| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου | | | | | | | |
| Αριθμός εγγράφου:<br>P31 | | | | | Τίτλος εγγράφου:<br>**Πολιτική Συλλογής Τεκμηρίων και Ψηφιακής Διερεύνησης** | | | | | | | |
| Έκδοση:<br>1.0 | | Ημερομηνία έναρξης ισχύος:<br>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** |
| | | | |
| | | | |

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

| Πρότυπο/Κανονιστικό πλαίσιο | Ρήτρα/Άρθρο | Σχόλιο |
|---|---|---|
| ISO/IEC 27001:2022 | Clause 8 | |
| ISO/IEC 27002:2022 | Controls 5.25–5.27, 8 | |
| ISO/IEC 27035:2016 | Parts 1 & 3 | |
| NIST SP 800-53 Rev.5 | IR-1 έως IR-9, AU-6, PL-2 | |
| NIST SP 800-101 Rev.1 | Mobile-Media Forensics | Ψηφιακή διερεύνηση φορητών συσκευών/μέσων |
| NIST SP 800-86 | Integrating Forensic Techniques | Ενσωμάτωση τεχνικών ψηφιακής διερεύνησης στην απόκριση σε περιστατικά |
| ΓΚΠΔ της ΕΕ | Άρθρο 5, 33–34 | |
| Οδηγία NIS2 της ΕΕ | Άρθρο 23(1)–(4) | |
| Κανονισμός DORA της ΕΕ | Άρθρο 17(1)–(3) | |
| COBIT 2019 | DSS01.07, DSS05 | |

**1. Σκοπός**

1.1 Η παρούσα πολιτική θεσπίζει ένα δομημένο και νομικά υπερασπίσιμο πλαίσιο για την αναγνώριση, συλλογή, διατήρηση, ανάλυση και διάθεση ψηφιακών τεκμηρίων κατά τη διάρκεια πραγματικών ή πιθανολογούμενων περιστατικών ασφάλειας.

**1.2 Διασφαλίζει ότι οι διαδικασίες ετοιμότητας για ψηφιακή διερεύνηση και χειρισμού τεκμηρίων:**

1.2.1 Διατηρούν την ακεραιότητα των τεκμηρίων και την αλυσίδα επιμέλειας.

1.2.2 Υποστηρίζουν εσωτερικές διερευνήσεις, δικαστικές διαδικασίες ή κανονιστικές υποχρεώσεις γνωστοποίησης.

1.2.3 Ευθυγραμμίζονται με διεθνώς αποδεκτά πρότυπα ψηφιακής διερεύνησης και κριτήρια νομικής παραδεκτότητας.

1.3 Η πολιτική υποστηρίζει τη δέσμευση του οργανισμού για προληπτική απόκριση σε περιστατικά, νομική συμμόρφωση και διαφάνεια στη διακυβέρνηση, ελαχιστοποιώντας παράλληλα τη λειτουργική διαταραχή.

**2. Πεδίο εφαρμογής**

**2.1 Η παρούσα πολιτική εφαρμόζεται σε:**

2.1.1 Όλους τους εργαζομένους, αναδόχους, προμηθευτές και παρόχους υπηρεσιών που εμπλέκονται στη διαχείριση συστημάτων, στον χειρισμό περιστατικών ή σε δραστηριότητες ψηφιακής διερεύνησης.

2.1.2 Όλα τα τερματικά σημεία, τους διακομιστές, τις εφαρμογές, τα δίκτυα και τις πλατφόρμες νέφους που τελούν υπό τον έλεγχο του οργανισμού ή υπό τη συμβατική του ευθύνη.

**2.1.3 Κάθε περιστατικό ή συμβάν που απαιτεί χειρισμό τεκμηρίων, συμπεριλαμβανομένων:**

2.1.3.1 Εσωτερικών απειλών, παραβιάσεων δεδομένων ή διερευνήσεων απάτης.

2.1.3.2 Κακής χρήσης συστημάτων ή διαπιστευτηρίων.

2.1.3.3 Περιστατικών λειτουργικής τεχνολογίας (OT) ή βιομηχανικού ελέγχου.

2.1.3.4 Παραβιάσεων φυσικής πρόσβασης που αφορούν ψηφιακά περιουσιακά στοιχεία.

