					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P05					Τίτλος εγγράφου: **Πολιτική Διαχείρισης Αλλαγών P05**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγράμμιση με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 6.1, 5.15	Καλύπτει ενέργειες αντιμετώπισης κινδύνων, έλεγχο πρόσβασης και διαχείριση αλλαγών
ISO/IEC 27002:2022	Έλεγχος 8.32	Εφαρμόζει δομημένη διαδικασία διαχείρισης αλλαγών
NIST SP 800-53 Rev.5	CM-2 έως CM-14	Δικλίδες διαχείρισης διαμόρφωσης
ΓΚΠΔ της ΕΕ	Άρθρα 32(1)(β–δ), 25· Αιτιολογική σκέψη 78	Τεχνικά και οργανωτικά μέτρα για την ασφάλεια συστημάτων και δεδομένων κατά τις αλλαγές
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(α, β, δ, ε)	Επιβάλλει τη διαχείριση κινδύνων ΤΠΕ που συνδέονται με αλλαγές
Κανονισμός DORA της ΕΕ	Άρθρα 5, 8, 12	Διέπει τον λειτουργικό κίνδυνο, τον κίνδυνο ΤΠΕ και την αναφορά περιστατικών
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Δομημένη διαχείριση αλλαγών ΤΠ, απόδοση, συμμόρφωση και σχετικές απαιτήσεις

1. Σκοπός

1.1. Η παρούσα πολιτική θεσπίζει επίσημο πλαίσιο για την έναρξη, αξιολόγηση, έγκριση, υλοποίηση και ανασκόπηση αλλαγών στα πληροφοριακά συστήματα, τις υποδομές, τις εφαρμογές και τις συναφείς διαδικασίες του οργανισμού.

1.2. Διασφαλίζει ότι όλες οι αλλαγές εκτελούνται με ελεγχόμενο και ελέγξιμο τρόπο, ελαχιστοποιώντας τον κίνδυνο διακοπής, παραβίασης της ασφάλειας ή κανονιστικής μη συμμόρφωσης.

1.3. Υποστηρίζει το Παράρτημα Α, Έλεγχο 8.32 του ISO/IEC 27001:2022, επιβάλλοντας ασφαλείς, τεκμηριωμένες και ευθυγραμμισμένες με τον κίνδυνο πρακτικές διαχείρισης αλλαγών.

1.4. Η πολιτική διασφαλίζει επίσης την ιχνηλασιμότητα των αποφάσεων αλλαγής και ενισχύει τη λειτουργική ανθεκτικότητα κατά τις προγραμματισμένες ή επείγουσες τροποποιήσεις.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλες τις αλλαγές που επηρεάζουν συστήματα, δεδομένα και περιβάλλοντα εντός του πεδίου εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), συμπεριλαμβανομένων:

2.1.1. Υποδομών ΤΠ (εγκαταστάσεις στις εγκαταστάσεις του οργανισμού, περιβάλλον νέφους, υβριδικό περιβάλλον)

2.1.2. Περιβαλλόντων παραγωγής, προπαραγωγής και αποκατάστασης καταστροφών

2.1.3. Επιχειρησιακών εφαρμογών, υπηρεσιών, API και διασυνδέσεων

2.1.4. Ρυθμίσεων διαμόρφωσης, εγκατάστασης διορθώσεων, εκδόσεων λογισμικού και μεταφορών συστημάτων

2.1.5. Επειγουσών διορθώσεων και αλλαγών βάσει έργου ή προγραμματισμένων αλλαγών

2.2. Διέπει αλλαγές που εκκινούνται από:

2.2.1. Εσωτερικό προσωπικό (λειτουργία ΤΠ, προγραμματιστές, ιδιοκτήτες συστημάτων)

2.2.2. Εξωτερικούς προμηθευτές, παρόχους διαχειριζόμενων υπηρεσιών (MSP) και αναδόχους

2.2.3. Ομάδες έργου κατά την υλοποίηση συστημάτων, αναβαθμίσεις ή μεταβάσεις υπηρεσιών

2.3. Η παρούσα πολιτική δεν εφαρμόζεται σε:

2.3.1. Προσωρινά περιβάλλοντα δοκιμών/ανάπτυξης χωρίς πρόσβαση σε δεδομένα παραγωγής

2.3.2. Προσωπικές ρυθμίσεις χρηστών (καλύπτονται από την Πολιτική Αποδεκτής Χρήσης)

2.3.3. Αλλαγές σε συστήματα εκτός του ορίου ελέγχου του οργανισμού, εκτός εάν επηρεάζουν ενταγμένα στοιχεία ενεργητικού ή υποχρεώσεις συμμόρφωσης

3. Στόχοι

3.1. Να διασφαλίζεται ότι όλες οι αλλαγές ανασκοπούνται, εγκρίνονται, δοκιμάζονται και τεκμηριώνονται πριν από την εκτέλεσή τους.

