Όνομα Οργανισμού

Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης |
| **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](#_Toc187833902)

[1.1 Σκοπός 4](#_Toc187833903)

[1.2 Πεδίο Εφαρμογής 4](#_Toc187833904)

[2. Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης 4](#_Toc187833905)

[2.1 Διαχείριση Αλλαγών (Change Management) 5](#_Toc187833906)

[2.2 Διαχείριση Διαμόρφωσης (Configuration Management) 6](#_Toc187833907)

[3. Αναθεώρηση 6](#_Toc187833908)

[4. Αναφορές 7](#_Toc187833909)

[1. Διαδικασία Διαχείρισης Αλλαγών και Διαμόρφωσης 8](#_Toc187833910)

[2. Ρόλοι και αρμοδιότητες 8](#_Toc187833911)

[3. Ενεργοποίηση Συμβάντων 9](#_Toc187833912)

[4. Διαδικασία Διαχείρισης Αλλαγών 10](#_Toc187833913)

[5. Βήματα εκτέλεσης της Διαδικασίας ελέγχου Αλλαγής και Διαμόρφωσης 13](#_Toc187833914)

[5.1. Βήμα 1 13](#_Toc187833915)

[5.2. Βήμα 2 15](#_Toc187833916)

[5.3. Βήμα 3 15](#_Toc187833917)

[5.4. Βήμα 4 16](#_Toc187833918)

[5.5. Βήμα 5 16](#_Toc187833919)

[Παράρτημα 1 – Έντυπα 17](#_Toc187833920)

# Εισαγωγή

## Σκοπός

Η παρούσα Πολιτική περιλαμβάνει ενδεικτικούς όρους για τη συστηματική διαχείριση των αλλαγών και διαμόρφωσης των πόρων και δεδομένων του [Όνομα Οργανισμού] για τη διατήρηση της ασφάλειας, της σταθερότητας και της συμμόρφωσης.

Σκοπός της είναι να διασφαλιστεί ότι οι οποιεσδήποτε αλλαγές στο υλισμικό, το λογισμικό, δικτυακές υποδομές και υπηρεσίες cloud εισάγονται με ελεγχόμενο και συντονισμένο τρόπο στο κύριο κέντρο δεδομένων και στις κρίσιμες διαμορφώσεις του [Όνομα Οργανισμού]. Αυτή η διαδικασία μειώνει την πιθανότητα να εισαχθούν περιττές αλλαγές ή/και να εισαχθούν εξουσιοδοτημένες και μη αλλαγές με ανεξέλεγκτο τρόπο εισάγοντας πιθανά προβλήματα στα πληροφοριακά συστήματα του [Όνομα Οργανισμού].

## Πεδίο Εφαρμογής

Η πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης του [Όνομα Οργανισμού] εφαρμόζεται σε όλες τις αλλαγές και παραμετροποιήσεις που επηρεάζουν τις λειτουργίες, τις διαδικασίες, τα συστήματα και την τεχνολογική υποδομή του [Όνομα Οργανισμού]. Η πολιτική αυτή ισχύει για όλους τους υπαλλήλους, τους συνεργάτες, τους προμηθευτές και τους εξωτερικούς συνεργάτες του [Όνομα Οργανισμού] που συμμετέχουν ή επηρεάζονται από τις αλλαγές αυτές. Η συμμόρφωση με την πολιτική διασφαλίζει ότι όλες οι αλλαγές πραγματοποιούνται με ασφάλεια, αποτελεσματικότητα και με ελάχιστο κίνδυνο για τη σταθερότητα και την ασφάλεια του [Όνομα Οργανισμού].

Αυτή η πολιτική δύναται να εφαρμόζεται για τους ακόλουθους τύπους αλλαγών:

* Εγκατάσταση νέου υλισμικού ή λογισμικού.
* Αναβάθμιση υλισμικού ή λογισμικού.
* Αναδιαμόρφωση, αλλαγή ή αναβάθμιση εγκαταστάσεων π.χ. ρεύμα, δίκτυο
* Τυπική περιοδική συντήρηση
* Αλλαγές διαμόρφωσης που έχουν τη δυνατότητα να επηρεάσουν σημαντικά την υπηρεσία π.χ. τείχος προστασίας, δρομολογητής κ.λπ.

# Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης

Σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] οφείλει να διασφαλίσει ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών, θεσπίζοντας διαδικασίες διαχείρισης αλλαγών για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών. Τηρεί μητρώο των διαμορφώσεων που ισχύουν για τα εν λόγω στοιχεία ενεργητικού.

## Διαχείριση Αλλαγών (Change Management)

Πιο συγκεκριμένα:

