οποιασδήποτε σύνδεσης, τα δικαιώματα πρόσβασης στους τρίτους πρέπει να αφαιρούνται άμεσα.
* Όλες οι συνδέσεις πρέπει να παρακολουθούνται όπως προβλέπεται στην Πολιτική Ασφάλειας Δικτύου*.*
* Σε περίπτωση που απαιτείται η ασυνόδευτη (unattended) πρόσβαση από εξωτερικούς συνεργάτες:
  + η πρόσβαση πρέπει να περιορίζεται μόνο σε εξωτερικούς συνεργάτες που έχουν υπογράψει σχετική συμφωνία παροχής υπηρεσιών και συμφωνία εμπιστευτικότητας. (Βλέπε Πολιτική Διαχείρισης).
  + πρόσβαση πρέπει να περιορίζεται ΜΟΝΟ στο εξωτερικό δίκτυο (DMZ) του Οργανισμού, σε απομονωμένο τοπικό δίκτυο (isolated VLAN). Νοείται ότι σε καμία περίπτωση δεν πρέπει να παραχωρείται η ασυνόδευτη (unattended) πρόσβαση στους εξωτερικούς συνεργάτες σε περιβάλλον παραγωγής (production environment).
  + η πρόσβαση πρέπει να περιορίζεται αυστηρά μόνο στα συστήματα που τα δεδομένα που διαχειρίζονται είναι masked (data maskιng) ή/και scrambled, pseudonymization ή και σε συστήματα που δεν περιέχουν εμπιστευτικής φύσεως πληροφορίες ή και δεδομένα προσωπικού χαρακτήρα.
  + ο μηχανογραφικός εξοπλισμός που χρησιμοποιείται ως μέσο σύνδεσης, για την απομακρυσμένη πρόσβαση στο δίκτυο, στα πληροφοριακά συστήματα και πληροφορίες του Οργανισμού, θα πρέπει να τυγχάνει αξιολόγησης (posture assessment) προτού παραχωρηθεί η πρόσβαση σε αυτόν. Πιο συγκεκριμένα, ο μηχανογραφικός εξοπλισμός θα πρέπει να:
    - είναι ενημερωμένος με τις τελευταίες ενημερώσεις ασφαλείας.
    - σαρώνεται με λογισμικό αντιμετώπισης κακόβουλων λογισμικών.
    - προστατεύεται (on-access scanning) με λογισμικό αντιμετώπισης κακόβουλων λογισμικών. (βλέπε Πολιτική Ασφάλειας Συστημάτων).
    - μην είναι συνδεδεμένος σε κακόβουλες δικτυακές διευθύνσεις (bad reputations IPs).
  + Όλες οι απομακρυσμένες συνδέσεις θα πρέπει να τυγχάνουν οπτικογράφησης, με την βοήθεια εξειδικευμένου λογισμικού. (π.χ. Observe IT, CyberArk, Centrify, Balabit).
* Σε περίπτωση όπου δεν πληρούνται τα πιο πάνω για την ασυνόδευτη (unattended) πρόσβαση και η σύνδεση από τους εξωτερικούς συνεργάτες ή/και τρίτους απαιτείται σε συστήματα παραγωγής, ή/και στο εσωτερικό δίκτυο του Οργανσιμού, η εν λόγω σύνδεση θα πρέπει να συνοδεύεται καθ’ όλη τη διάρκεια της (είτε μέσω webex είτε τοπικά) από εξουσιοδοτημένο λειτουργό/διαχειριστή του [Όνομα Οργανισμού].
* Σε περιπτώσεις κατάχρησης των εν λόγω δικαιωμάτων, ο [Όνομα Οργανισμού] διατηρεί το δικαίωμα αναίρεσης της εξουσιοδότησης για την απομακρυσμένη πρόσβαση.