					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P22S					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**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρα 8	Επιχειρησιακοί έλεγχοι, συμπεριλαμβανομένης της καταγραφής
ISO/IEC 27002:2022	Έλεγχοι 8.15, 8.16, 8.17	Καταγραφή συμβάντων, προστασία και παρακολούθηση
NIST SP 800-53 Rev.5	AU-2 έως AU-12, SI-4	Περιεχόμενο και ανασκόπηση αρχείων ελέγχου, διατήρηση, ανίχνευση ανωμαλιών, ειδοποιήσεις
ΓΚΠΔ της ΕΕ	Άρθρα 5(1)(f), 32, 33	Εμπιστευτικότητα και ακεραιότητα δεδομένων, τεχνικά μέτρα και γνωστοποίηση παραβίασης
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(d), 23	Μηχανισμοί καταγραφής για ανωμαλίες και αναφορά περιστατικών εντός 24 ωρών
Κανονισμός DORA της ΕΕ	Άρθρα 10, 15	Ψηφιακή λειτουργική ανθεκτικότητα, παρακολούθηση και καταγραφή παρόχων υπηρεσιών
COBIT 2019	DSS01.03, DSS05.02	Ιχνηλασιμότητα δραστηριότητας και προστασία μέσω καταγραφής και παρακολούθησης

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικούς ελέγχους καταγραφής και παρακολούθησης, ώστε να διασφαλίζονται η ασφάλεια, η λογοδοσία και η επιχειρησιακή ακεραιότητα των πληροφοριακών συστημάτων του οργανισμού.

1.2 Ορίζει τους τύπους συμβάντων που πρέπει να καταγράφονται, τον τρόπο αποθήκευσης των αρχείων καταγραφής, τον τρόπο ανασκόπησής τους, καθώς και τις αρμοδιότητες του προσωπικού και των παρόχων υπηρεσιών.

1.3 Η καταγραφή και η παρακολούθηση υποστηρίζουν την ανίχνευση απειλών, τη συμμόρφωση με κανονιστικές απαιτήσεις, την απόκριση σε περιστατικά και την εγκληματολογική διερεύνηση.

1.4 Η παρούσα πολιτική επιτρέπει στον οργανισμό να καλύπτει τις απαιτήσεις επιχειρησιακών ελέγχων του ISO/IEC 27001 και υποστηρίζει τη συνεχή ετοιμότητα για έλεγχο, την εμπιστοσύνη των πελατών και τη συμμόρφωση με τον ΓΚΠΔ της ΕΕ, την Οδηγία NIS2 της ΕΕ και τον Κανονισμό DORA της ΕΕ.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα συστήματα και όλους τους χρήστες του οργανισμού, συμπεριλαμβανομένων των εξής:

2.1.1 Σταθμοί εργασίας, φορητοί υπολογιστές, διακομιστές, τείχη προστασίας, μεταγωγείς, δρομολογητές και ασύρματα σημεία πρόσβασης

2.1.2 Υπηρεσίες υπολογιστικού νέφους που χρησιμοποιούνται για επιχειρησιακή λειτουργία (π.χ. ηλεκτρονικό ταχυδρομείο, αποθήκευση αρχείων, αντίγραφα ασφαλείας, εργαλεία συνεργασίας)

2.1.3 Λειτουργίες καταγραφής σε λογισμικό προστασίας από ιούς, εφαρμογές, λειτουργικά συστήματα και εξοπλισμό δικτύου

2.1.4 Όλους τους εργαζομένους, αναδόχους και παρόχους διαχειριζόμενων υπηρεσιών (MSP) που χρησιμοποιούν ή διαχειρίζονται συστήματα

2.1.5 Κάθε τοποθεσία στην οποία χρησιμοποιούνται εταιρικά πληροφοριακά συστήματα, συμπεριλαμβανομένων περιβαλλόντων απομακρυσμένης εργασίας, υβριδικών περιβαλλόντων ή BYOD

2.2 Η πολιτική εφαρμόζεται επίσης στα αρχεία καταγραφής που παράγονται από υπηρεσίες τρίτων, όταν ο οργανισμός διαθέτει διοικητική πρόσβαση ή συμβατικά δικαιώματα ελέγχου.