* Ο [Όνομα Οργανισμού] διατηρεί και εφαρμόζει διαδικασία σχετικά με τον έλεγχο και την διαχείριση αλλαγών σε Πληροφοριακά Συστήματα και Δεδομένα και να αναθέτει σχετικούς ρόλους και αρμοδιότητες στο προσωπικό.
* Για κάθε αλλαγή πρέπει να υπάρχει κατάλληλη εξουσιοδότηση από τον υπεύθυνο του συστήματος στο οποίο θα υλοποιηθεί η αλλαγή. Η διαδικασία διαχείρισης αλλαγών πρέπει να περιλαμβάνει προβλέψεις και τρόπους χειρισμού για επείγουσες αλλαγές.
* Για κάθε αλλαγή πρέπει να πραγματοποιείται αξιολόγηση των κινδύνων που θα επιφέρει η αλλαγή. Ανάλογα με τον βαθμό κρισιμότητας έχουν καθοριστεί ελάχιστα μέτρα ασφάλειας που θα πρέπει να εφαρμοστούν σε όλο τον κύκλο διαχείρισης της αλλαγής.
* Για κάθε αλλαγή πραγματοποιούνται κατάλληλες δοκιμές ελέγχου. Η οποιαδήποτε αλλαγή σε περιπτώσεις κρίσιμων συστημάτων πρέπει να γίνεται αποκλειστικά σε δοκιμαστικό περιβάλλον.
* Για κάθε αλλαγή πρέπει να περιλαμβάνεται σχέδιο roll-back για τις περιπτώσεις που οι αλλαγές είναι ανεπιτυχείς ή έχει προκύψει κάποιο γεγονός που δεν επιτρέπει την επιτυχή ολοκλήρωση της αλλαγής.
* Η υλοποίηση της διαδικασίας διαχείρισης αλλαγών πρέπει να πραγματοποιείται μέσω εργαλείου που επιτρέπει την ιχνηλάτηση των αλλαγών.
* Ο [Όνομα Οργανισμού] εδραιώνει την αξιολόγηση κινδύνου των αιτημάτων και τον σχεδιασμό αλλαγών με βάση τα κατάλληλα μέτρα ασφαλείας, αξιοποιώντας τη διαδικασία διαχείρισης αλλαγών και αιτημάτων αλλαγής, με σκοπό τη δημιουργία κατηγοριών αλλαγών.
* Όπου είναι δυνατό, συστήνεται η ύπαρξη σχετικής επιτροπής για τον έλεγχο και την έγκριση των αλλαγών, για την εξασφάλιση μη συγκρουόμενων συμφερόντων ανάμεσα στα άτομα που αιτούνται την αλλαγή, υλοποιούν την αλλαγή και εγκρίνουν την αλλαγή κυρίως σε περιπτώσεις κρίσιμων συστημάτων.
* Δοκιμές πρέπει να πραγματοποιούνται στην εφαρμογή της διαδικασίας διαχείρισης αλλαγών ώστε να βεβαιώνεται ότι οι αλλαγές κρίσιμων συστημάτων γίνονται πάντα με προκαθορισμένο τρόπο, αλλά και τακτικές ανασκοπήσεις για τον έλεγχο τήρησης της διαδικασίας.
* Ο [Όνομα Οργανισμού] καθορίζει και καταγράφει τις σχέσεις ανάμεσα στις διαμορφώσεις των στοιχείων ενεργητικού με σκοπό τον προσδιορισμό των αλληλεξαρτήσεων και τη διασφάλιση της κατάλληλης διαχείρισης της αλλαγής όσον αφορά την τροποποίηση των διαμορφώσεων [CM2].

## Διαχείριση Διαμόρφωσης (Configuration Management)

Η διαχείριση διαμόρφωσης επικεντρώνεται στην καθιέρωση, διατήρηση και παρακολούθηση ασφαλών βασικών διαμορφώσεων σε όλα τα περιουσιακά στοιχεία πληροφορικής του [Όνομα Οργανισμού], συμπεριλαμβανομένου του υλισμικού, του λογισμικού, των δικτύων υποδομών και των περιβαλλόντων cloud. Η διαχείριση διαμόρφωσης συνδέεται άμεσα με τη διαχείριση αλλαγών, καθώς παρέχει τη βάση για τον εντοπισμό και την αξιολόγηση των επιπτώσεων των αλλαγών σε θέματα ασφάλεια πληροφοριών καθώς της λειτουργικής σταθερότητα.

Στα πλαίσια της Διαχείρισης Διαμόρφωσης ο [Όνομα Οργανισμού] :

* Διατηρεί ένα μητρώο στοιχείων ενεργητικού, που υποχρεωτικά πρέπει να διαθέτει εγγραφές για τα ακόλουθα:
  + α) registry settings
  + β) permission settings σε επίπεδο αρχείων, φακέλων αλλά και άλλων πόρων
  + γ) ρυθμίσεις που σχετίζονται με ανοικτές θύρες, ενεργοποιημένες ή αποκλεισμένες υπηρεσίες ή πρωτόκολλα, επιτρεπτές ή αποκλεισμένες συνδέσεις, καθώς και οποιαδήποτε άλλη σχετική ρύθμιση που επηρεάζει την ασφάλεια ή τη λειτουργικότητα του συστήματος ή της υπηρεσίας.
* Προβλέπεται η δημιουργία αντιγράφου ασφαλείας της παραμετροποίησης του στοιχείου και η αποθήκευσή του σε ασφαλές σημείο, με σαφή αναφορά στην αντίστοιχη αλλαγή.
* Πρέπει να πραγματοποιούνται επιθεωρήσεις με άξονα την πληρότητα και την ακεραιότητα των αλλαγών που έχουν υλοποιηθεί.
* Οι διαμορφώσεις των Πληροφοριακών Συστημάτων (κυρίως των κρίσιμων) προστατεύονται με το ανώτερο επίπεδο διαβάθμισης του Οργανισμού.

Όπου είναι δυνατό θα πρέπει να χρησιμοποιούνται αυτοματοποιημένα εργαλεία για την επαλήθευση των βασικών διαμορφώσεων των στοιχείων ενεργητικού, ώστε να εντοπίζονται μη εξουσιοδοτημένες αλλαγές.

