Όνομα Οργανισμού

Πολιτική Διαχείρισης Στοιχείων Ενεργητικού

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Διαχείρισης Στοιχείων Ενεργητικού |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

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

Καταγραφή Τροποποιήσεων

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

Αναφορές

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

Υποστηρικτικό Υλικό

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

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

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

Πίνακας Περιεχομένων

[1. Εισαγωγή 4](#_Toc188535532)

[1.1. Σκοπός 4](#_Toc188535533)

[1.2. Πεδίο Εφαρμογής 4](#_Toc188535534)

[2. Πολιτική Διαχείρισης Στοιχείων Ενεργητικού 6](#_Toc188535535)

[2.1. Διαχείριση του κύκλου ζωής στοιχείων ενεργητικού 6](#_Toc188535536)

[2.2. Πολιτική καταγραφής και παρακολούθησης στοιχείων ενεργητικού 8](#_Toc188535537)

[2.3. Καθορισμός Παραμέτρων καταγραφής και παρακολούθησης 8](#_Toc188535538)

[3. Ασφαλής απόσυρση ή επαναχρησιμοποίηση στοιχείων ενεργητικού 10](#_Toc188535539)

[4. Αναθεώρηση 12](#_Toc188535540)

[5. Αναφορές 13](#_Toc188535541)

# Εισαγωγή

# Σκοπός

Το παρόν έγγραφο περιλαμβάνει ενδεικτικούς Όρους Πολιτικής για τη διαχείριση Στοιχείων Ενεργητικού του [Όνομα Οργανισμού] με σκοπό τον καθορισμό κατευθυντήριων γραμμών για τη διατήρηση της κατάλληλης προστασίας των στοιχείων ενεργητικού του [Όνομα Οργανισμού].

Η πολιτική αυτή καθορίζει μια δομημένη προσέγγιση για τη διαχείριση των περιουσιακών στοιχείων καθ' όλη τη διάρκεια του κύκλου ζωής τους, τη διαφύλαξη τους από απειλές σε σχέση με την ασφάλεια πληροφοριών στο κυβερνοχώρο και τη διασφάλιση της συμμόρφωσης με τις νομικές και κανονιστικές απαιτήσεις. Διατηρώντας ακριβή αρχεία και ελέγχους, η πολιτική υποστηρίζει την ικανότητα του [Όνομα Οργανισμού] να εντοπίζει, να προλαμβάνει και να ανταποκρίνεται σε κινδύνους κυβερνοασφάλειας.

Οι στόχοι της Πολιτικής συνοψίζονται ως εξής:

* Η δημιουργία και διατήρηση ακριβούς καταλόγου (μητρώου ενεργητικού) όλων των περιουσιακών στοιχείων πληροφοριών, συμπεριλαμβανομένης της κυριότητας, της ταξινόμησης και της κρισιμότητας τους.
* Καθορισμός ρόλων και αρμοδιοτήτων για τη διαχείριση και την προστασία των στοιχείων ενεργητικού.
* Καθορισμός ιδιοκτήτη του κάθε στοιχείου ενεργητικού οποίος είναι υπεύθυνος για τη διασφάλιση την προστασίας, εύρυθμης λειτουργίας, διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των πληροφοριακών περιουσιακών αυτών στοιχείων
* Διασφάλιση της κατάλληλης κατηγοριοποίησης και χειρισμού των στοιχείων ενεργητικού με βάση την ευαισθησία της πληροφορίας και την αξία αυτού.
* Ελαχιστοποίηση των κινδύνων κατάχρησης, κλοπής ή μη εξουσιοδοτημένης πρόσβασης σε περιουσιακά στοιχεία μέσω κατάλληλων ελέγχων και παρακολούθησης.
* Υποστήριξη των προσπαθειών αντιμετώπισης περιστατικών και αποκατάστασης με την παροχή σαφούς παρακολούθησης των στοιχείων ενεργητικού.
* Ευθυγράμμιση με τα ισχύοντα πρότυπα, όπως το ISO 27001, και τα κανονιστικά πλαίσια για τη διασφάλιση της συμμόρφωσης π.χ. Απόφαση Κ.Δ.Π 389/2020.