3.2. Να διατηρούνται η διαθεσιμότητα των συστημάτων, η ακεραιότητα των δεδομένων και η συνέχεια των υπηρεσιών κατά τη διάρκεια και μετά τις δραστηριότητες αλλαγής.

3.3. Να απαιτούνται καθορισμένες κατηγοριοποιήσεις αλλαγών, σχέδια επαναφοράς και αξιολογήσεις κινδύνου για όλους τους τύπους αλλαγών.

3.4. Να καθίσταται δυνατή η διαφανής λήψη αποφάσεων και η κλιμάκωση μέσω δομημένης διακυβέρνησης.

3.5. Να υποστηρίζεται η ετοιμότητα για έλεγχο μέσω ιχνηλάσιμων αρχείων αλλαγών και ανασκοπήσεων μετά την υλοποίηση.

3.6. Να επιβάλλεται ο διαχωρισμός καθηκόντων και να μειώνεται ο κίνδυνος μη εξουσιοδοτημένων ή συγκρουόμενων αλλαγών σε κρίσιμα συστήματα.

4. Ρόλοι και αρμοδιότητες

4.1. Ανώτατη Διοίκηση

4.1.1. Εγκρίνει την Πολιτική Διαχείρισης Αλλαγών και διασφαλίζει την ευθυγράμμισή της με τους στρατηγικούς στόχους και τις κανονιστικές υποχρεώσεις.

4.1.2. Εγκρίνει προγράμματα αλλαγών υψηλού αντικτύπου ή διαλειτουργικού χαρακτήρα στο πλαίσιο της εποπτείας διακυβέρνησης.

4.1.3. Διαθέτει τους αναγκαίους πόρους και τον προϋπολογισμό για εργαλεία ελέγχου αλλαγών και εκπαίδευση προσωπικού.

4.2. Συμβουλευτική Επιτροπή Αλλαγών (CAB)

4.2.1. Ανασκοπεί και εγκρίνει τυπικές και μείζονες αλλαγές, διασφαλίζοντας την κατάλληλη αξιολόγηση κινδύνου, αντικτύπου και εξαρτήσεων.

4.2.2. Επικυρώνει σχέδια επαναφοράς, αποτελέσματα δοκιμών, επικοινωνίες με τα ενδιαφερόμενα μέρη και προγραμματισμό.

4.2.3. Αποτελείται από ιδιοκτήτες συστημάτων, εκπροσώπους ασφάλειας πληροφοριών, λειτουργίας ΤΠ, επιχειρησιακών μονάδων και συμμόρφωσης.

4.2.4. Μπορεί να εκχωρεί αποφάσεις για αλλαγές χαμηλού κινδύνου ή επείγουσες αλλαγές υπό τεκμηριωμένες προϋποθέσεις.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1. Ενεργοποιητές και συχνότητα ανασκόπησης

9.1.1. Η παρούσα πολιτική πρέπει να ανασκοπείται ετησίως ή όταν προκύπτει:

9.1.1.1. Μείζων αλλαγή στην ΤΠ ή στην υποδομή

9.1.1.2. Σημαντικό περιστατικό σχετικό με αποτυχημένες ή μη εξουσιοδοτημένες αλλαγές

9.1.1.3. Κανονιστική επικαιροποίηση ή νέα νομική υποχρέωση σχετική με αλλαγές

9.1.1.4. Εφαρμογή νέων εργαλείων ή πλατφορμών CMS

9.2. Διαδικασία ανασκόπησης της Πολιτικής Διαχείρισης Αλλαγών

9.2.1. Ο Υπεύθυνος Διαχείρισης Αλλαγών ηγείται της διαδικασίας ανασκόπησης σε συνεργασία με:

9.2.1.1. ΤΠ, Ασφάλεια και Λειτουργία

9.2.1.2. Εσωτερικό Έλεγχο και Διαχείριση Κινδύνων

9.2.1.3. Εκπροσώπους της CAB

9.2.2. Οι επικαιροποιήσεις πρέπει να ανασκοπούνται και να εγκρίνονται από την Ανώτατη Διοίκηση και την Επιτροπή Καθοδήγησης ISMS.

9.2.3. Οι επανεκδιδόμενες εκδόσεις πρέπει να παρακολουθούνται στο Μητρώο Εγγράφων και να γνωστοποιούνται στα επηρεαζόμενα μέρη, με εκ νέου επιβεβαίωση όπου απαιτείται.

