					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P22					Τίτλος εγγράφου: **Πολιτική Καταγραφής και Παρακολούθησης**							
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**

1. Σκοπός

1.1 Σκοπός της παρούσας πολιτικής είναι να θεσπίσει σαφείς και δεσμευτικές απαιτήσεις για την παραγωγή, προστασία, ανασκόπηση και ανάλυση των αρχείων καταγραφής που αποτυπώνουν κρίσιμα συμβάντα συστημάτων και ασφάλειας σε όλο το περιβάλλον πληροφορικής του οργανισμού.

1.2 Η καταγραφή και η παρακολούθηση είναι κρίσιμες για την ανίχνευση ανωμαλιών, την απόκριση σε απειλές, τη διερεύνηση με χρήση ψηφιακών πειστηρίων, την ετοιμότητα για έλεγχο και τη νομική συμμόρφωση. Η παρούσα πολιτική διασφαλίζει ότι όλα τα συμβάντα που παράγονται από τα συστήματα καταγράφονται, διατηρούνται και συσχετίζονται ορθά, με ακριβή συγχρονισμό χρόνου.

1.3 Η παρούσα πολιτική είναι ουσιώδης για την υποστήριξη της Ρήτρας 8.1 του ISO/IEC 27001 και των ελέγχων 8.15 (Καταγραφή), 8.16 (Παρακολούθηση) και 8.17 (Συγχρονισμός ρολογιών) του Παραρτήματος Α και αντιστοιχίζεται άμεσα με τις κανονιστικές υποχρεώσεις βάσει του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ, του Κανονισμού DORA της ΕΕ και του COBIT 2019.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα συστήματα, τις υπηρεσίες και τα περιβάλλοντα που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν δεδομένα τα οποία καλύπτονται από το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ), συμπεριλαμβανομένων των εξής:

2.1.1 υποδομές εντός εγκαταστάσεων, υπηρεσίες νέφους (π.χ. IaaS, PaaS, SaaS) και υβριδικά περιβάλλοντα

2.1.2 λειτουργικά συστήματα, βάσεις δεδομένων, εφαρμογές και δικτυακές συσκευές

2.1.3 συστήματα ασφάλειας, όπως SIEM, τείχη προστασίας, πλατφόρμες ανίχνευσης και απόκρισης τερματικών σημείων (EDR), συγκεντρωτές VPN και πάροχοι ταυτότητας

2.2 Τα ακόλουθα ενδιαφερόμενα μέρη εμπίπτουν στο πεδίο εφαρμογής:

2.2.1 εσωτερικοί χρήστες με δικαιώματα συστήματος ή διαχειριστικά δικαιώματα

2.2.2 προσωπικό υποδομών και λειτουργίας πληροφορικής

2.2.3 το Κέντρο Επιχειρήσεων Ασφάλειας (SOC) και οι ομάδες ανίχνευσης απειλών

2.2.4 προγραμματιστές λογισμικού και Ιδιοκτήτες Εφαρμογών

2.2.5 τρίτοι πάροχοι υπηρεσιών που διαχειρίζονται συστήματα τα οποία παράγουν αρχεία καταγραφής

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλα τα κρίσιμα συστήματα παράγουν αρχεία καταγραφής συμβάντων ασφάλειας και αρχεία δραστηριότητας συστήματος, τα οποία διατηρούνται σύμφωνα με κανονιστικές, νομικές και συμβατικές απαιτήσεις.

3.2 Να καθορίζονται οι ελάχιστοι τύποι συμβάντων και το ελάχιστο περιεχόμενο αρχείων καταγραφής που απαιτούνται για την ανίχνευση μη εξουσιοδοτημένων δραστηριοτήτων, την ιχνηλασιμότητα ενεργειών χρηστών και την υποστήριξη διερευνήσεων με χρήση ψηφιακών πειστηρίων.

3.3 Να εφαρμόζονται δικλίδες ασφαλείας για την αποτροπή παραποίησης αρχείων καταγραφής, μη εξουσιοδοτημένης διαγραφής ή ανεξέλεγκτης πρόσβασης στα δεδομένα καταγραφής.

3.4 Να θεσπίζονται κεντρικά συστήματα καταγραφής και ειδοποίησης (π.χ. SIEM) για τη συγκέντρωση, συσχέτιση και κλιμάκωση ύποπτης δραστηριότητας σχεδόν σε πραγματικό χρόνο.

3.5 Να διασφαλίζεται ο συγχρονισμός των ρολογιών των συστημάτων, ώστε να είναι δυνατή η ακριβής συσχέτιση μεταξύ συστημάτων και η ανάλυση περιστατικών.