# Αναθεώρηση

Τα έγγραφα σχετικά με την Διαχείριση Αλλαγών και Διαμόρφωσης θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] (π.χ. τις επιχειρηματικές δραστηριότητες και τις τάσεις της αγοράς, κανονιστικές απαιτήσεις και τις απαιτήσεις συμμόρφωσης, την εφαρμογή νέων συστημάτων, τους νέους κινδύνους, τις αναδυόμενες απειλές κλπ.).

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Διαχείριση Αλλαγών | CM1 | Διαχείριση αλλαγών | Να διασφαλιστεί ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών. |
| Διαχείριση Αλλαγών | CM2 | Διαχείριση διαμόρφωσης (configuration) | Να εντοπίζονται, να διατηρούνται και να επαληθεύονται οι πληροφορίες για τα στοιχεία ενεργητικού και τις διαμορφώσεις του οργανισμού. |

*Σημείωση: το πιο κάτω μέρος αφορά τη Διαδικασία Διαχείρισης Αλλαγών και Διαμόρφωσης που σκοπό έχει την υποστήριξη της Πολιτικής που καταγράφεται στις πιο πάνω παραγράφους. Η διαδικασία συστήνεται να είναι σε ξεχωριστό έγγραφο από τη Πολιτική.*

# Διαδικασία Διαχείρισης Αλλαγών και Διαμόρφωσης

Κατά τη διαδικασία αλλαγής, οποιαδήποτε παραμετροποίηση που αφορά το στοιχείο ενεργητικού θα υπόκειται σε αντιγραφή ασφαλείας. Τα αντίγραφα ασφαλείας των παραμετροποιήσεων του στοιχείου ενεργητικού θα αποθηκεύονται σε προστατευμένο σημείο, εξασφαλίζοντας την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών. Οι διαδικασίες αποθήκευσης και επαναφοράς των παραμετροποιήσεων θα υπόκεινται σε τακτικούς ελέγχους ασφαλείας και επανάκτησης.

Κατά τον καθορισμό της διαδικασίας διαχείρισης αλλαγών, θα πρέπει να ετοιμάζονται αιτήσεις διαχείρισης 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 σύμφωνα με το CM1 της Απόφασης Κ.Δ.Π 389/2020.

# Ρόλοι και αρμοδιότητες

Η αποτελεσματική εφαρμογή μιας Πολιτικής Διαχείρισης Αλλαγών και Διαμόρφωσης βασίζεται στην ξεκάθαρη ανάθεση ρόλων και αρμοδιοτήτων. Αυτοί οι ρόλοι διασφαλίζουν τη λογοδοσία, την ασφαλή εκτέλεση και την ευθυγράμμιση με τους εκάστοτε επιχειρησιακούς στόχους του [Όνομα Οργανισμού]. Παρακάτω καταγράφονται οι βασικοί ρόλοι και οι αρμοδιότητές τους:

**Χρήστης**: Άτομο που εκκινεί τη διαδικασία αιτήματος αλλαγής μέσω υποβολής αιτημάτων αλλαγής, κατά περίπτωση. Είναι υπεύθυνος για την τεκμηρίωση του αιτήματος αλλαγής και την καταγραφή των αναγκών αλλά και των επιχειρηματικών πλεονεκτημάτων που θα επιφέρει η αλλαγή. Επιπρόσθετα είναι πιθανό να κάνει αναφορά θεμάτων ή πιθανών προβλημάτων ασφαλείας πληροφορικών που σχετίζονται με διάφορες διαμορφώσεις σε στοιχεία ενεργητικού του [Όνομα Οργανισμού].

**Υπεύθυνο άτομο Λογιστηρίου**: Υπεύθυνος για την εξέταση και την έγκριση αιτημάτων κυρίως μεγάλης κλίμακας πριν αυτά προωθηθούν στο οικείο Τμήμα Πληροφορικής εφόσον προκύπτει ανάγκη χρηματικής αποζημίωσης για τη διεκπεραίωση της αλλαγής.

**Υπεύθυνος άτομο Πληροφορικής (ΔΠ)**: Υπεύθυνος για τη διενέργεια ανάλυσης κινδύνου και την τεκμηρίωση των γεγονότων που δικαιολογούν την έγκριση/απόρριψη ενός αιτήματος.

**Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων/δικτύου/υπηρεσιών cloud**: Υπεύθυνος για την τεχνική αξιολόγηση του αιτήματος αλλαγής και τη συνέχιση είτε με την έγκριση είτε την απόρριψη.

**Τεχνικοί πληροφορικής**: Υπεύθυνοι για την υλοποίηση των αιτημάτων που αφορούν κρίσιμες διαμορφώσεις υλισμικού/λογισμικού-συστημάτων/δικτύου/υπηρεσιών cloud κατόπιν οδηγιών.

**Προγραμματιστές συστημάτων**: Υπεύθυνοι για την εφαρμογή των αλλαγών λογισμικού που αφορούν στα Συστήματα που χρησιμοποιεί ο [Όνομα Οργανισμού].

**Υποσημείωση:** Ο κάθε οργανισμός δύναται να καθορίσει μόνο τους ρόλους οι οποίοι ευθυγραμμίζονται με τις ανάγκες και την δομή του και να απαλείψει τους ρόλους οι οποίοι δεν εφαρμόζονται σε κάθε περίπτωση. Επιπρόσθετα, ανάλογα με το μέγεθος του κάθε οργανισμού, θα υπάρχουν περιπτώσεις κατά τις οποίες δεν θα είναι εφικτός ο διορισμός ξεχωριστών ατόμων για τον κάθε ρόλο. Σε μια τέτοια περίπτωση ο οργανισμός δύναται να καθορίσει πέραν του ενός ρόλου σε ένα άτομο, νοουμένου ότι δεν θα προκύπτει σύγκρουση συμφέροντος μεταξύ των ρόλων αυτών.

