					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P31S					Τίτλος εγγράφου: **Πολιτική Συλλογής Τεκμηρίων και Ψηφιακής Διερεύνησης**							
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, 6.3, 8	Σχεδιασμός βάσει κινδύνου, ενέργειες βελτίωσης και λειτουργικοί έλεγχοι για τη διασφάλιση της ακεραιότητας των τεκμηρίων
ISO/IEC 27002:2022	Έλεγχοι 5.24–5.27	Καθοδηγεί τον ασφαλή χειρισμό, τις ανασκοπήσεις μετά το περιστατικό και τις βελτιώσεις βάσει τεκμηρίων
ISO/IEC 27035-3:2016	Ρήτρες 6.3, 6.4, 7	Διασφαλίζει τον κατάλληλο σχεδιασμό, τη νόμιμη συλλογή και τον ασφαλή χειρισμό ψηφιακών τεκμηρίων με τεκμηρίωση της αλυσίδας επιμέλειας
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Ετοιμότητα ψηφιακής διερεύνησης, προστασία αρχείων καταγραφής ελέγχου και αποτελεσματική ενσωμάτωση στην απόκριση σε περιστατικά
ΓΚΠΔ της ΕΕ	Άρθρα 33, 34	Τεκμηρίωση και ιχνηλασιμότητα για παραβιάσεις δεδομένων προσωπικού χαρακτήρα
Οδηγία NIS2 της ΕΕ	Άρθρο 23	Ιχνηλάσιμη αναφορά περιστατικών και ασφαλής διαχείριση τεκμηρίων
Κανονισμός DORA της ΕΕ	Άρθρο 17(1), 17(2)	Διασφαλίζει τη συλλογή, αποθήκευση και διατήρηση τεκμηρίων για περιστατικά που σχετίζονται με ΤΠΕ, την εγκληματολογική ακεραιότητα και τα αιτήματα των ρυθμιστικών αρχών
COBIT 2019	DSS05.06, DSS05.07	Αξιόπιστη καταγραφή και δομημένος χειρισμός τεκμηρίων για ασφαλείς, ελέγξιμες διερευνήσεις

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο ο οργανισμός χειρίζεται ψηφιακά τεκμήρια που σχετίζονται με περιστατικά ασφάλειας, παραβιάσεις δεδομένων ή εσωτερικές διερευνήσεις. Διασφαλίζει ότι τα τεκμήρια συλλέγονται, αποθηκεύονται και διατηρούνται με νομικά ορθό τρόπο και με ετοιμότητα ελέγχου, υποστηρίζοντας τόσο την εσωτερική λήψη αποφάσεων όσο και πιθανές εξωτερικές ενέργειες.

1.2. Η πολιτική επιτρέπει σε μικρούς οργανισμούς να προστατεύουν την ακεραιότητα των αρχείων καταγραφής, των αρχείων και των εικόνων συστήματος, επιδεικνύοντας παράλληλα τη δέουσα επιμέλεια σύμφωνα με το ISO/IEC 27001, τον ΓΚΠΔ της ΕΕ και τα συναφή πρότυπα.

1.3. Υποστηρίζει την ετοιμότητα ψηφιακής διερεύνησης χωρίς να απαιτούνται προηγμένοι τεχνικοί πόροι ή πλήρως στελεχωμένη ομάδα Πληροφορικής, μέσω του καθορισμού σαφών αρμοδιοτήτων, διαδικασιών και απαιτήσεων διατήρησης.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1. Όλους τους εργαζομένους, τους εξωτερικούς παρόχους υπηρεσιών πληροφορικής και τους εξωτερικούς συμβούλους που συμμετέχουν στην απόκριση σε περιστατικά, στη διερεύνηση ή στην ανάλυση παραβιάσεων

2.1.2. Όλα τα εταιρικά συστήματα, συμπεριλαμβανομένων φορητών υπολογιστών, φορητών συσκευών, διακομιστών, λογαριασμών ηλεκτρονικού ταχυδρομείου, πλατφορμών SaaS και αποθήκευσης σε υποδομές νέφους (π.χ. Microsoft 365, Google Workspace)

2.1.3. Κάθε συμβάν που απαιτεί τεκμήρια για εσωτερική πειθαρχική ενέργεια, νομική υπεράσπιση, ασφαλιστικές αξιώσεις ή εμπλοκή ρυθμιστικής αρχής

2.2. Αυτό περιλαμβάνει τόσο πραγματικά όσο και πιθανολογούμενα συμβάντα που αφορούν:

2.2.1. διαρροή δεδομένων

2.2.2. εσωτερικές απειλές ή κακή χρήση

2.2.3. παραβιάσεις ασφάλειας (π.χ. κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση)

2.2.4. παράπονα πελατών που απαιτούν ψηφιακή επιβεβαίωση

2.2.5. αιτήματα από ρυθμιστικές ή διωκτικές αρχές

3. Στόχοι

3.1. Να διασφαλίζεται ότι όλα τα τεκμήρια συλλέγονται και διαχειρίζονται με τρόπο που διατηρεί την ακεραιότητα, την αυθεντικότητα και την αλυσίδα επιμέλειας.