2.2 Η πολιτική διέπει επίσης κάθε αλληλεπίδραση με υπηρεσίες ψηφιακής διερεύνησης τρίτων ή με αρχές επιβολής του νόμου κατά τη διάρκεια νομικής ή κανονιστικής κλιμάκωσης ή σχετικών διαδικασιών.

**3. Στόχοι**

3.1 Να καθίσταται δυνατή η ταχεία, ασφαλής και σύμφωνη με την παρούσα πολιτική απόκτηση τεκμηρίων κατά τη διάρκεια συμβάντων ασφάλειας ή διερευνήσεων.

3.2 Να διαφυλάσσεται η ακεραιότητα, η αυθεντικότητα και η παραδεκτότητα των συλλεγόμενων ψηφιακών τεκμηρίων μέσω αυστηρού ελέγχου πρόσβασης, αρχείων καταγραφής και διαδικασιών επαλήθευσης.

3.3 Να διασφαλίζεται ότι όλες οι δραστηριότητες ψηφιακής διερεύνησης συντονίζονται με τις νομικές και κανονιστικές υποχρεώσεις, περιλαμβανομένων της προστασίας δεδομένων, του εργατικού δικαίου και των περιορισμών διεθνών διαβιβάσεων.

3.4 Να υποστηρίζεται η ανάλυση μετά το περιστατικό, ο προσδιορισμός της βασικής αιτίας και η βελτίωση των ελέγχων μέσω υψηλής ποιότητας αποτελεσμάτων ψηφιακής διερεύνησης.

3.5 Να ενσωματώνεται η ετοιμότητα για ψηφιακή διερεύνηση στο συνολικό Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ), υποστηρίζοντας ελέγχους, γνωστοποιήσεις παραβιάσεων και τη λήψη αποφάσεων από την εκτελεστική διοίκηση.

**4. Ρόλοι και αρμοδιότητες**

**4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)**

4.1.1 Έχει την ευθύνη της παρούσας πολιτικής και διασφαλίζει ότι όλες οι εργασίες ψηφιακής διερεύνησης είναι νομικά υπερασπίσιμες, ελέγξιμες και βασισμένες στον κίνδυνο.

4.1.2 Εγκρίνει την κλιμάκωση προς εξωτερικούς νομικούς φορείς και παρόχους υπηρεσιών ψηφιακής διερεύνησης.

**4.2 Αναλυτές ψηφιακής διερεύνησης / χειριστές περιστατικών**

4.2.1 Ηγούνται της απόκτησης, διατήρησης και τεχνικής ανάλυσης τεκμηρίων.

4.2.2 Διασφαλίζουν ότι η αλυσίδα επιμέλειας καταγράφεται και διατηρείται ορθά.

4.2.3 Τεκμηριώνουν όλες τις ενέργειες, τα ευρήματα και τις ρυθμίσεις των εργαλείων που χρησιμοποιούνται κατά τις διερευνήσεις.

[ ... 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 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον ετησίως και να επικαιροποιείται όταν απαιτείται, ώστε να αποτυπώνει:**

9.1.1 Αλλαγές σε νόμους, κανονιστικές απαιτήσεις ή νομολογία που επηρεάζουν τις διαδικασίες ψηφιακής διερεύνησης ή τη διαχείριση δεδομένων.

9.1.2 Επικαιροποιήσεις σε αναγνωρισμένα από τον κλάδο πρότυπα ή σύνολα εργαλείων ψηφιακής διερεύνησης.

9.1.3 Διδάγματα από ανασκοπήσεις μετά το περιστατικό, νομικές διαφορές ή ευρήματα ελέγχου.

9.1.4 Τεχνολογικές αλλαγές σε πλατφόρμες, συσκευές ή συστήματα που τελούν υπό διερεύνηση.

**9.2 Η διαδικασία ανασκόπησης ανήκει στον CISO και πρέπει να περιλαμβάνει διαβούλευση με:**

9.2.1 Νομική Υπηρεσία και Κανονιστική Συμμόρφωση.

9.2.2 Υπεύθυνο Προστασίας Δεδομένων (DPO).

9.2.3 Ομάδες Επιχειρήσεων Ασφάλειας και ψηφιακής διερεύνησης.