# Ενεργοποίηση Συμβάντων

Η διαδικασία διαχείρισης αλλαγών δύναται να ενεργοποιηθεί στις ακόλουθες περιπτώσεις:

• Περιστατικό ασφάλειας πληροφοριών / κυβερνοασφάλειας,

• Εγκατάσταση νέου υλισμικού (Hardware),

• Νέα λειτουργία/ λειτουργικότητα,

• Αναβάθμιση πληροφοριακών υποδομών συμπεριλαμβανομένων υπηρεσιών cloud,

• Εγκατάσταση τεχνικών επιδιορθώσεων,

• Νέα ή τροποποιημένη νομοθεσία,

• Νέες/Τροποποιημένες επιχειρησιακές ανάγκες ή νέα κατεύθυνση του [Όνομα Οργανισμού],

• Απόσυρση συγκεκριμένης υπηρεσίας/λειτουργικότητας,

• Παρακολούθηση συμβάντος (υπέρβαση του ορίου υπηρεσίας) –Capacity Management,

• Υλοποίησης ή/και εγκατάσταση νέας εφαρμογής/ λογισμικού

# Διαδικασία Διαχείρισης Αλλαγών

Τα ακόλουθα βήματα ακολουθούνται για τη διαδικασία διαχείρισης αλλαγών:

|  |  |  |  |
| --- | --- | --- | --- |
| No | Κύρια Βήματα | Αρμοδιότητα | Σημειώσεις/Αναφορές |
| 1 | **Δημιουργία Αιτήματος Αλλαγής (AA)** | Χρήστης που υποβάλλει το ΑΑ | Δημιουργία ενός ΑΑ που καταγράφει λεπτομερώς όλες τις απαιτούμενες πληροφορίες σε σχέση με την απαιτούμενη αλλαγή.    Με την ολοκλήρωση του βήματος 1, προχωρήστε στο Βήμα 2. |
| 2 | **Έλεγχος του Αιτήματος Αλλαγής (ΑΑ) για πληρότητα** | Υπεύθυνος άτομο Πληροφορικής (ΔΠ) & Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων /δικτύου/υπηρεσιών cloud | Επιβεβαίωση ότι το αίτημα αλλαγής περιλαμβάνει τις απαιτούμενες πληροφορίες.  Η αλλαγή θα πρέπει να απορριφθεί / επιστραφεί εάν είναι:  1.Πλήρως ανέφικτο (Προχωρήστε στο βήμα 13 για κλείσιμο του ΑΑ).  2. Ένα αίτημα διπλής αλλαγής (Προχωρήστε στο βήμα 13 για κλείσιμο του ΑΑ).  3. Ημιτελής  Με την ολοκλήρωση του βήματος, Προχωρήστε στο Βήμα 3. |
| 3 | **Τροποποίηση ΑΑ εφόσον είναι αναγκαίο** | Εκείνος που υποβάλλει το ΑΑ | Η προσθήκη περαιτέρω πληροφοριών εάν απαιτείται ή αποσαφήνιση των υπαρχουσών πληροφοριών.  Με την ολοκλήρωση του βήματος, προχωρήστε στο Βήμα 4. |
| 4 | **Κατηγοριοποίηση και Αξιολόγηση ΑΑ** | Υπεύθυνος άτομο Πληροφορικής(ΔΠ) & Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων /δικτύου/υπηρεσιών cloud | Αξιολόγηση εάν το ΑΑ πρόκειται για «Σημαντική» αλλαγή, «Κανονική» αλλαγή ή αλλαγή έκτακτης ανάγκης.  Με την ολοκλήρωση του βήματος, προχωρήστε στο Βήμα 5. |
| 5 | **Αξιολόγηση, έγκριση, απόρριψη ή αναφορά του αιτήματος αλλαγής** | Υπεύθυνος άτομο Πληροφορικής(ΔΠ), Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων /δικτύου/υπηρεσιώνcloud και Υπεύθυνος Ασφάλειας Πληροφοριών | Αξιολόγηση της επίπτωσης της αλλαγής και των σχετικών πιθανών κινδύνων.  Εάν η αλλαγή κατηγοριοποιηθεί ως «Σημαντική», θα πρέπει να υπάρξει έγκριση από Ανώτατη Διοίκηση κατόπι ενημέρωσης του Υπεύθυνου Ασφάλειας Πληροφοριών.  Για αλλαγές «έκτακτης ανάγκης», δύναται να υπάρξει έγκριση του Διαχειριστή (Δ) ή του Υπεύθυνου Ασφάλειας Πληροφοριών.  «Κανονικές» αλλαγές πρέπει να εγκρίνονται από τους ΔΠ & Δ.  Εάν εγκριθεί, προχωρήστε στο Βήμα 6.  Εάν απορριφθεί, παροχή αιτιολόγησης και προχωρήστε στο βήμα 13 για να ενημερώσετε και να κλείσετε την αλλαγή. |
| 6 | **Χρονο-προγραμματισμός της αλλαγής** | Υπεύθυνος άτομο Πληροφορικής(ΔΠ), Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων /δικτύου/υπηρεσιώνcloud | Ενημερώστε εκείνον που έκανε την αίτηση αλλαγής και προγραμματίστε χρονικά την αλλαγή.  Κατανέμεται την αλλαγή σε διορισμένο τεχνικό πληροφορικής.  Κοινοποιήστε τα στοιχεία αλλαγής σε όλα τα ενδιαφερόμενα μέρη.  Με την ολοκλήρωση του βήματος, προχωρήστε στο Βήμα 7. |
| 7 | **Ενημέρωση τρίτων μερών** | Υπεύθυνος άτομο Πληροφορικής(ΔΠ), Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων /δικτύου/υπηρεσιώνcloud | Αποστείλετε ενημέρωση σε όλα τα ενδιαφερόμενα μέρη με ηλεκτρονικά μέσα (email ή μέσω πλατφόρμας διαχείρισης αλλαγών).  Με την ολοκλήρωση του βήματος, προχωρήστε στο Βήμα 8. |
| 8 | **Ανάπτυξη και δοκιμή αλλαγής (Δοκιμαστικό Περιβάλλον)** | Τεχνικός Τμήματος Πληροφορικής | Ανάπτυξη αλλαγής και δοκιμή, όπου απαιτείται, χρησιμοποιώντας το περιβάλλον δοκιμής.  Με την ολοκλήρωση του βήματος, προχωρήστε στο Βήμα 9. |
| 9 | **Πραγματοποίηση της δοκιμής αποδοχής επιχειρησιακού χρήστη** | Χρήστης που υποβάλλει το ΑΑ | Εάν είναι επιτυχής, προχωρήστε στο Βήμα 10.  Εάν όχι, επιστρέψτε στο Βήμα 9 |
| 10 | **Εγκατάσταση της αλλαγής σε περιβάλλον Παραγωγής** | Τεχνικός Τμήματος Πληροφορικής | Κάντε την αλλαγή την προγραμματισμένη ημερομηνία και ώρα.  Δοκιμάστε για να βεβαιωθείτε ότι έχει λειτουργήσει επιτυχώς στο περιβάλλον παραγωγής .  Εάν είναι επιτυχής, προχωρήστε στο Βήμα 12 για να επικυρώσετε την εφαρμογή.  Εάν δεν είναι επιτυχής, προχωρήστε στο Βήμα 11 για να επαναφέρετε τις αλλαγές. |
| 11 | **Κατάργηση αλλαγής (Rollback)** | Τεχνικός Τμήματος Πληροφορικής | Καταργήστε την αλλαγή εάν δεν είναι επιτυχής (Rollback).  Με την ολοκλήρωση του βήματος, προχωρήστε στο βήμα 12. |
| 12 | **Επιβεβαίωση εγκατάστασης** | Υπεύθυνος άτομο Πληροφορικής(ΔΠ), Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων /δικτύου/υπηρεσιώνcloud | Επιβεβαίωση επιτυχούς εγκατάστασης της αλλαγής.  Επιβεβαίωση επιτυχούς κατάργησης αλλαγής (Rollback).  Με την ολοκλήρωση του βήματος, προχωρήστε στο Βήμα 13. |
| 13 | **Ενημέρωση κατάστασης αλλαγής** | Υπεύθυνος άτομο Πληροφορικής(ΔΠ), Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων /δικτύου/υπηρεσιώνcloud | Ενημερώστε την κατάσταση αλλαγής.  Με την ολοκλήρωση του βήματος, προχωρήστε στο Βήμα 14 |
| 14 | **Κλείσιμο αλλαγής** | Υπεύθυνος άτομο Πληροφορικής(ΔΠ), Διαχειριστής (Δ) υλισμικού/λογισμικού-συστημάτων /δικτύου/υπηρεσιώνcloud | Κλείσιμο της εγγραφής αλλαγής. |