# Πεδίο Εφαρμογής

Η Πολιτική Διαχείρισης Στοιχείων Ενεργητικού αποσκοπεί στην αποτελεσματική αναγνώριση, ταξινόμηση και προστασία των περιουσιακών στοιχείων του [Όνομα Οργανισμού]. Ισχύει για όλα τα περιουσιακά στοιχεία που ανήκουν, μισθώνονται ή διαχειρίζεται ο [Όνομα Οργανισμού], συμπεριλαμβανομένων του ανθρώπινου δυναμικού, υλισμικού, του λογισμικού, των πόρων σε cloud περιβάλλον, των δεδομένων, των διαδικασιών και ότι άλλο μπορεί να χαρακτηριστεί ως πνευματική ιδιοκτησία του [Όνομα Οργανισμού]. Περιλαμβάνει όλους τους υπαλλήλους, τους εργολάβους και τρίτα μέρη που έχουν πρόσβαση σε αυτά τα περιουσιακά στοιχεία.

Η Πολιτική καλύπτει όλα τα στάδια του κύκλου ζωής των στοιχείων ενεργητικού, από την απόκτηση και την ανάπτυξη έως τον ολοκλήρωση του κύκλου ζωής του και διαγραφή του, και εφαρμόζεται σε όλες τις τοποθεσίες του [Όνομα Οργανισμού], συμπεριλαμβανομένων των απομακρυσμένων περιβαλλόντων(π.χ. cloud, DR) και των περιβαλλόντων τρίτων συμβαλλομένων μερών.

# Πολιτική Διαχείρισης Στοιχείων Ενεργητικού

# Διαχείριση του κύκλου ζωής στοιχείων ενεργητικού

* Η διαχείριση του κύκλου ζωής των στοιχείων ενεργητικού περιλαμβάνει τη συστηματική διαχείριση των περιουσιακών στοιχείων του [Όνομα Οργανισμού] καθ' όλη τη διάρκεια του κύκλου ζωής τους. Ως εκ τούτου, ο [Όνομα Οργανισμού] εφαρμόζει και διατηρεί μια διαδικασία για την διαχείριση και την ασφάλεια των στοιχείων ενεργητικού κατά την διάρκεια του κύκλου ζωής τους (προμήθεια, εγκατάσταση, συντήρηση και διάθεση) καθορίζοντας αρμόδιους ρόλους για την υλοποίηση της.
* Το επίπεδο των μέτρων ασφάλειας που εφαρμόζονται σε κάθε στοιχείο του ενεργητικού πρέπει να είναι ίσο ή υψηλότερο από το επίπεδο των μέτρων ασφάλειας που εφαρμόζονται για τα δεδομένα που επεξεργάζονται από το στοιχείο ενεργητικού.
* Κάθε στοιχείο ενεργητικού πρέπει να επισημαίνεται σύμφωνα με το επίπεδο διαβάθμισης του.
* Ο [Όνομα Οργανισμού] πρέπει να αναφέρει της προδιαγραφές ασφάλειας των στοιχείων ενεργητικού πριν την προμήθεια τους.
* Ανά επίπεδο κρισιμότητας στοιχείου ενεργητικού, πρέπει να καθορίζονται οι ελάχιστες διαδικασίες συντήρησης τους.
* Τουλάχιστον σε ετήσια βάση θα πρέπει να διενεργείται έλεγχος για την αναγνώριση κατά πόσο το σχέδιο διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού εφαρμόζεται ορθά και αποτελεσματικά. Από τον έλεγχο πρέπει να προκύπτει επίσης κατά πόσο υπάρχουν επαρκείς πόροι (άνθρωποι, εξοπλισμός, εργαλεία, χρήματα κ.α.) για την αποτελεσματική λειτουργία του σχεδίου.
* Διασφάλιση ότι πριν ο εξοπλισμός επαναχρησιμοποιηθεί ή ολοκληρώσει τον κύκλο ζωής του, τα δεδομένα καταστρέφονται με τα κατάλληλα μέτρα ασφαλείας.
* Ο [Όνομα Οργανισμού] διατηρεί κατάλογο (μητρώο) καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίζει ότι έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες) που διατηρεί είτε εντός είτε εκτός του [Όνομα Οργανισμού] (π.χ. σε τρίτα μέρη).
* Ο κατάλογος (μητρώο) ο οποίος καταρτίστηκε για καταγραφή των στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του [Όνομα Οργανισμού], καταγράφει τις εξαρτήσεις και αλληλεξαρτήσεις μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο θα πραγματοποιηθεί η εκτίμηση κινδύνου. Μια σαφής εικόνα του πλαισίου του [Όνομα Οργανισμού] επιτρέψει τον εντοπισμό των κινδύνων εντός του οργανισμού σύμφωνα με το [RM2] της Απόφασης Κ.Δ.Π 389/2020.
* Για κάθε στοιχείο ενεργητικού του [Όνομα Οργανισμού] πρέπει να έχει οριστεί ένας ιδιοκτήτης. Ο Ιδιοκτήτης δύναται να προσδιορίσει και το επίπεδο κρισιμότητας του κάθε στοιχείου ενεργητικού.