9.2.4 Εσωτερικό Έλεγχο.

**9.3 Όλες οι αναθεωρήσεις πρέπει να:**

9.3.1 Ελέγχονται ως προς την έκδοση και να αποθηκεύονται στο αποθετήριο πολιτικών.

9.3.2 Κοινοποιούνται στα επηρεαζόμενα ενδιαφερόμενα μέρη, περιλαμβανομένων των ομάδων ψηφιακής διερεύνησης και απόκρισης.

9.3.3 Συνοδεύονται από επικαιροποιήσεις των σχετικών λειτουργικών διαδικασιών και του εκπαιδευτικού υλικού.

9.4 Έκτακτες ανασκοπήσεις πρέπει να ενεργοποιούνται μετά από κάθε κρίσιμο περιστατικό που περιλαμβάνει εσφαλμένο χειρισμό τεκμηρίων, αστοχία της αλυσίδας επιμέλειας ή ζητήματα νομικής παραδεκτότητας.

**10. Συναφείς πολιτικές και διασυνδέσεις**

**10.1 Η παρούσα πολιτική ευθυγραμμίζεται με και υποστηρίζεται από τις ακόλουθες πολιτικές του οργανισμού:**

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τη θεμελιώδη εντολή για διερεύνηση, έλεγχο τεκμηρίων και συμμόρφωση με την εφαρμοστέα νομοθεσία.

10.1.2 P5 – Πολιτική Διαχείρισης Αλλαγών: Διασφαλίζει ότι τα συστήματα που τελούν υπό διερεύνηση δεν τροποποιούνται κατά τη διάρκεια ενεργών διαδικασιών ψηφιακής διερεύνησης.

10.1.3 P14 – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Διέπει την ασφαλή διάθεση και τα χρονοδιαγράμματα διατήρησης για τεκμήρια και δεδομένα που σχετίζονται με υποθέσεις.

10.1.4 P18 – Πολιτική Κρυπτογραφικών Ελέγχων: Παρέχει απαιτήσεις κρυπτογράφησης για την αποθήκευση και μεταφορά ευαίσθητων δεδομένων ή δεδομένων με αποδεικτική αξία.

10.1.5 P22 – Πολιτική Καταγραφής και Παρακολούθησης: Διασφαλίζει τη διαθεσιμότητα αρχείων καταγραφής συμβάντων και τηλεμετρίας για συλλογή τεκμηρίων και συσχέτιση στο πλαίσιο ψηφιακής διερεύνησης.

10.1.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών: Ορίζει τις διαδρομές αρχικής αξιολόγησης περιστατικών και κλιμάκωσης όπου ενεργοποιούνται διαδικασίες ψηφιακής διερεύνησης.

10.1.7 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Επικυρώνει την τήρηση των πρωτοκόλλων ψηφιακής διερεύνησης και των απαιτήσεων αλυσίδας επιμέλειας μέσω τακτικών ελέγχων.

**11. Πρότυπα και πλαίσια αναφοράς**

11.1 Η παρούσα πολιτική ευθυγραμμίζεται με διεθνή πρότυπα ψηφιακής διερεύνησης και χειρισμού περιστατικών, διασφαλίζοντας την ακεραιότητα των τεκμηρίων, τη νομική υπερασπισιμότητα και τη συμμόρφωση σε πολλαπλές δικαιοδοσίες.

**11.2 ISO/IEC 27001**

11.2.1 Ρήτρα 8.1 – Υποστηρίζει τον επιχειρησιακό έλεγχο της ετοιμότητας ψηφιακής διερεύνησης και των διαδικασιών τεκμηρίων.

**11.3 ISO/IEC 27002**

11.3.1 Παράρτημα Α, Έλεγχος 5.25 – Αρμοδιότητες για τη διαχείριση περιστατικών: Απαιτεί καθορισμένους ρόλους για τον χειρισμό περιστατικών ασφάλειας πληροφοριών και διερευνήσεων.

11.3.2 Παράρτημα Α, Έλεγχος 5.26 – Αναφορά συμβάντων ασφάλειας πληροφοριών: Υποστηρίζει τη συλλογή τεχνουργημάτων που σχετίζονται με συμβάντα ως τεκμήρια.