# Βήματα εκτέλεσης της Διαδικασίας ελέγχου Αλλαγής και Διαμόρφωσης

# Βήμα 1

Η απαίτηση προσδιορίζεται και χαρακτηρίζεται είτε ως αίτημα αλλαγής είτε ως αίτημα διαμόρφωσης (βλ. Παράρτημα 1 - Φόρμα αιτήματος αλλαγής και διαμόρφωσης). Καθορίζεται η κλίμακα και ο επείγων χαρακτήρας του αιτήματος. Ο αιτών πρέπει να παράσχει μια σύντομη περιγραφή του αιτήματος, να περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών και να απαριθμήσει τα αναμενόμενα οφέλη από τη στιγμή που το αίτημα γίνει αποδεκτό και υλοποιηθεί. Η φόρμα επιτρέπει επίσης στον αιτούντα να επιλέξει τον τύπο του αιτήματος ως εξής:

Σύμφωνα με τη Διαδικασία Διαχείρισης Αλλαγών, χρησιμοποιούνται οι ακόλουθες κατηγορίες Αλλαγών:

1. Κανονική Αλλαγή
2. Έκτακτη Αλλαγή
3. Σημαντική Αλλαγή

Κάθε μία από αυτές τις κατηγορίες θα απαιτεί διαφορετική διαχείριση ως εξής:

1. Κανονική Αλλαγή

Πρόκειται για "φυσιολογικές" αλλαγές, οι οποίες αναμένεται να είναι η πλειονότητα των αιτημάτων αλλαγών που καταγράφονται και αντιμετωπίζονται μέσω της διαδικασίας διαχείρισης αλλαγών, όπως περιγράφεται σε αυτό το έγγραφο. Αν και δεν είναι καταστάσεις έκτακτης ανάγκης, θα δοθεί προτεραιότητα ώστε οι πόροι να μπορούν να διατεθούν με αποτελεσματικό τρόπο.