3.2. Να αποτρέπεται η ακούσια τροποποίηση, διαγραφή ή εσφαλμένος χειρισμός αρχείων καταγραφής, αρχείων ή εικόνων συστήματος που ενδέχεται να απαιτηθούν για διερευνήσεις.

3.3. Να παρέχεται συνεπής και ελέγξιμη προσέγγιση στη διαχείριση τεκμηρίων, η οποία ικανοποιεί νομικές και κανονιστικές απαιτήσεις, όπως η κοινοποίηση παραβίασης βάσει του ΓΚΠΔ της ΕΕ και η ιχνηλασιμότητα βάσει της Οδηγίας NIS2 της ΕΕ.

3.4. Να ορίζονται σαφείς ρόλοι και αρμοδιότητες, ώστε να διασφαλίζεται η ταχεία, ασφαλής και νομικά σύννομη αποτύπωση τεκμηρίων κατά τη διάρκεια περιστατικών ασφάλειας.

3.5. Να υποστηρίζεται η ετοιμότητα ψηφιακής διερεύνησης σε επίπεδο ΜΜΕ, με ελαχιστοποίηση της πολυπλοκότητας και χωρίς διατάραξη της καθημερινής λειτουργίας.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής (GM)

4.1.1. Εγκρίνει όλες τις επίσημες διερευνήσεις που απαιτούν συλλογή τεκμηρίων.

4.1.2. Ανασκοπεί και εγκρίνει τις αναφορές περιστατικών που περιλαμβάνουν πιθανές νομικές ή πειθαρχικές ενέργειες.

4.1.3. Αποφασίζει αν πρέπει να ενημερωθούν εξωτερικός νομικός σύμβουλος ή ρυθμιστικές αρχές.

4.1.4. Διασφαλίζει ότι η πολιτική ανασκοπείται και επικαιροποιείται τακτικά.

4.2. Εξωτερικός πάροχος υπηρεσιών πληροφορικής / Διαχειριστής συστημάτων

4.2.1. Συλλέγει και διατηρεί ψηφιακά τεκμήρια ακολουθώντας ασφαλείς διαδικασίες.

4.2.2. Τεκμηριώνει χρονοσημάνσεις, στοιχεία συστημάτων και βήματα χειρισμού.

4.2.3. Ασφαλίζει όλο το συλλεγμένο υλικό σε προστατευμένη τοποθεσία.

4.2.4. Συνδράμει στην ψηφιακή διερεύνηση, εφόσον απαιτείται.

[... 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 της πολιτικής

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

9.1.1.1. η συμμόρφωση με τους ελέγχους του Παραρτήματος Α του ISO/IEC 27001

9.1.1.2. η διαρκής καταλληλότητα σε σχέση με τις τρέχουσες ψηφιακές πλατφόρμες και τις υπηρεσίες πληροφορικής

9.1.1.3. η επάρκεια των διαδικασιών καταγραφής, διατήρησης τεκμηρίων και ετοιμότητας ψηφιακής διερεύνησης

9.2. Συμβάντα ενεργοποίησης αναθεώρησης της πολιτικής

9.2.1. Η πολιτική ανασκοπείται και επικαιροποιείται επίσης μετά από:

9.2.1.1. οποιοδήποτε σημαντικό περιστατικό που απαιτεί συλλογή τεκμηρίων

9.2.1.2. αποτυχημένο έλεγχο ή αίτημα ρυθμιστικής αρχής, όπου αμφισβητήθηκε η ακεραιότητα των τεκμηρίων

9.2.1.3. υιοθέτηση νέων εργαλείων ή διαδικασιών για την απόκριση σε περιστατικά ή την παρακολούθηση συστημάτων

9.2.1.4. νομικές αλλαγές (π.χ. επικαιροποιημένη καθοδήγηση για τον ΓΚΠΔ της ΕΕ ή την Οδηγία NIS2 της ΕΕ)

9.3. Έγκριση και διανομή αλλαγών

9.3.1. Όλες οι αλλαγές ανασκοπούνται και εγκρίνονται από τον GM.

9.3.2. Η επικαιροποιημένη έκδοση κοινοποιείται σε:

9.3.2.1. εξωτερικούς παρόχους υπηρεσιών πληροφορικής και συμβούλους που συμμετέχουν σε διερευνήσεις

9.3.2.2. κάθε μέλος του προσωπικού με αρμοδιότητες διαχείρισης συστημάτων

9.3.3. Επικαιροποιημένο αντίγραφο διατηρείται στο αρχειακό αποθετήριο πολιτικών της εταιρείας και τίθεται στη διάθεση των ελεγκτών κατόπιν αιτήματος.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική αλληλεξαρτάται με τις ακόλουθες πολιτικές ευθυγραμμισμένες με τις ανάγκες των ΜΜΕ:

10.1.1. P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τις αρμοδιότητες για διερευνήσεις περιστατικών, αποφάσεις σχετικά με τεκμήρια και νομική κλιμάκωση.