11.3.3 Παράρτημα Α, Έλεγχος 5.27 – Απόκριση σε περιστατικά ασφάλειας πληροφοριών: Επιβάλλει δομημένη αποκατάσταση και διερεύνηση με βάση τα τεκμήρια.

11.3.4 Παράρτημα Α, Έλεγχος 8.27 – Ασφαλής ανάπτυξη και ψηφιακή διερεύνηση (όπου εφαρμόζεται): Αντιμετωπίζει την προστασία συστημάτων και εργαλείων κατά τις διερευνήσεις.

**11.4 ISO/IEC 27035:2016 (Μέρη 1 και 3)**

11.4.1 Περιγράφει τις αρχές της ανίχνευσης περιστατικών, της απόκρισης και της ετοιμότητας ψηφιακής διερεύνησης, συμπεριλαμβανομένου του σχεδιασμού, της αλυσίδας επιμέλειας και της διαχείρισης τεκμηρίων περιστατικών.

**11.5 NIST SP 800-53 Rev.5**

11.5.1 IR-1 έως IR-9, AU-6, PL-2: Ορίζει δομημένες απαιτήσεις για τον σχεδιασμό, την ανίχνευση, την ανάλυση, τον περιορισμό και την απόκριση σε περιστατικά ασφάλειας. Υποστηρίζει τη συλλογή και την ελεγξιμότητα των τεκμηρίων (AU-6) και διασφαλίζει την ευθυγράμμιση με τα σχέδια ασφάλειας συστημάτων και ιδιωτικότητας (PL-2) κατά τις διερευνήσεις.

**11.6 NIST SP 800-86**

11.6.1 Παρέχει κατευθύνσεις για την ενσωμάτωση των διαδικασιών ψηφιακής διερεύνησης στον ευρύτερο κύκλο ζωής της απόκρισης σε περιστατικά και για τη διασφάλιση ετοιμότητας ψηφιακής διερεύνησης.

**11.7 NIST SP 800-101 Rev.1**

11.7.1 Εστιάζει σε βέλτιστες πρακτικές για την απόκτηση, διατήρηση και ανάλυση ψηφιακών μέσων και τεκμηρίων από φορητές συσκευές με νομικά υπερασπίσιμο τρόπο.

**11.8 ΓΚΠΔ της ΕΕ (2016/679)**

11.8.1 Άρθρο 5 – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα: Εφαρμόζεται σε τεκμήρια που περιέχουν προσωπικά ή ευαίσθητα δεδομένα, διασφαλίζοντας την ελαχιστοποίηση και τον περιορισμό του σκοπού.

11.8.2 Άρθρα 33–34 – Γνωστοποίηση παραβίασης δεδομένων: Τα δεδομένα ψηφιακής διερεύνησης υποστηρίζουν τη συμμόρφωση με τις υποχρεώσεις γνωστοποίησης παραβίασης και τις διαδικασίες νομικής γνωστοποίησης.

**11.9 Οδηγία NIS2 της ΕΕ (2022/2555)**

11.9.1 Άρθρο 23 – Υποχρεώσεις αναφοράς: Η τεκμηρίωση και τα ευρήματα ψηφιακής διερεύνησης υποστηρίζουν την έγκαιρη και ακριβή αναφορά περιστατικών στις αρμόδιες αρχές.

**11.10 Κανονισμός DORA της ΕΕ (2022/2554)**

11.10.1 Άρθρο 17 – Αναφορά περιστατικών ΤΠΕ: Απαιτεί λεπτομερή αρχεία ανάλυσης βασικής αιτίας και αποδεικτικών στοιχείων για μείζονα περιστατικά που σχετίζονται με ΤΠΕ, ιδίως στον χρηματοοικονομικό τομέα.

**11.11 COBIT 2019**

11.11.1 DSS01.07 – Διαχείριση περιστατικών ασφάλειας: Επιβάλλει τεκμηρίωση περιστατικών και αυστηρότητα στη διερεύνηση.

11.11.2 DSS05.04 – Διαχείριση διερευνήσεων ασφάλειας: Τονίζει τη διατήρηση ψηφιακών τεκμηρίων και την υποστήριξη πειθαρχικών και νομικών ενεργειών.