					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P05S					Τίτλος εγγράφου: **Πολιτική Διαχείρισης Αλλαγών**							
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, 8.	
ISO/IEC 27002:2022	Έλεγχος 8.	
NIST SP 800-53 Rev.5	CM-2 έως CM-5, CM-11	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(b)	
Κανονισμός DORA της ΕΕ	Άρθρα 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Σκοπός

1.1 Η παρούσα πολιτική διασφαλίζει ότι όλες οι αλλαγές σε πληροφοριακά συστήματα, παραμετροποιήσεις, επιχειρησιακές εφαρμογές ή υπηρεσίες νέφους σχεδιάζονται, αξιολογούνται ως προς τον κίνδυνο, δοκιμάζονται και εγκρίνονται πριν από την υλοποίησή τους.

1.2 Στόχος είναι η μείωση των επιχειρησιακών διαταραχών, των κινδύνων ασφάλειας και των διακοπών υπηρεσιών μέσω της θέσπισης μιας απλοποιημένης αλλά δεσμευτικής διαδικασίας, η οποία εφαρμόζεται ακόμη και σε μικρές επιχειρήσεις με περιορισμένους πόρους.

1.3 Η παρούσα πολιτική υποστηρίζει την πιστοποίηση κατά ISO/IEC 27001:2022, καθορίζοντας με τυπικό τρόπο τον τρόπο με τον οποίο οι τεχνικές και επιχειρησιακές αλλαγές διαχειρίζονται και τεκμηριώνονται.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Εργαζομένους και προϊσταμένους τμημάτων που εισηγούνται ή υλοποιούν αλλαγές

2.1.2 Εξωτερικούς παρόχους υπηρεσιών πληροφορικής που διαχειρίζονται συστήματα ή λογισμικό

2.1.3 Τον Γενικό Διευθυντή, ο οποίος φέρει τη συνολική ευθύνη για την έγκριση αλλαγών

2.2 Καλύπτει αλλαγές σε:

2.2.1 Λογισμικό (ενημερώσεις, διορθωτικές ενημερώσεις, νέες εφαρμογές)

2.2.2 Υλικό (αντικαταστάσεις, αναβαθμίσεις)

2.2.3 Ρυθμίσεις δικτύου και τείχους προστασίας

2.2.4 Υπηρεσίες νέφους, δικαιώματα πρόσβασης χρηστών ή διασυνδέσεις με προμηθευτές

2.2.5 Κρίσιμες αλλαγές επιχειρησιακών διαδικασιών που αφορούν πληροφοριακά συστήματα

2.3 Στο πεδίο εφαρμογής της παρούσας πολιτικής εμπίπτουν τόσο οι προγραμματισμένες όσο και οι επείγουσες αλλαγές.

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλες οι αλλαγές σε πληροφοριακά και επιχειρησιακά συστήματα είναι εγκεκριμένες, τεκμηριωμένες και αναστρέψιμες σε περίπτωση προβλημάτων.

3.2 Να προλαμβάνεται μη προγραμματισμένος χρόνος διακοπής λειτουργίας, απώλεια δεδομένων ή περιστατικά ασφάλειας που προκαλούνται από ανεξέλεγκτες αλλαγές.

3.3 Να ορίζονται απλές και επαναλήψιμες διαδικασίες για την υποβολή, την έγκριση, τη δοκιμή και την αναστροφή αλλαγών.

3.4 Να τηρείται ελέγξιμο Αρχείο Καταγραφής Αλλαγών που υποστηρίζει τη λογοδοσία σε επιχειρησιακό επίπεδο και τη συμμόρφωση με κανονιστικές απαιτήσεις.

3.5 Να υποστηρίζεται η λήψη αποφάσεων βάσει κινδύνου για σημαντικές ή ευαίσθητες αλλαγές.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής

4.1.1 Φέρει την τελική λογοδοσία για όλες τις μείζονες αλλαγές.

4.1.2 Ανασκοπεί και εγκρίνει μη συνήθεις, κρίσιμες ή υψηλού κινδύνου αλλαγές.

4.1.3 Ανασκοπεί το Αρχείο Καταγραφής Αλλαγών σε τριμηνιαία βάση ή μετά από σοβαρά περιστατικά.

4.2 Υποστήριξη Πληροφορικής ή Εξωτερικός Πάροχος Υπηρεσιών Πληροφορικής

4.2.1 Υλοποιεί αλλαγές, συμπεριλαμβανομένων ενημερώσεων παραμετροποίησης, εφαρμογής διορθωτικών ενημερώσεων και μεταβάσεων συστημάτων.

4.2.2 Τηρεί βασικό Αρχείο Καταγραφής Αλλαγών, στο οποίο καταγράφονται ημερομηνίες, είδη αλλαγών, αποτελέσματα και εγκρίνοντες.

4.2.3 Δοκιμάζει τις αλλαγές πριν από την υλοποίηση και εφαρμόζει ενέργειες αναστροφής όπου απαιτείται.

4.2.4 Ενημερώνει τους επηρεαζόμενους χρήστες πριν και μετά από μείζονες αλλαγές.