3.6 Να υποστηρίζεται η συνεχής βελτίωση και η συμμόρφωση μέσω της ενσωμάτωσης της παρακολούθησης αρχείων καταγραφής στις διαδικασίες ελέγχου, διαχείρισης κινδύνων και διαχείρισης περιστατικών.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει ότι αυτή ευθυγραμμίζεται με την ανοχή κινδύνου του οργανισμού, τις απαιτήσεις ελέγχου και τις υποχρεώσεις του ΣΔΑΠ.

4.1.2 Εγκρίνει το πεδίο εφαρμογής της καταγραφής για ρυθμιζόμενα ή υψηλού κινδύνου συστήματα και ασκεί εποπτεία στην αναφορά συμμόρφωσης.

4.2 Υπεύθυνος Κέντρου Επιχειρήσεων Ασφάλειας (SOC)

4.2.1 Λειτουργεί και συντηρεί τις κεντρικές πλατφόρμες διαχείρισης αρχείων καταγραφής (π.χ. SIEM).

4.2.2 Καθορίζει κανόνες συγκέντρωσης αρχείων καταγραφής, κατώφλια ειδοποιήσεων και διαδρομές κλιμάκωσης για την αρχική αξιολόγηση περιστατικών.

4.2.3 Ανασκοπεί καθημερινές αναφορές και διασφαλίζει ότι οι ανωμαλίες αναλύονται, τεκμηριώνονται και κλιμακώνονται όπου 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 Η παρούσα πολιτική πρέπει να ανασκοπείται ετησίως ή νωρίτερα σε απόκριση σε:

9.1.1 σημαντικές αλλαγές στην αρχιτεκτονική συστημάτων ή στην υποδομή καταγραφής (π.χ. μετεγκατάσταση SIEM)

9.1.2 αναθεωρήσεις κανονιστικών απαιτήσεων καταγραφής (π.χ. υποχρεώσεις καταγραφής βάσει NIS2 ή DORA)

9.1.3 ευρήματα από ελέγχους ή ανασκοπήσεις μετά από περιστατικά

9.1.4 αναδυόμενες απειλές που απαιτούν ενισχυμένη παρακολούθηση (π.χ. εσωτερικές απειλές, παραβίαση της εφοδιαστικής αλυσίδας)

9.2 Η διαδικασία ανασκόπησης διενεργείται υπό τον συντονισμό του Υπεύθυνου Κέντρου Επιχειρήσεων Ασφάλειας (SOC), σε συνεργασία με τον Επικεφαλής Ασφάλειας Πληροφοριών, τη Διαχείριση Κινδύνων, τη Λειτουργία Συμμόρφωσης και τις ομάδες υποδομών πληροφορικής.

9.3 Οι εγκεκριμένες αλλαγές πρέπει να υπόκεινται σε έλεγχο εκδόσεων στο Μητρώο Εγγράφων του ΣΔΑΠ και να γνωστοποιούνται:

9.3.1 σε όλα τα ενδιαφερόμενα μέρη που έχουν ευθύνη για τη συντήρηση των συστημάτων καταγραφής

9.3.2 στους Ιδιοκτήτες Εφαρμογών και στους Ιδιοκτήτες Συστημάτων

9.3.3 σε τρίτους παρόχους που έχουν υποχρεώσεις τηλεμετρίας ή ενσωμάτωσης με το SIEM

9.4 Όλες οι καταργημένες εκδόσεις πρέπει να αρχειοθετούνται με ασφάλεια, με περιορισμένη πρόσβαση μόνο σε εξουσιοδοτημένους θεματοφύλακες του ΣΔΑΠ για σκοπούς ελέγχου και νομικούς σκοπούς.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 – Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει τη θεμελιώδη δέσμευση για την προστασία συστημάτων και δεδομένων, στο πλαίσιο της οποίας η καταγραφή και η παρακολούθηση λειτουργούν ως κρίσιμοι ανιχνευτικοί έλεγχοι και μηχανισμοί υποστήριξης της απόκρισης.

10.2 P4 – Πολιτική Ελέγχου Πρόσβασης. Διασφαλίζει ότι η προνομιούχα πρόσβαση, οι συνδέσεις χρηστών και τα συμβάντα εξουσιοδότησης καταγράφονται και παρακολουθούνται για κακή χρήση ή ανώμαλη συμπεριφορά.