Η ύπαρξη ενός αναγνωρισμένου ιδιοκτήτη του καταλόγου διασφαλίζει την ορθή, συστηματική και ασφαλή διαχείριση των πληροφοριακών καταλόγων εντός του [Όνομα Οργανισμού]. Ένας ιδιοκτήτης καταλόγου πρέπει να :

* + έχει καθορισμένες αρμοδιότητες και ευθύνες για την τήρηση, επικαιροποίηση και ασφάλεια των δεδομένων του καταλόγου.
  + ενημερώνεται για τις αλλαγές στις πολιτικές και διαδικασίες που αφορούν τη διαχείριση των πληροφοριακών στοιχείων ενεργητικού του καταλόγου.
  + συνεργάζεται με διάφορα τμήματα του [Όνομα Οργανισμού], όπως το Τμήμα Πληροφορικής για εφαρμογή μέτρων ασφαλείας για την προστασία του στοιχείου στο οποίο είναι υπεύθυνος.
  + Ο ιδιοκτήτης μπορεί να αναθέσει την παρακολούθηση του καταλόγου για επικαιροποίηση του, για την εφαρμογή των δικλείδων ασφαλείας καθώς και για την καταστροφή πληροφορίας / συστήματος αλλά παραμένει διοικητικά υπεύθυνος για την ορθή εφαρμογή των πιο πάνω καθ’ όλη τη διάρκεια της ζωής της πληροφορίας / του συστήματος.
* Στον κατάλογο πρέπει να συμπεριλαμβάνονται κατ’ ελάχιστον η περιγραφή της αποδεκτής χρήσης της λειτουργίας και της τοποθεσίας των στοιχείων, προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών, καθώς και οι αλληλεξαρτήσεις μεταξύ των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών σύμφωνα με το [AM3] της Απόφασης Κ.Δ.Π 389/2020. Επίσης πρέπει να περιλαμβάνει πληροφορίες σχετικές με την ανάκτηση του στοιχείου ενεργητικού σε περίπτωση της καταστροφής ή της αλλοίωσης ή και απώλειας του.
* Όλα τα στοιχεία ενεργητικού πρέπει να ανιχνεύονται, να προσδιορίζονται και να απογράφονται. Όπου είναι δυνατό ο [Όνομα Οργανισμού] πρέπει να χρησιμοποιεί αυτόματο σύστημα για την αναγνώριση και καταγραφή στοιχείων ενεργητικού και συστημάτων εντός αλλά και εκτός του [Όνομα Οργανισμού].
* Ο κατάλογος να επιτρέπει επίσης στον [Όνομα Οργανισμού] να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία θα πρέπει να εφαρμόζει και να διατηρεί μέτρα ασφάλειας πληροφοριών, τουλάχιστον με χειροκίνητο τρόπο σύμφωνα με το [ΑΜ2] της Απόφασης Κ.Δ.Π 389/2020.
* Όπου εφαρμόζεται ο [Όνομα Οργανισμού] διατηρεί κατάλογο με μη εξουσιοδοτημένες εφαρμογές και κατηγορίες εκτελέσιμων αρχείων και διασφαλίζεται ότι απαγορεύεται η εκτέλεση τους στα στοιχεία του οργανισμού (application blacklisting).
* Όπου είναι δυνατό, τα στοιχεία που εξάγονται από το αυτόματο σύστημα αναγνώρισης, συμπληρώνονται με στοιχεία διαδικασιών και δημιουργείται αποτύπωση των σχετικών εξαρτήσεων και αλληλεξαρτήσεων με όσο περισσότερο αυτοματοποιημένο τρόπο γίνεται.
* Ο εν λόγω κατάλογος επικαιροποιείται σε τακτά χρονικά διαστήματα (τουλάχιστο σε ετήσια βάση) και περιλαμβάνει:
  + την πληροφορία / σύστημα πληροφορικής
  + την ηλεκτρονική / φυσική τοποθεσία του
  + τον ιδιοκτήτη
  + το ενδεικνυόμενο επίπεδο ασφάλειας του

