					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P30S					Τίτλος εγγράφου: **Πολιτική Διαχείρισης Περιστατικών Ασφάλειας Πληροφοριών**							
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**

Νομική σημείωση (πνευματικά δικαιώματα και περιορισμοί χρήσης)

(C) 2025 Clarysec LLC. All rights reserved.

Το παρόν έγγραφο αποτελεί πνευματική ιδιοκτησία της Clarysec LLC. Απαγορεύεται η αντιγραφή, επαναχρησιμοποίηση, διανομή ή τροποποίησή του, εν όλω ή εν μέρει, για εμπορικούς ή σκοπούς υλοποίησης χωρίς προηγούμενη ρητή έγγραφη άδεια.
Η μη εξουσιοδοτημένη χρήση απαγορεύεται αυστηρά και ενδέχεται να επιφέρει νομικές ενέργειες.
Για θέματα αδειοδότησης, επικοινωνήστε με: info@clarysec.com

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 6.1, 6.3, 8	Διαχείριση περιστατικών, συνεχής βελτίωση, επιχειρησιακός έλεγχος
ISO/IEC 27002:2022	Έλεγχοι 5.24, 5.25	Ανίχνευση περιστατικών, ετοιμότητα, άντληση διδαγμάτων
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Χειρισμός περιστατικών, παρακολούθηση και αναφορά
ΓΚΠΔ της ΕΕ	Άρθρο 33	Απαιτήσεις γνωστοποίησης παραβίασης
Οδηγία NIS2 της ΕΕ	Άρθρο 23	Υποχρεωτική αναφορά κυβερνοπεριστατικών
Κανονισμός DORA της ΕΕ	Άρθρο 17	Διαχείριση περιστατικών ΤΠΕ
COBIT 2019	DSS02, DSS04	Διαχείριση υπηρεσιών/περιστατικών και επιχειρησιακή συνέχεια

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο ο οργανισμός ανιχνεύει, αναφέρει και διαχειρίζεται περιστατικά ασφάλειας πληροφοριών που επηρεάζουν τα ψηφιακά του συστήματα, τα δεδομένα ή τις υπηρεσίες του.

1.2. Επιτρέπει στον οργανισμό να περιορίζει τη ζημία, να προστατεύει τα δεδομένα πελατών και να συμμορφώνεται με κανονιστικές υποχρεώσεις, όπως η απαίτηση του ΓΚΠΔ της ΕΕ για γνωστοποίηση παραβίασης εντός 72 ωρών.

1.3. Η πολιτική διασφαλίζει σαφείς αρμοδιότητες, βήματα επικοινωνίας και ενέργειες παρακολούθησης μετά το περιστατικό, ακόμη και σε μικρούς οργανισμούς χωρίς εξειδικευμένη ομάδα ασφάλειας.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1. Όλους τους εργαζομένους, τους αναδόχους και τους εξωτερικούς παρόχους υπηρεσιών πληροφορικής

2.1.2. Όλα τα συστήματα και τις υπηρεσίες που διαχειρίζεται η εταιρεία, συμπεριλαμβανομένων ιστοτόπων, υποδομών νέφους, φορητών συσκευών, φορητών υπολογιστών και λογαριασμών ηλεκτρονικού ταχυδρομείου

2.1.3. Όλους τους τύπους περιστατικών, συμπεριλαμβανομένων:

2.1.3.1. μη εξουσιοδοτημένης πρόσβασης σε δεδομένα ή συστήματα

2.1.3.2. μολύνσεων από κακόβουλο λογισμικό ή λυτρισμικό

2.1.3.3. απόπειρων ηλεκτρονικού ψαρέματος ή κοινωνικής μηχανικής

2.1.3.4. διακοπών λειτουργίας συστημάτων λόγω κυβερνοεπίθεσης ή κακής χρήσης

2.1.3.5. τυχαίας γνωστοποίησης ή διαγραφής ευαίσθητων πληροφοριών

2.1.3.6. απώλειας ή κλοπής επιχειρησιακών συσκευών ή μέσων αποθήκευσης

3. Στόχοι

3.1. Καθιέρωση σαφούς διαδικασίας για την αναγνώριση και την κλιμάκωση περιστατικών ασφάλειας.

3.2. Διασφάλιση ότι τα περιστατικά αναφέρονται, καταγράφονται και αντιμετωπίζονται εντός προκαθορισμένων χρονικών πλαισίων.

3.3. Δυνατότητα ταχείας συγκράτησης της ζημίας, ανάκτησης δεδομένων και αποκατάστασης υπηρεσιών.