[... 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 Ετήσια ανασκόπηση

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται ετησίως από τον Γενικό Διευθυντή ή από τον ορισμένο Υπεύθυνο Πληροφορικής, ώστε να διασφαλίζεται η ευθυγράμμιση με τα ισχύοντα συστήματα, τις ροές εργασίας και τις κανονιστικές απαιτήσεις.

9.2 Ενδιάμεσες ανασκοπήσεις

9.2.1 Ανασκοπήσεις πρέπει επίσης να ενεργοποιούνται από:

9.2.1.1 Περιστατικά ασφάλειας που προκαλούνται από ανεπαρκή χειρισμό αλλαγών

9.2.1.2 Εισαγωγή νέων πληροφοριακών συστημάτων

9.2.1.3 Αλλαγές σε σχετικά πρότυπα όπως το ISO, η Οδηγία NIS2 της ΕΕ ή ο Κανονισμός DORA της ΕΕ

9.3 Τεκμηρίωση επικαιροποιήσεων

9.3.1 Οι αλλαγές στην παρούσα πολιτική πρέπει να υπόκεινται σε έλεγχο εκδόσεων και να εγκρίνονται από τον Γενικό Διευθυντή. Κάθε έκδοση πρέπει να καταγράφει την ημερομηνία, τη σύνοψη των αλλαγών και τον εγκρίνοντα.

9.4 Κοινοποίηση της πολιτικής

9.4.1 Κάθε επικαιροποίηση πρέπει να κοινοποιείται σε όλους τους επηρεαζόμενους εργαζομένους και εξωτερικούς παρόχους. Η τεκμηρίωση πρέπει να επικαιροποιείται σε όλα τα σημεία αναφοράς (π.χ. πύλη προσωπικού, κοινόχρηστοι δίσκοι).

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική συνδέεται στενά με τις ακόλουθες πολιτικές SME:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει την αρμοδιότητα έγκρισης για τις αλλαγές.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Διασφαλίζει ότι οι τροποποιήσεις πρόσβασης που προκύπτουν από αλλαγές τεκμηριώνονται και εφαρμόζονται ορθά.

10.1.3 P7S – Πολιτική Ένταξης και Αποχώρησης Προσωπικού: Συντονίζει τις αλλαγές που σχετίζονται με μεταβολές ρόλων και χορήγηση πρόσβασης.

10.1.4 P15S – Πολιτική Αντιγράφων Ασφαλείας και Επαναφοράς: Διασφαλίζει ότι μπορούν να εκτελεστούν ενέργειες αναστροφής και αποκατάστασης εάν μια αλλαγή αποτύχει.

10.1.5 P30S – Πολιτική Απόκρισης σε Περιστατικά: Ρυθμίζει τον τρόπο με τον οποίο οι αποτυχημένες ή μη εγκεκριμένες αλλαγές αντιμετωπίζονται ως περιστατικά ασφάλειας.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 6.1 – Ο σχεδιασμός βάσει κινδύνου πρέπει να περιλαμβάνει δραστηριότητες αλλαγών.

11.1.2 Ρήτρα 8.1 – Οι επιχειρησιακοί έλεγχοι πρέπει να εφαρμόζονται με συνέπεια στις δραστηριότητες που σχετίζονται με αλλαγές, ώστε να διασφαλίζεται η ακεραιότητα των υπηρεσιών.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 8.32 – Παρέχει κατευθύνσεις για ασφαλείς διαδικασίες διαχείρισης αλλαγών, συμπεριλαμβανομένων της τεκμηρίωσης, των δοκιμών και της έγκρισης.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-2 – Βασική διαμόρφωση συστημάτων πριν από την αλλαγή.

11.3.2 CM-3 – Έλεγχος αλλαγών διαμόρφωσης.

11.3.3 CM-4 – Ανάλυση επιπτώσεων στην ασφάλεια.

11.3.4 CM-5 – Έγκριση και τεκμηρίωση αλλαγών.

11.3.5 CM-11 – Έλεγχος και παρακολούθηση αλλαγών.

11.4 Οδηγία NIS2 της ΕΕ

11.4.1 Άρθρο 21(2)(b) – Απαιτεί τυπικές διαδικασίες για τεχνικά και οργανωτικά μέτρα ασφάλειας, συμπεριλαμβανομένης της διαχείρισης αλλαγών.

11.5 Κανονισμός DORA της ΕΕ

11.5.1 Άρθρα 6(9) και 8(4)(b) – Απαιτούν από τις χρηματοοικονομικές οντότητες να τηρούν διαδικασίες διαχείρισης αλλαγών και διαμόρφωσης για συστήματα ΤΠΕ.

11.6 COBIT 2019

11.6.1 BAI06 – Διαχείριση αλλαγών: Δίνει έμφαση στον σχεδιασμό, την αξιολόγηση κινδύνου και τις δυνατότητες αναστροφής.

11.6.2 DSS01 – Διαχείριση λειτουργιών: Διασφαλίζει την επιχειρησιακή ακεραιότητα κατά τις τεχνικές μεταβάσεις και αλλαγές.