διασφαλίζοντας με την εφαρμογή των προνοιών που αφορούν το κάθε επίπεδο, την αποτελεσματική προστασία της πληροφορίας / συστήματος.

Η απογραφή στοιχείων ενεργητικού θα γίνεται μέσα στο «Asset Based Risk Assessment Workbook».

# Πολιτική καταγραφής και παρακολούθησης στοιχείων ενεργητικού

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί δυνατότητες παρακολούθησης των στοιχείων ενεργητικού (ορισμός του στόχου της παρακολούθησης και των στοιχείων που θα υπόκεινται σε παρακολούθηση) βάσει του [ΑΜ3] της Απόφασης 389/2020, ώστε να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών (εφαρμογή αλγορίθμων και μηχανισμών παρακολούθησης για την ανίχνευση ανωμαλιών στα στοιχεία ενεργητικού).

# Καθορισμός Παραμέτρων καταγραφής και παρακολούθησης

Ο [Όνομα Οργανισμού] καταγράφει και να παρακολουθεί την δραστηριότητα που σχετίζεται με την ασφάλεια σε όλα τα συστήματά του, και κατ’ ελάχιστο, στα κρίσιμα στοιχεία ενεργητικού του. Μέσα σε αυτά τα πλαίσια:

* Όλα τα στοιχεία ενεργητικού πρέπει να συγχρονίζονται στο ίδιο δικτυακό ρολόι μέσω χρήσης Network Time Protocol (NTP).
* Τα αρχεία καταγραφής πρέπει να προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή διαγραφή.
* Η διαχείριση των ενεργειών καταγραφής και παρακολούθησης πρέπει να έχει ανατεθεί σε ένα υποσύνολο χρηστών με λογαριασμούς αυξημένων προνομίων.
* Με αυτόν τον τρόπο, εξασφαλίζεται η αποτελεσματική παρακολούθηση, αντίδραση σε ανωμαλίες και την ασφάλεια των στοιχείων ενεργητικού του οργανισμού.
* Σε περίπτωση που εντοπιστούν ανωμαλίες κατά την διάρκεια της παρακολούθησης των δραστηριοτήτων στα στοιχεία ενεργητικού πρέπει να ενεργοποιούνται διαδικασίες διαχείρισης συμβάντων και περιστατικών.
* Τα αποτελέσματα της παρακολούθησης (logs) περιέχουν κατ’ ελάχιστο τις ακόλουθες πληροφορίες:
  + ημερομηνία,
  + ώρα,
  + Εμπλεκόμενα στοιχεία ενεργητικού (IP διεύθυνση πηγής, IP διεύθυνση του συμβάντος προορισμού)
  + τύπος καταγραφής
  + και όποια άλλη πληροφορία μπορεί να δοθεί επιπλέον ως επεξήγηση.
* Για κάθε στοιχείο ενεργητικού, ο [Όνομα Οργανισμού] πρέπει να έχει προσδιορίσει το είδος της παρακολούθησης, την έκταση, το χρονικό διάστημα διατήρησης των αρχείων καταγραφής καθώς και την τοποθεσία αποθήκευσης των αρχείων καταγραφής όπως αναλύεται πιο κάτω:
  + **Είδος Παρακολούθησης:**

Καθορισμός του είδους παρακολούθησης ανά στοιχείο ενεργητικού (π.χ., System, Security, Application).