1. Έκτακτη Αλλαγή

Ενώ όλες οι αλλαγές που ενδέχεται να απαιτηθούν πρέπει να προβλεφθούν και να προγραμματιστούν, αναμένεται ότι θα υπάρξουν περιπτώσεις στις οποίες οι επιχειρησιακές απαιτήσεις απαιτούν αλλαγές σε κατάσταση έκτακτης ανάγκης. Τέτοιες αλλαγές είναι εκείνα τα αιτήματα που επηρεάζουν εσωτερικά ή εξωτερικά συστήματα τα οποία βρίσκονται σε περιβάλλον «παραγωγής» και απαιτούν επίλυση (ή αποτροπή) ενός τρέχοντος συμβάντος, προβλήματος ή επιχειρηματικής ανάγκης υψηλής προτεραιότητας.

Σε τέτοιες περιπτώσεις, ένα Αίτημα Αλλαγής (AA) πρέπει να τύχει άμεσης προτεραιότητας (ακόμη και αν δεν είναι διαθέσιμα τα πλήρη στοιχεία αλλαγής) και θα πρέπει να υπάρξει ειδοποίηση των ΔΠ & Υπεύθυνου Ασφάλειας Πληροφοριών. Αυτό γίνεται για να διασφαλιστεί ότι όλα τα ενδιαφερόμενα μέρη είναι ενήμερα το συντομότερο δυνατό.

Από την αρχική καταγραφή της αλλαγής, οι βασικές αρχές της διαδικασίας διαχείρισης αλλαγών θα πρέπει να τηρούνται όσο γίνεται περισσότερο, ωστόσο, όλες οι αλλαγές έκτακτης ανάγκης απαιτούν επίσης έγκριση των Διαχειριστών & του Υπεύθυνου Ασφάλειας Πληροφοριών του [Όνομα Οργανισμού]. Όταν μια αλλαγή έκτακτης ανάγκης δεν έχει εγκριθεί πλήρως, θα λαμβάνεται απόφαση από τη Διοίκηση σχετικά με το εάν η αλλαγή θα υλοποιηθεί. Αυτή η απόφαση δύναται να αντικαταστήσει προσωρινά τη πλήρη διαδικασία διαχείρισης αλλαγών.

Εάν μια αλλαγή έκτακτης ανάγκης δεν μπορεί να εγκριθεί επίσημα μετά από εύλογες προσπάθειες για την παρακολούθηση της διαδικασίας (π.χ. εκτός ωρών εργασίας) μπορεί να ληφθεί απόφαση σχετικά με το εάν αυτή η αλλαγή θα υλοποιηθεί. Ωστόσο, οι λεπτομέρειες της αλλαγής πρέπει να καταγράφονται και η διαδικασία διαχείρισης αλλαγών θα διασφαλίζει ότι τα αρχεία διατηρούνται με ακρίβεια και ότι η επιτυχία ή η αποτυχία της αλλαγής μπορεί να αναθεωρηθεί.

1. Σημαντική Αλλαγή

Οι σημαντικές αλλαγές θα καταγράφονται μέσω της διαδικασίας διαχείρισης αλλαγών και θα κοινοποιούνται σε σχετική Επιτροπή Ασφάλειας Πληροφοριών που συστάθηκε στον [Όνομα Οργανισμού] (βλέπε Πολιτική Διακυβέρνησης). Στη συνέχεια θα καταγράφονται ως έργα με δική τους επιχειρησιακή περίπτωση έργου (Project Business Case), ομάδα έργου και προϋπολογισμό.

Ωστόσο, ένα έργο μπορεί να δημιουργήσει περαιτέρω αιτήματα αλλαγών που θα διαχειρίζονται στη διαδικασία διαχείρισης αλλαγών ως κανονικές αλλαγές.

* 1. Πρόγραμμα Αλλαγών

Τηρείτε ένα πρόγραμμα αλλαγών το οποίο εκδίδεται σε εβδομαδιαία ή μηνιαία βάση και σε αυτό δύναται να συμπεριληφθούν οι ακόλουθες πληροφορίες:

• Ημερομηνία και ώρα εγκατάστασης,

• Αναφορά Αλλαγής,

• Περιγραφή Αλλαγής,

• Συστήματα και χρήστες που επηρεάζονται,

• Αναμενόμενη διάρκεια αλλαγής.

* 1. Αναφορά Αλλαγών

Οι ακόλουθες αναφορές εκπονούνται από τους Διαχειριστές/ΔΠ σε τριμηνιαία βάση και θα αναθεωρηθούν από τον Υπεύθυνο Ασφάλειας Πληροφοριών καθώς επίσης θα συζητιούνται στο πλαίσιο των συνεδριάσεων Επιτροπής Ασφάλειας Πληροφορικών προκειμένου να εντοπιστούν οι τάσεις και οι πιθανές βελτιώσεις της διαδικασίας:

• Αριθμός αλλαγών που καταγράφηκαν και έκλεισαν ανά εβδομάδα/ μήνα,

• Κατανομή κατηγοριών αιτημάτων αλλαγής που εγείρονται,

• Μέσος χρόνος επεξεργασίας ενός αιτήματος αλλαγής κάθε κατηγορίας,

• Ποσοστό επιτυχημένων αιτήσεων αλλαγής,

• Πηγές αιτημάτων αλλαγής π.χ. του [Όνομα Οργανισμού],

• Τύποι αιτημάτων αλλαγής π.χ. διακομιστή, δίκτυο ή εφαρμογή.

Ο Διευθυντής Τμήματος πρέπει να εξετάσει το αίτημα και έχει την εξουσία είτε να το απορρίψει είτε να το προωθήσει στο [Αρμόδιο Τμήμα Πληροφορικής].