10.1.2. P4S – Πολιτική Ελέγχου Πρόσβασης: Διασφαλίζει ότι μόνο εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση σε ευαίσθητα συστήματα και αρχεία καταγραφής κατά τη διάρκεια διερευνήσεων.

10.1.3. P22S – Πολιτική Καταγραφής και Παρακολούθησης: Παρέχει τα πρωτογενή δεδομένα που χρησιμοποιούνται ως εγκληματολογικά τεκμήρια και καθορίζει απαιτήσεις διατήρησης, ελέγχου πρόσβασης και καταγραφής.

10.1.4. P30S – Πολιτική Αντιμετώπισης Περιστατικών: Ενεργοποιεί την ανάγκη συλλογής τεκμηρίων και καθορίζει την επιχειρησιακή ροή που οδηγεί στη διατήρηση για σκοπούς ψηφιακής διερεύνησης.

10.1.5. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι κάθε δεδομένο προσωπικού χαρακτήρα που συλλέγεται ως τεκμήριο υποβάλλεται σε νόμιμη επεξεργασία σύμφωνα με τον ΓΚΠΔ της ΕΕ και τις συναφείς κανονιστικές απαιτήσεις.

10.2. Οι πολιτικές αυτές λειτουργούν συνδυαστικά για να υποστηρίζουν τη νομική τεκμηρίωση θέσης, την ακεραιότητα της διερεύνησης και την πλήρη ετοιμότητα ελέγχου κατά ISO/IEC 27001:2022.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 6.1 – Ο σχεδιασμός βάσει κινδύνου περιλαμβάνει ετοιμότητα απόκρισης και διαδικασίες τεκμηρίων.

11.1.2. Ρήτρα 6.3 – Υποστηρίζει ενέργειες βελτίωσης βάσει τεκμηρίων από περιστατικά.

11.1.3. Ρήτρα 8.1 – Απαιτεί λειτουργικούς ελέγχους για την ακεραιότητα των τεκμηρίων.

11.2. ISO/IEC 27002

11.2.1. Έλεγχοι 5.24–5.27 – Καθοδηγούν τον ασφαλή χειρισμό, τις ανασκοπήσεις μετά το περιστατικό και τις βελτιώσεις βάσει τεκμηρίων.

11.3. ISO/IEC 27035-3

11.3.1. Ρήτρες 6.3, 6.4 και 7.3 για τη διασφάλιση κατάλληλου σχεδιασμού, νόμιμης συλλογής και ασφαλούς χειρισμού ψηφιακών τεκμηρίων κατά την απόκριση σε περιστατικά, συμπεριλαμβανομένης της διατήρησης και της τεκμηρίωσης της αλυσίδας επιμέλειας.

11.4. NIST SP 800-53 Rev. 5

11.4.1. Τα IR-07, IR-08, AU-09 και AU-12 διασφαλίζουν ετοιμότητα ψηφιακής διερεύνησης, προστασία αρχείων καταγραφής ελέγχου και αποτελεσματική ενσωμάτωση της συλλογής τεκμηρίων στον κύκλο ζωής της απόκρισης σε περιστατικά.

11.5. NIST SP 800-86

11.5.1. Ορίζει βέλτιστες πρακτικές για την απόκτηση, ανάλυση και προστασία ψηφιακών τεκμηρίων κατά την απόκριση σε περιστατικά.

11.6. ΓΚΠΔ της ΕΕ

11.6.1. Άρθρα 33–34 – Απαιτούν τεκμηρίωση και ιχνηλασιμότητα περιστατικών και τεκμηρίων κατά την αναφορά παραβιάσεων δεδομένων προσωπικού χαρακτήρα.

11.7. Οδηγία NIS2 της ΕΕ (2022/2555)

11.7.1. Άρθρο 23 – Απαιτεί ιχνηλάσιμη αναφορά περιστατικών και ασφαλή διαχείριση τεκμηρίων για ουσιώδεις και σημαντικές οντότητες.

11.8. Κανονισμός DORA της ΕΕ

11.8.1. Άρθρο 17(1) – Διασφαλίζει ότι τα τεκμήρια που σχετίζονται με περιστατικά που αφορούν ΤΠΕ συλλέγονται και αποθηκεύονται με τρόπο που υποστηρίζει εγκληματολογικές διερευνήσεις.

11.8.2. Άρθρο 17(2) – Απαιτεί οι χρηματοοικονομικές οντότητες να διατηρούν όλα τα σχετικά δεδομένα και αρχεία καταγραφής που συνδέονται με συμβάντα ασφάλειας, ευθυγραμμισμένα με την εγκληματολογική ακεραιότητα και τα αιτήματα των ρυθμιστικών αρχών.

11.9. COBIT 2019

11.9.1. DSS05.06 – Παρακολούθηση, εντοπισμός και αναφορά περιστατικών: Δίνει έμφαση στην αξιόπιστη καταγραφή για την υποστήριξη της διερεύνησης.

11.9.2. DSS05.07 – Διερεύνηση και ενέργειες για περιστατικά: Απαιτεί δομημένο χειρισμό τεκμηρίων ώστε να καθίστανται δυνατές ασφαλείς και ελέγξιμες διερευνήσεις.