Προσδιορισμός των συγκεκριμένων παραμέτρων παρακολούθησης για κάθε είδος (π.χ., συστημικά γεγονότα, ασφάλεια, εφαρμογές).

* + **Έκταση Παρακολούθησης:**

Καθορισμός της έκτασης της παρακολούθησης σε επίπεδο γεγονότος.

Καταγραφή διαφόρων τύπων γεγονότων (π.χ., audit success, audit failure, login success, object access success, warning).

* + **Χρονικό Διάστημα Διατήρησης:**

Καθορισμός του χρονικού διαστήματος διατήρησης των σχετικών εγγραφών.

Κατά προτίμηση, ορισμός συγκεκριμένου χρονικού διαστήματος (π.χ., 3 μήνες) για την αποθήκευση των logs.

* + **Τοποθεσία Αποθήκευσης:**

Καθορισμός της τοποθεσίας αποθήκευσης των logs.

Επιλογή ανάμεσα σε ενσωματωμένη αποθήκευση στη συσκευή, αποθήκευση σε syslog server, ή άλλο αποθηκευτικό μέσο.

* + **Διαχείριση Παραμέτρων:**

Υλοποίηση διασφαλίζοντας ότι οι παράμετροι παρακολούθησης είναι ενημερωμένοι και ανταποκρίνονται στις ανάγκες του οργανισμού.

* Ο [Όνομα Οργανισμού] διασφαλίζει ότι καταγράφονται τα ακόλουθα:
  + Πρόσβαση σε αρχεία και διεργασίες των στοιχείων ενεργητικού (χωρίς να είναι ορατό το password ή άλλο μυστικό στοιχείο αυθεντικοποίησης
  + Αποτυχημένες προσπάθειες εκτέλεσης αρχείων
  + Χρήση ή απόπειρα χρήσης αυξημένων προνομίων
  + Δικτυακές κινήσεις και αιτήματα HTTP και DNS
  + Μεταφορές δεδομένων από και προς αφαιρούμενα αποθηκευτικά μέσα.
  + Αλλαγές στην παραμετροποίηση των στοιχείων
  + Αλλαγές σε λογαριασμούς και σε πολιτικές ασφάλειας στοιχείων ενεργητικού
  + Αλλαγή κωδικού πρόσβασης σε λογαριασμούς προνομιακής πρόσβασης
  + Δημιουργία λογαριασμών προνομιακής πρόσβασης
  + Σύνδεση σε στοιχεία ενεργητικού από τοποθεσία που δεν έχει προβλεφθεί
  + Αποτυχημένες προσπάθειες πρόσβασης σε σύντομο χρονικό διάστημα
  + Διενέργεια σάρωσης δικτύου
  + Δημιουργία DHCP εντός δικτύου του [Όνομα Οργανισμού]
  + Διενέργεια αλλαγών σε αρχεία καταγραφής, συμπεριλαμβανομένης και της διαγραφής τους ή της απενεργοποίησης της σχετικής ικανότητας
* Ο [Όνομα Οργανισμού] πρέπει να έχει ορίσει τουλάχιστον δύο (2) πηγές δικτυακού ρολογιού ώστε να εξασφαλίζει ότι τα στοιχεία ενεργητικού έχουν σωστή χρονοσήμανση.
* Όπου είναι δυνατό, τα δεδομένα της παρακολούθησης πρέπει να ανασκοπούνται ημερησίως με χειροκίνητο ή ημιαυτόματο τρόπο με σκοπό την αναγνώριση πιθανών ανωμαλιών, τάσεων, επερχόμενων επιθέσεων ή πραγματικών επιθέσεων.
* Ο [Όνομα Οργανισμού] πρέπει να διασφαλίζει ότι οποιαδήποτε διακοπή στις διαδικασίες καταγραφής και παρακολούθησης αντιμετωπίζεται ως περιστατικό ασφάλειας.
* Σε περίπτωση που οι δυνατότητες παρακολούθησης αποτυγχάνουν, τότε πρέπει να λαμβάνονται κατάλληλες ενέργειες ώστε να τίθεται εκτός λειτουργίας το συγκεκριμένο στοιχείο μέχρις ότου διερευνηθεί πλήρως ο λόγος της αποτυχίας (δεν εφαρμόζεται για στοιχεία τα οποία έχουν άμεση σχέση με την διαχείριση της ασφάλειας).
* Οι σχετικές καταγραφές πρέπει να διατηρούνται για τουλάχιστον 3 μήνες ανά σύστημα. Σε περίπτωση που αυτό δεν είναι τεχνικά εφικτό, πρέπει να υπάρχει ένας μηχανισμός για τη δημιουργία εξαίρεσης από τη σχετική πολιτική.
* Η αίτηση για εξαίρεση πρέπει να αναφέρει τους τρόπους με τους οποίους ο σχετικός κίνδυνος μειώνεται μέσω άλλων αντισταθμιστικών μέτρων και η έγκριση της εξαίρεσης πρέπει να ακολουθεί την διαδικασία ελέγχου αλλαγών.