Όλα τα αιτήματα μεγάλης κλίμακας που μπορεί να οδηγήσουν σε εκτεταμένες αλλαγές στις υπάρχουσες διαδικασίες ή μπορεί να επηρεάσουν τον ετήσιο προϋπολογισμό του [Όνομα Οργανισμού] πρέπει να υποβάλλονται και να εγκρίνονται από τον Προϊστάμενο του [Αρμόδιου Τμήματος Λογιστηρίου] **πριν** από οποιαδήποτε εφαρμογή.

Οι ακόλουθοι ελάχιστοι έλεγχοι ασφαλείας εφαρμόζονται σε περιβάλλοντα ανάπτυξης, δοκιμών και παραγωγής:

* Χρησιμοποιούνται διαφορετικοί λογαριασμοί για πρόσβαση σε περιβάλλοντα μη παραγωγής και παραγωγής (δηλαδή, οι λογαριασμοί παραγωγής δεν θα πρέπει να έχουν πρόσβαση σε περιβάλλοντα μη παραγωγής και οι λογαριασμοί μη παραγωγής δεν θα πρέπει να έχουν πρόσβαση σε περιβάλλοντα παραγωγής).
* Οι λογαριασμοί με λειτουργίες διαχείρισης μπορούν να έχουν πρόσβαση μόνο σε περιβάλλοντα παραγωγής για την εκτέλεση συγκεκριμένων εργασιών.

# Βήμα 2

Το υπεύθυνος άτομο Πληροφορικής (ΔΑ) ή εκπρόσωπος του εκτελεί Ανάλυση Κινδύνων λαμβάνοντας υπόψη τις τρέχουσες διαδικασίες, τις επιπτώσεις στην ασφάλεια των πληροφοριών και την καταχώριση γνωστών και αναγνωρισμένων κινδύνων. Η αξιολόγηση κινδύνου λαμβάνει υπόψη τον απαιτούμενο χρόνο, τους περιορισμούς χρονοδιαγράμματος, τις απαιτήσεις πόρων και τη διαθεσιμότητα πόρων, τις τεχνολογικές δυνατότητες/περιορισμούς, τους απαραίτητους ελέγχους κ.λπ. Οι εντοπισμένοι κίνδυνοι (π.χ. πιθανοί φορείς επίθεσης, περιπτώσεις κατά της χρήσης, απόρρητο και εμπιστευτικότητα) αξιολογούνται και μετριάζονται σε αποδεκτό επίπεδο υπολειπόμενου κινδύνου πριν από την εγκατάσταση σε περιβάλλον παραγωγής. Οι έλεγχοι ασφαλείας σχεδιάζονται με βάση το αποτέλεσμα της αξιολόγησης κινδύνου.

Το υπεύθυνο άτομο Πληροφορικής (ΔΑ) πρέπει επίσης να παρέχει μια σύντομη περιγραφή σύμφωνα με τον λόγο έγκρισης/απόρριψης του αιτήματος.

# Βήμα 3

Όταν ληφθούν όλες οι απαραίτητες εγκρίσεις, η αλλαγή προωθείται στον Διαχειριστή **(Δ) υλισμικού/λογισμικού-συστημάτων/δικτύου/υπηρεσιών cloud** για εφαρμογή μαζί με αντίγραφο της διαμόρφωσης όπου θα καταγράφονται οι σχέσεις ανάμεσα στις διαμορφώσεις των στοιχείων ενεργητικού με σκοπό τον προσδιορισμό αλληλεξαρτήσεων. Ο Διαχειριστής **(Δ) υλισμικού/ λογισμικού-συστημάτων/δικτύου/υπηρεσιών cloud** αξιολογεί το αίτημα και αποφασίζει εάν είναι είτε τεχνικά εφικτό ή μη εφικτό βάσει μιας διαδικασίας αξιολόγησης.

Η διαδικασία αξιολόγησης περιλαμβάνει τα ακόλουθα βήματα:

* Καταχώριση των Συστημάτων που επηρεάζονται από την αλλαγή
* Τεχνική Μελέτη
  + Αναλυτικά οι περιορισμοί και ο τρόπος επίλυσης τους
  + Εκτίμηση των πιθανών επιπτώσεων στην ασφάλεια των πληροφοριών διασφαλίζοντας ότι δεν διακυβεύονται οι υπάρχουσες διαδικασίες ασφάλειας και ελέγχου περεταίρω το αντίγραφο ασφαλείας της παραμετροποίησης του στοιχείου θα αποθηκεύεται σε προστατευμένο σημείο.
  + Πώς θα διασφαλιστεί η διαθεσιμότητα των πόρων
  + Επιπρόσθετα:
    - Σχέδιο εφαρμογής
    - Δοκιμές και σχέδιο επικοινωνίας / δοκιμές αποδοχής εάν απαιτείται
    - Σχέδιο μετριασμού του κινδύνου
    - Σχέδιο επιστροφής

# Βήμα 4

Οι Τεχνικοί Υποδομής / Προγραμματιστές Λογισμικού, χρησιμοποιώντας την τεχνική μελέτη ως κατευθυντήριο μοχλό, υλοποιούν την αλλαγή τεκμηριώνοντας τη διαδικασία στην πορεία και πραγματοποιώντας δοκιμές μονάδας. Μόλις εφαρμοστεί η αλλαγή, το τεχνικό περιβάλλον/λογισμικό ελέγχεται πριν από την αποδοχή της αλλαγής.