9.3. Έλεγχος εγγράφων και εκδόσεων

9.3.1. Όλες οι εκδόσεις πρέπει να περιλαμβάνουν:

9.3.1.1. Αναγνωριστικό πολιτικής, τίτλο και επίπεδο διαβάθμισης

9.3.1.2. Ιδιοκτήτη και ιστορικό αναθεωρήσεων

9.3.1.3. Αρχείο αλλαγών και ημερομηνία έναρξης ισχύος

9.3.1.4. Αρχή έγκρισης

9.3.2. Οι αρχειοθετημένες εκδόσεις πρέπει να διατηρούνται σύμφωνα με την Πολιτική Διατήρησης Εγγράφων (τουλάχιστον 3 έτη).

10. Σχετικές πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική συνδέεται άμεσα και υποστηρίζει την εφαρμογή των εξής:

10.1.1. P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει την απαίτηση για επίσημες δικλίδες ασφάλειας και λογοδοσία σε επίπεδο διαδικασίας, συμπεριλαμβανομένης της διακυβέρνησης της διαχείρισης αλλαγών.

10.1.2. P2 – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τις αρμόδιες αρχές έγκρισης και τον διαχωρισμό καθηκόντων που σχετίζονται με την εξουσιοδότηση και την εποπτεία αλλαγών.

10.1.3. P4 – Πολιτική Ελέγχου Πρόσβασης: Διασφαλίζει ότι τα δικαιώματα πρόσβασης για όσους υλοποιούν και ανασκοπούν αλλαγές ακολουθούν την αρχή του ελάχιστου απαιτούμενου δικαιώματος.

10.1.4. P6 – Πολιτική Διαχείρισης Κινδύνων: Διασφαλίζει ότι όλες οι αλλαγές υπόκεινται σε κατάλληλη αξιολόγηση κινδύνου και στρατηγικές μετριασμού.

10.1.5. P33 – Πολιτική Παρακολούθησης Ελέγχου και Συμμόρφωσης: Διέπει την επικύρωση και την ελεγκτική ανασκόπηση των αρχείων και των παραβιάσεων που σχετίζονται με τη διαχείριση αλλαγών.

10.2. Οι πολιτικές αυτές, συνολικά, καθιστούν εφικτό έναν τεκμηριώσιμο, ιχνηλάσιμο και ασφαλή κύκλο ζωής διαχείρισης αλλαγών στο πλαίσιο του ISMS.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001:2022

11.1.1. Ρήτρα 6.1 – Ενέργειες για την αντιμετώπιση κινδύνων και ευκαιριών: Η παρούσα πολιτική υποστηρίζει την αναγνώριση, αξιολόγηση και αντιμετώπιση των κινδύνων που σχετίζονται με αλλαγές.

11.1.2. Ρήτρα 5.15 – Έλεγχος πρόσβασης: Διασφαλίζει ότι η πρόσβαση κατά τις αλλαγές ελέγχεται και είναι ιχνηλάσιμη.

11.1.3. Παράρτημα Α, Έλεγχος 8.32 – Διαχείριση αλλαγών: Η παρούσα πολιτική εφαρμόζει πλήρως την απαίτηση διαχείρισης αλλαγών σε εγκαταστάσεις επεξεργασίας πληροφοριών και συστήματα με προγραμματισμένο και ελεγχόμενο τρόπο.

11.2. ISO/IEC 27002:2022 – Έλεγχος 8.32

11.2.1. Ενισχύει την εφαρμογή δομημένης διαδικασίας διαχείρισης αλλαγών, συμπεριλαμβανομένων της κατηγοριοποίησης αλλαγών, της έγκρισης, των δοκιμών, της επαναφοράς και της τεκμηρίωσης.

11.3. NIST SP 800-53 Rev.5

11.3.1. Οικογένεια CM (CM-1 έως CM-14): Η παρούσα πολιτική ευθυγραμμίζεται στενά με τις δικλίδες διαχείρισης διαμόρφωσης, συμπεριλαμβανομένων των βασικών διαμορφώσεων (CM-2), του ελέγχου αλλαγών διαμόρφωσης (CM-3), της ανάλυσης αντικτύπου στην ασφάλεια (CM-4) και των περιορισμών πρόσβασης (CM-5).

11.3.2. Οικογένεια AU (AU-2, AU-6, AU-12): Οι μηχανισμοί καταγραφής και ελέγχου που αναφέρονται στην παρούσα πολιτική υποστηρίζουν την ιχνηλασιμότητα συμβάντων και την ανασκόπηση συμμόρφωσης για δραστηριότητες σχετικές με αλλαγές.