# Ασφαλής απόσυρση ή επαναχρησιμοποίηση στοιχείων ενεργητικού

Στοιχείο ενεργητικού του [Όνομα Οργανισμού] το οποίο περιέχει ευαίσθητες πληροφορίες, προσωπικά δεδομένα ή / και άδειες χρήσης λογισμικού είναι απαραίτητο να ελέγχεται πριν την απόσυρση του ότι αυτά έχουν αφαιρεθεί με ασφαλή τρόπο.

Η απόφαση για επιδιόρθωση ή απόσυρση κατεστραμμένου στοιχείου ενεργητικού, το οποίο περιέχει διαβαθμισμένες πληροφορίες και ευαίσθητα δεδομένα είναι απαραίτητο να αξιολογείται ως προς τον κίνδυνο για την ασφάλεια των πληροφοριών.

Διαδικασία διαχείρισης στοιχείων ενεργητικού όπως αναφέρθηκε πιο πάνω, υπάρχει μια καταγεγραμμένη διαδικασία η οποία περιγράφει τον τρόπο με τον οποίο διαχειρίζονται τα στοιχεία ενεργητικού κατά τη διάρκεια του κύκλου ζωής τους. Η συγκεκριμένη διαδικασία περιλαμβάνει ενέργειες που διενεργούνται από σχετικά εξουσιοδοτημένους ρόλους για την: προμήθεια (ορίζονται οι κατηγορίες ενεργητικού και οι απαιτήσεις ασφάλειας πληροφοριών), την εγκατάσταση (καθορίζονται οι απαραίτητες προετοιμασίες για την εγκατάσταση και πραγματοποιείται η επαλήθευσή τους), τη συντήρηση (καθορίζεται το πρόγραμμα συντήρησης για το ενεργητικό, περιλαμβάνονται περιοδικοί έλεγχοι και ενημερώσεις για την ασφάλεια, εφαρμόζονται τακτικές ενημερώσεις λογισμικού και αναβαθμίσεις εξοπλισμού, βεβαιώνεται η συμβατότητα τους με τις πολιτικές ασφαλείας, παρακολουθούνται συνεχώς οι ενδείξεις προβλημάτων και η άμεση επίλυσή τους) και τη διάθεση (πραγματοποιείται καταγραφή των δεδομένων και αποτελεσμάτων πριν από τη διάθεση).

Στα πλαίσια της διαδικασίας αυτής, περιλαμβάνονται και στοιχεία ασφάλειας πληροφοριών ώστε να διασφαλίζεται ότι η ασφάλεια των πληροφοριών είναι αναπόσπαστο κομμάτι αυτού του κύκλου ζωής, δηλαδή την προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση. Για περισσότερες πληροφορίες μπορείτε να ανατρέξετε στη Πολιτική Προστασίας Δεδομένων.