# Βήμα 5

Οι εξουσιοδοτημένοι χρήστες είναι υπεύθυνοι για την αποδοχή της αλλαγής πριν μεταφερθεί στην παραγωγή, υπογράφοντας την κατάλληλη ενότητα στη Φόρμα αιτήματος αλλαγής και διαμόρφωσης.

# Παράρτημα 1 – Έντυπα

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ενότητα 1. Αίτηση αιτήματος Αλλαγής & Διαμόρφωσης** | | | | | | |
| Η αίτηση αιτήματος «αλλαγής & διαμόρφωσης» πρέπει να συμπληρωθεί από τον Χρήστη. Μόλις συμπληρωθεί, το έντυπο θα πρέπει να προωθηθεί στον αρμόδιο Διευθυντή Τμήματος για αξιολόγηση και έγκριση. | | | | | | |
| 1. **Τύπος Αιτήματος** | | | | | | |
| **Αίτημα Αλλαγής** | | 🞏 | | **Αίτημα Διαμόρφωσης** | | 🞏 |
| 1. **Τύπος Αλλαγής / Διαμόρφωσης Μεγάλης Κλίμακας\* Μεσαίας Κλίμακας Μικρής Κλίμακας** | | | | | | |
| **Έκτακτη (Επείγουσα)** 🞏 | | 🞏 🞏 🞏 | | | | |
| **Σημαντική** 🞏 | | 🞏 🞏 🞏 | | | | |
| **Κανονική** 🞏 | | 🞏 🞏 🞏 | | | | |
| **Λεπτομέρειες αλλαγής ή διαμόρφωσης (Δώστε μια σύντομη περιγραφή):** | | | | | | |
| **Επιχειρηματικά οφέλη από την αλλαγή ή τη διαμόρφωση:** | | | | | | |
| **Χρήστης (Ονοματεπώνυμο):** | | | | | | |
| **Τμήμα** |  | | **Υπογραφή:** | |  | |
| **Διευθυντής Τμήματος (Ονοματεπώνυμο):** | | | **Ονοματεπώνυμο:** | | **Υπογραφή:** | |
| **Ημερομηνία:** |  | | **Email :** | |  | |
| **Τελική έγκριση μετά την ολοκλήρωση της Αλλαγής/Διαμόρφωσης** | | | | | | |
| **Υπογραφή:** |  | | **Ημερομηνία** | |  | |
| **Σχόλια** |  | | | | | |

\*Για αλλαγές μεγάλης κλίμακας απαιτούνται εγκρίσεις από τον Προϊστάμενο του Τμήματος Λογιστηρίου του [Όνομα Οργανισμού]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ενότητα Β. Αξιολόγηση αιτήματος Αλλαγής & Διαμόρφωσης** | | | | |
| H. η Αίτηση Αλλαγής & Διαμόρφωσης πρέπει να συμπληρωθεί από τον Χρήστη. Μόλις συμπληρωθεί, το έντυπο θα πρέπει να προωθηθεί στο Υπεύθυνο άτομο Πληροφορικής (ΔΑ) για αξιολόγηση. | | | | |
| 1. **Αξιολόγηση Αιτήματος** | | | | |
| Το αίτημα αλλαγής ή διαμόρφωσης: | | | | |
| **Εγκρίθηκε :** | 🞏 | **Απορρίφθηκε:** | | 🞏 |
| 1. **Αιτιολόγηση** | | | | |
| **Αιτιολόγηση έγκρισης/απόρριψης:** | | | | |
| 1. **Risks** | | | | |
| **Γνωστοί και αναγνωρισμένοι κίνδυνοι:** | | | | |
| **Υπεύθυνο Άτομο Πληροφορικής (ΔΑ) (Ονοματεπώνυμο):** | | | **Υπογραφή:** | |
| **Τμήμα:** | | |  | |
| **Ημερομηνία:** | | |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ενότητα Γ. Τεχνικός Σχεδιασμός αίτησης Αλλαγής και Διαμόρφωσης** | | | | | | |
| Η ενότητα «Γ. Τεχνικός Σχεδιασμός» πρέπει να συμπληρωθεί από τους αρμόδιους Διαχειριστές (Δ) υλισμικού/ λογισμικού-συστημάτων/δικτύου/υπηρεσιών cloud  Στην υποενότητα «2. Αιτιολόγηση», πρέπει να αναφέρονται οι λόγοι έγκρισης ή απόρριψης. | | | | | | |
| **Γ. Τεχνική Αξιολόγηση** | | | | | | |
| 1. **Τελική Αξιολόγηση Αιτήματος** | | | | | | |
| **Το αίτημα αλλαγής ή διαμόρφωσης είναι:** | | | | | | |
| **Τεχνικά εφικτό** | | 🞏 | | **Τεχνικά μη εφικτό** | | 🞏 |
|  | | | | | | |
| 1. **Αιτιολόγηση** | | | | | | |
| **Αιτιολόγηση έγκρισης/απόρριψης** | | | | | | |
| **Συστήματα που επηρεάζονται:** | | | | | | |
| **Λεπτομέρειες τεχνικής σχεδίασης (Προτεινόμενη διαμόρφωση και λεπτομέρειες υλοποίησης αλλαγής):** | | | | | | |
| **Διαχειριστής** υλισμικού/ λογισμικού-συστημάτων/δικτύου/υπηρεσιών cloud **(Ονομετεπώνυμο):** | | | | |  | |
| **Τμήμα** |  | | **Υπογραφή** | |  | |
| **Ημερομηνία:** |  | | **Email :** | |  | |