11.3.3. RA-3, RA-5: Οι αξιολογήσεις κινδύνου που προκαλούνται από αλλαγές και οι σαρώσεις ευπαθειών είναι ενσωματωμένες στη διαδικασία αξιολόγησης αλλαγών.

11.3.4. PM-11 (Ορισμός αποστολής/επιχειρησιακής διαδικασίας): Διασφαλίζει ότι η επιχειρησιακή συνέχεια και οι λειτουργικοί στόχοι διατηρούνται κατά τις αλλαγές.

11.4. ΓΚΠΔ της ΕΕ (2016/679)

11.4.1. Άρθρο 32(1)(β–δ): Η παρούσα πολιτική υποστηρίζει την απαίτηση για κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζεται η ασφάλεια των δεδομένων, ιδίως κατά τις αλλαγές συστημάτων.

11.4.2. Άρθρο 25 – Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού: Διασφαλίζει ότι οι αλλαγές που επηρεάζουν δεδομένα προσωπικού χαρακτήρα ενσωματώνουν την προστασία της ιδιωτικότητας και την ασφάλεια στον σχεδιασμό και στην υλοποίηση.

11.4.3. Αιτιολογική σκέψη 78: Απαιτεί από τους υπευθύνους επεξεργασίας να εφαρμόζουν μηχανισμούς, όπως πολιτικές ελέγχου αλλαγών, ώστε να διασφαλίζεται διαρκώς η εμπιστευτικότητα, η ακεραιότητα και η ανθεκτικότητα των συστημάτων επεξεργασίας.

11.5. Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1. Άρθρο 21(2)(α, β, δ, ε): Επιβάλλει τεχνικά και οργανωτικά μέτρα για τη διαχείριση κινδύνων ΤΠΕ, συμπεριλαμβανομένων εκείνων που απορρέουν από αλλαγές συστημάτων, επικαιροποιήσεις λογισμικού και τροποποιήσεις υποδομής.

11.6. Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1. Άρθρο 5 – Πλαίσιο διακυβέρνησης και εσωτερικού ελέγχου: Η παρούσα πολιτική επιβάλλει αρχές διαχείρισης λειτουργικού κινδύνου που συνδέονται με αλλαγές και επικαιροποιήσεις ΤΠΕ.

11.6.2. Άρθρο 8 – Πλαίσιο διαχείρισης κινδύνων ΤΠΕ: Επιβάλλει στις χρηματοοικονομικές οντότητες να διαχειρίζονται όλες τις αλλαγές που επηρεάζουν συστήματα ΤΠΕ στο πλαίσιο δομημένων διαδικασιών διαχείρισης αλλαγών, κάτι που αποτυπώνεται στις απαιτήσεις της παρούσας πολιτικής για κατηγοριοποίηση, δοκιμές, επαναφορά και τεκμηρίωση.

11.6.3. Άρθρο 12 – Αναφορά περιστατικών: Διασφαλίζει ότι αποτυχημένες αλλαγές που οδηγούν σε διαταραχές ΤΠΕ είναι ιχνηλάσιμες, τεκμηριωμένες και αναφέρονται όπου απαιτείται.

11.7. COBIT 2019

11.7.1. BAI06 – Διαχειριζόμενες αλλαγές ΤΠ: Η παρούσα πολιτική ικανοποιεί άμεσα τους στόχους του BAI06, καθιερώνοντας δομημένες ροές εργασίας για έγκριση αλλαγών, αξιολόγηση αντικτύπου, επικοινωνία και δοκιμές.

11.7.2. BAI02 – Διαχειριζόμενος ορισμός απαιτήσεων και BAI03 – Διαχειριζόμενος προσδιορισμός και ανάπτυξη λύσεων: Διασφαλίζουν ότι οι αλλαγές που καθοδηγούνται από επιχειρησιακές ανάγκες ανασκοπούνται και υλοποιούνται με ασφαλή τρόπο.

11.7.3. DSS01 – Διαχειριζόμενες λειτουργίες: Υποστηρίζει τη διαρκή ακεραιότητα των συστημάτων κατά την εκτέλεση αλλαγών.

11.7.4. MEA01 και MEA03 – Παρακολούθηση, αξιολόγηση και αποτίμηση απόδοσης και συμμόρφωσης: Καθιστά δυνατή τη συνεχή εποπτεία της αποτελεσματικότητας και της εφαρμογής της πολιτικής διαχείρισης αλλαγών.