Αλλαγές στα στοιχεία ενεργητικού γίνονται σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1] της Απόφασης Κ.Δ.Π 389/2020 , για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών. Κατά τον καθορισμό της διαδικασίας διαχείρισης αλλαγών, ο [Όνομα Οργανισμού] προνοεί αιτήσεις αλλαγής, προκειμένου να λαμβάνονται υπόψη οι αλλαγές που ζητούνται από τους συμμετέχοντες. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να επιτρέπει στον [Όνομα Οργανισμού] να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών [βλέπε Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης].

Στα πλαίσια του σχεδίου περιγράφονται και τα κριτήρια που χρησιμοποιεί ο [Όνομα Οργανισμού] προκειμένου να κατανέμει τους πόρους σε κατηγορίες κρισιμότητας. Προδιαγραφές ασφαλείας, κατάλληλες για την επικείμενη χρήση του στοιχείου ενεργητικού προδιαγράφονται πριν την προμήθεια κατά την ετοιμασία των απαιτήσεων (request for proposal (RFP).

# Αναθεώρηση

Τα έγγραφα σχετικά με την Διαχείριση Στοιχείων Ενεργητικού θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] ώστε να διασφαλίζεται ότι παραμένει αποτελεσματική, ασφαλής και ευθυγραμμισμένη με τους οργανωτικούς στόχους. Πιο συγκεκριμένα αυτή δύναται να αναθεωρείτε σε σημαντικές προσθήκες, αναβαθμίσεις ή αφαίρεση υφιστάμενων περιουσιακών στοιχείων, ενσωμάτωση τρίτων προμηθευτών ή παρόχων υπηρεσιών που διαχειρίζονται ή έχουν πρόσβαση σε οργανωτικά περιουσιακά στοιχεία.

Υπενθυμίζεται ότι σε περίπτωση αλλαγών στα στοιχεία ενεργητικού, η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.

# 

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Διαχείριση Στοιχείων Ενεργητικού | AM1 | Διαχείριση του κύκλου ζωής στοιχείων ενεργητικού | Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι ασφαλή καθ’ όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της προμήθειας, της ανάπτυξης, της συντήρησης και της διάθεσης τους. |
| Διαχείριση Στοιχείων Ενεργητικού | AM2 | Καταγραφή των στοιχείων ενεργειακού και ιδιοκτησία | Να διασφαλιστεί ότι τα στοιχεία ενεργητικού καταγράφονται σε κατάλογο και ότι η ιδιοκτησία καθορίζεται με σκοπό την επίτευξη της ιχνηλασιμότητας και της ευθύνης για τα στοιχεία. |
| Διαχείριση στοιχείων ενεργητικού | AM3 | Παρακολούθηση στοιχείων ενεργητικού | Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι υπό παρακολούθηση για επιθέσεις, ανωμαλίες και απειλές κατά της ασφάλειας, προκειμένου να ενεργοποιηθούν οι διαδικασίες για την αντιμετώπιση συμβάντων και περιστατικών. |
| Διαχείριση Στοιχείων Ενεργητικού | AM5 | Κρυπτογραφία | Να διασφαλιστεί η εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των πληροφοριών με την υιοθέτηση κατάλληλων κρυπτογραφικών λύσεων. |
| Διαχείριση Κινδύνων | RM2 | Πλαίσιο | Να καταρτιστεί κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού. |
| Διαχείριση ταυτότητας και πρόσβασης | IAM6 | Ιχνηλασιμότητα και έλεγχος | Να διασφαλιστεί η μη-άρνηση ανιχνευσιμότητας των ενεργειών των χρηστών που εκτελούνται στο  πλαίσιο των οργανωτικών πόρων, ώστε να είναι δυνατή η ανίχνευση και η διερεύνηση εκούσιων ή ακούσιων δραστηριοτήτων που έχουν αρνητικό  αντίκτυπο. |