3.4. Διασφάλιση ότι τα επηρεαζόμενα μέρη, όπως πελάτες και ρυθμιστικές αρχές, ενημερώνονται όταν αυτό απαιτείται από τη νομοθεσία.

3.5. Πρόληψη επανάληψης μέσω ανάλυσης βασικής αιτίας, διορθωτικών ενεργειών και βελτίωσης της πολιτικής.

3.6. Δυνατότητα στις ΜΜΕ να καλύπτουν τις απαιτήσεις πιστοποίησης ISO 27001 και να αποδεικνύουν λογοδοσία κατά τη διάρκεια ελέγχων.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής (GM)

4.1.1. Έχει την κυριότητα της παρούσας πολιτικής και διασφαλίζει την εφαρμογή της.

4.1.2. Ασκεί εποπτεία επί των δραστηριοτήτων διαχείρισης περιστατικών και εγκρίνει τις γνωστοποιήσεις προς ρυθμιστικές αρχές ή πελάτες.

4.1.3. Ανασκοπεί τις αναφορές μετά το περιστατικό και διασφαλίζει ότι η πολιτική επικαιροποιείται όταν απαιτείται.

4.1.4. Μπορεί να εκχωρεί καθήκοντα συντονισμού, αλλά διατηρεί τη λογοδοσία.

4.2. Εξωτερικός πάροχος υπηρεσιών πληροφορικής / Διαχειριστής συστημάτων (εσωτερικός ή εξωτερικός)

4.2.1. Ανιχνεύει και διερευνά πιθανά περιστατικά ασφάλειας.

4.2.2. Εφαρμόζει ενέργειες περιορισμού και ανάκαμψης, όπως απενεργοποίηση πρόσβασης και αποκατάσταση από αντίγραφα ασφαλείας.

4.2.3. Ενημερώνει τον GM για όλα τα επιβεβαιωμένα ή ύποπτα περιστατικά εντός 1 ώρας από την ανακάλυψή τους.

4.2.4. Τηρεί αρχείο καταγραφής περιστατικών με χρονοσήμανση, εκτίμηση αντικτύπου και ενέργειες απόκρισης.

[... 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. Προγραμματισμένη ανασκόπηση

9.1.1. Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά κάθε 12 μήνες από τον Γενικό Διευθυντή (GM), ώστε να διασφαλίζεται:

9.1.1.1. η ευθυγράμμιση με τους ελέγχους του ISO/IEC 27001:2022

9.1.1.2. η ανταπόκριση σε νέες απειλές, κινδύνους και περιστατικά

9.1.1.3. η διαρκής συμμόρφωση με νομικές και συμβατικές υποχρεώσεις, όπως ο ΓΚΠΔ της ΕΕ και ο Κανονισμός DORA της ΕΕ

9.2. Εναύσματα ανασκόπησης

9.2.1. Η πολιτική πρέπει επίσης να ανασκοπείται και να επικαιροποιείται μετά από:

9.2.1.1. οποιοδήποτε περιστατικό υψηλής σοβαρότητας ή γνωστοποίηση προς ρυθμιστική αρχή

9.2.1.2. εισαγωγή νέας υποδομής πληροφορικής ή αλλαγών σε συστήματα

9.2.1.3. τροποποιήσεις νομικών απαιτήσεων που αφορούν παραβιάσεις ασφάλειας

9.3. Τεκμηρίωση ανασκόπησης και διανομή

9.3.1. Όλες οι ανασκοπήσεις και οι αλλαγές πρέπει να τεκμηριώνονται στο αρχείο μεταβολών της πολιτικής

9.3.2. Οι επικαιροποιημένες εκδόσεις πρέπει να διανέμονται σε όλους τους εργαζομένους, τους προμηθευτές και τους παρόχους ΤΠ που εμπλέκονται στην ασφάλεια ή στη λειτουργία συστημάτων

9.3.3. Τεκμήρια ευαισθητοποίησης του προσωπικού, όπως πρακτικά συναντήσεων ή επιβεβαιώσεις μέσω ηλεκτρονικού ταχυδρομείου, πρέπει να διατηρούνται για σκοπούς ελεγκτικής ετοιμότητας

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική πρέπει να εφαρμόζεται σε συντονισμό με τις ακόλουθες πολιτικές ΜΜΕ:

10.1.1. P1S – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις συνολικές απαιτήσεις για τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας κατά τις λειτουργίες, συμπεριλαμβανομένης της διαχείρισης περιστατικών.