10.3 P5 – Πολιτική Διαχείρισης Αλλαγών. Επιβάλλει την καταγραφή αλλαγών συστημάτων, εγκατάστασης διορθώσεων και επικαιροποιήσεων ρυθμίσεων που μπορεί να εισάγουν κίνδυνο ή μη εξουσιοδοτημένες τροποποιήσεις.

10.4 P21 – Πολιτική Ασφάλειας Δικτύου. Απαιτεί καταγραφή σε επίπεδο δικτύου (π.χ. αρχεία καταγραφής τειχών προστασίας, ειδοποιήσεις IDS/IPS, δραστηριότητα VPN) και ενσωμάτωση με το SIEM για ορατότητα σε ανωμαλίες της δικτυακής κίνησης και προστασία της περιμέτρου.

10.5 P23 – Πολιτική Συγχρονισμού Χρόνου. Επιβάλλει τη συνέπεια των ρολογιών μεταξύ συστημάτων, η οποία είναι απαραίτητη για αξιόπιστη καταγραφή και συσχέτιση συμβάντων ασφάλειας σε πολλαπλά περιβάλλοντα.

10.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών. Βασίζεται σε δεδομένα καταγραφής και μηχανισμούς ειδοποίησης για τον εντοπισμό, τη διερεύνηση και την απόκριση σε περιστατικά ασφάλειας, διατηρώντας παράλληλα ψηφιακά πειστήρια για ανασκόπηση μετά το περιστατικό.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί ελέγχους για την παρακολούθηση λειτουργιών και την προστασία από μη εξουσιοδοτημένη πρόσβαση και κακή χρήση συστημάτων.

11.2 ISO/IEC 27002:2022 – Έλεγχοι 8.15, 8.16, 8.17

11.2.1 Καθορίζει λεπτομερείς απαιτήσεις καταγραφής, συμπεριλαμβανομένου του ποια συμβάντα πρέπει να καταγράφονται, πώς πρέπει να προστατεύονται και να αναλύονται τα αρχεία καταγραφής και πώς διασφαλίζεται η αξιοπιστία των χρονοσημάνσεων μεταξύ συστημάτων.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 έως AU-12: Καλύπτει την επιλογή συμβάντων, την καταγραφή, την προστασία, την ανασκόπηση ελέγχου, την απόκριση σε αστοχίες ελέγχου και τη διατήρηση αρχείων ελέγχου.

11.3.2 SI-4 – Παρακολούθηση συστημάτων: Απαιτεί ενεργή παρακολούθηση συστημάτων με ειδοποιήσεις βάσει ανώμαλης δραστηριότητας.

11.3.3 SC-45 – Συγχρονισμός χρόνου συστήματος: Ενισχύει την ακρίβεια χρόνου για την ιχνηλασιμότητα συμβάντων και τη συσχέτιση περιστατικών.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Απαιτεί τεχνικά μέτρα, όπως η καταγραφή και η παρακολούθηση, ώστε να διασφαλίζονται η ασφάλεια και η λογοδοσία, ιδίως ως προς την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(e): Επιβάλλει συστήματα καταγραφής συμβάντων και παρακολούθησης για την ταχεία ανίχνευση και απόκριση σε περιστατικά ασφάλειας.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 9 – Διαχείριση κινδύνων ΤΠΕ: Απαιτεί μηχανισμούς για την ανίχνευση ανώμαλης δραστηριότητας, την καταγραφή περιστατικών και τη διατήρηση εγκληματολογικών δεδομένων.

11.6.2 Άρθρο 11 – Δοκιμές σχεδίων επιχειρησιακής συνέχειας ΤΠΕ: Δίνει έμφαση στη συνέχεια της παρακολούθησης και στην επικύρωση της διαθεσιμότητας των αρχείων καταγραφής κατά τη διάρκεια λειτουργικών διαταραχών.

11.7 COBIT 2019

11.7.1 DSS01.05 – Διαχείριση αρχείων καταγραφής ασφάλειας: Απαιτεί την εφαρμογή δυνατοτήτων καταγραφής για όλη την κρίσιμη υποδομή.

11.7.2 DSS05.04 – Παρακολούθηση συμβάντων ασφάλειας: Επιβάλλει παρακολούθηση και ανάλυση αρχείων καταγραφής σε πραγματικό χρόνο για την ανίχνευση και απόκριση σε συμβάντα.

11.7.3 MEA03 – Παρακολούθηση, αξιολόγηση και εκτίμηση συμμόρφωσης: Απαιτεί τακτική ανασκόπηση των πρακτικών καταγραφής και ευθυγράμμιση με τους στόχους ελέγχου.