10.1.2. P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τις δομές αρμοδιότητας και λογοδοσίας για την ανίχνευση, αναφορά και κλιμάκωση περιστατικών.

10.1.3. P4S – Πολιτική Ελέγχου Πρόσβασης: Επιτρέπει την άμεση ανάκληση δικαιωμάτων πρόσβασης κατά τις ενέργειες διαχείρισης περιστατικών.

10.1.4. P8S – Πολιτική Εκπαίδευσης και Ευαισθητοποίησης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι όλοι οι εργαζόμενοι μπορούν να εντοπίζουν και να αναφέρουν αποτελεσματικά περιστατικά ασφάλειας.

10.1.5. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Καθοδηγεί τις νομικές διαδικασίες γνωστοποίησης παραβίασης βάσει ΓΚΠΔ και υποστηρίζει τη συμμόρφωση με κανονιστικές απαιτήσεις κατά τη διαχείριση περιστατικών.

10.1.6. P22S – Πολιτική Καταγραφής και Παρακολούθησης: Παρέχει τα αναγκαία εργαλεία και την απαιτούμενη ορατότητα για την ανίχνευση, ανάλυση και ελεγκτική τεκμηρίωση συμβάντων ασφάλειας.

10.1.7. P31S – Πολιτική Συλλογής Τεκμηρίων και Ψηφιακής Διερεύνησης: Υποστηρίζει τη διερεύνηση και τη νομική τεκμηρίωση ενεργειών που σχετίζονται με περιστατικά, μέσω ορθού χειρισμού τεκμηρίων.

10.2. Οι πολιτικές αυτές διαμορφώνουν από κοινού το επιχειρησιακό πλαίσιο της ΜΜΕ για την ανίχνευση, την απόκριση και την ανάκαμψη από περιστατικά ασφάλειας πληροφοριών.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 6.1 – Απαιτεί σχεδιασμό αντιμετώπισης κινδύνων, συμπεριλαμβανομένης της προετοιμασίας για περιστατικά.

11.1.2. Ρήτρα 6.3 – Υποστηρίζει τη συνεχή βελτίωση μέσω των διδαγμάτων που αντλούνται από συμβάντα ασφάλειας.

11.1.3. Ρήτρα 8.1 – Δίνει έμφαση στον επιχειρησιακό έλεγχο για τη διαχείριση περιστατικών και διαταραχών.

11.2. ISO/IEC 27002

11.2.1. Έλεγχος 5.24 – Απαιτεί δομημένη προσέγγιση για την αναφορά, αξιολόγηση και διαχείριση περιστατικών ασφάλειας πληροφοριών.

11.2.2. Έλεγχος 5.25 – Εστιάζει στην άντληση διδαγμάτων από τα περιστατικά για τη βελτίωση της μελλοντικής ετοιμότητας και της ανθεκτικότητας των συστημάτων.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Ορίζει διαδικασίες χειρισμού περιστατικών, συμπεριλαμβανομένου του περιορισμού και της ανάκαμψης.

11.3.2. IR-5 – Καθιερώνει απαιτήσεις για την παρακολούθηση και ανάλυση περιστατικών.

11.3.3. IR-6 – Επιβάλλει πρωτόκολλα εξωτερικής και εσωτερικής αναφοράς περιστατικών.

11.4. ΓΚΠΔ της ΕΕ

11.4.1. Άρθρο 33 – Απαιτεί τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα στις ρυθμιστικές αρχές εντός 72 ωρών, με λεπτομέρειες για το πεδίο και τον μετριασμό.

11.5. Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1. Άρθρο 23 – Απαιτεί από ουσιώδεις και σημαντικές οντότητες να γνωστοποιούν σημαντικά περιστατικά στις αρμόδιες αρχές με χρήση τυποποιημένων μορφότυπων αναφοράς.

11.6. Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1. Άρθρο 17 – Απαιτεί από τις χρηματοοικονομικές οντότητες να ταξινομούν, να αναφέρουν και να παρακολουθούν περιστατικά και διαταραχές που σχετίζονται με ΤΠΕ.

11.7. COBIT 2019

11.7.1. DSS02 – Διαχείριση Αιτημάτων Υπηρεσιών και Περιστατικών: Παρέχει καθοδήγηση για την αποτελεσματική διαχείριση επιχειρησιακών περιστατικών και περιστατικών ασφάλειας σε ευθυγράμμιση με τους στόχους διακυβέρνησης.

11.7.2. DSS04 – Διαχείριση Συνέχειας: Συνδέει τη διαχείριση περιστατικών με ευρύτερες στρατηγικές συνέχειας και ανάκαμψης.