3. Στόχοι

3.1 Να διασφαλίζεται η καταγραφή της δραστηριότητας των συστημάτων, συμπεριλαμβανομένης της αυθεντικοποίησης, των αλλαγών διαμόρφωσης, της πρόσβασης σε ευαίσθητα δεδομένα και των ειδοποιήσεων ασφάλειας

3.2 Να διατηρούνται ασφαλή και ακριβή αρχεία καταγραφής για την ανίχνευση παραβιάσεων πολιτικής, σφαλμάτων συστήματος ή μη εξουσιοδοτημένων ενεργειών

3.3 Να καθίσταται δυνατή η ταχεία ανασκόπηση των αρχείων καταγραφής κατά τη διάρκεια περιστατικών, διερευνήσεων και ελέγχων

3.4 Να υποστηρίζεται ο συγχρονισμός χρόνου ώστε να διασφαλίζονται η ακεραιότητα και η συσχέτιση των δεδομένων καταγραφής

3.5 Να προστατεύονται τα αρχεία καταγραφής από παραποίηση, απώλεια ή πρόωρη διαγραφή

3.6 Να εκπληρώνονται οι νομικές και κανονιστικές υποχρεώσεις για λογοδοσία συστημάτων, ιχνηλασιμότητα και απόκριση σε παραβιάσεις

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Εγκρίνει την παρούσα πολιτική και διασφαλίζει την εφαρμογή της σε όλα τα επιχειρησιακά συστήματα

4.1.2 Ανασκοπεί ειδοποιήσεις υψηλής σοβαρότητας και σοβαρά ευρήματα ελέγχου που αναφέρονται από τις λειτουργίες πληροφορικής ή προστασίας δεδομένων

4.1.3 Εγκρίνει εξαιρέσεις όταν η καταγραφή ή η διατήρηση δεν μπορεί να εφαρμοστεί τεχνικά

4.2 Πάροχος Υποστήριξης Πληροφορικής / Εσωτερική λειτουργία Πληροφορικής

4.2.1 Υλοποιεί και ρυθμίζει την καταγραφή για λειτουργικά συστήματα, συσκευές δικτύου, εργαλεία προστασίας από ιούς και βασικές εφαρμογές

4.2.2 Διασφαλίζει ότι τα αρχεία καταγραφής διατηρούνται, δημιουργούνται αντίγραφα ασφαλείας και προστατεύονται από αλλοίωση

4.2.3 Ανασκοπεί τα αρχεία καταγραφής σε προγραμματισμένη βάση και διερευνά ύποπτη ή μη εξουσιοδοτημένη δραστηριότητα

4.2.4 Διατηρεί μηχανισμούς ειδοποίησης που επισημαίνουν ανώμαλη συμπεριφορά ή ενδείξεις εισβολής

[... 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 τουλάχιστον ετησίως από τον Γενικό Διευθυντή με την υποστήριξη του Παρόχου Υποστήριξης Πληροφορικής και του Συντονιστή Ιδιωτικότητας.

9.2 Εναύσματα ανασκόπησης

9.2.1 Έκτακτες ανασκοπήσεις πρέπει να διενεργούνται ως απόκριση στα εξής:

9.2.1.1 Ευρήματα σχετικά με αρχεία καταγραφής από εσωτερικούς ή εξωτερικούς ελέγχους

9.2.1.2 Περιστατικά ασφάλειας στα οποία τα αρχεία καταγραφής έλειπαν, είχαν αλλοιωθεί ή ήταν ανεπαρκή

9.2.1.3 Ουσιώδεις αλλαγές στην υποδομή πληροφορικής (π.χ. μετάβαση σε πλατφόρμες καταγραφής σε περιβάλλον υπολογιστικού νέφους)

9.2.1.4 Επικαιροποιήσεις νομικών ή κανονιστικών υποχρεώσεων (π.χ. ΓΚΠΔ της ΕΕ, Οδηγία NIS2 της ΕΕ, Κανονισμός DORA της ΕΕ)

9.3 Έλεγχος εκδόσεων

9.3.1 Όλες οι αλλαγές στην παρούσα πολιτική πρέπει να καταγράφονται με αριθμό έκδοσης, ημερομηνία και σύνοψη αναθεωρήσεων

9.3.2 Οι προηγούμενες εκδόσεις πρέπει να αρχειοθετούνται και να διατηρούνται για τουλάχιστον 3 έτη

9.3.3 Οι επικαιροποιημένες πολιτικές πρέπει να γνωστοποιούνται στα ενδιαφερόμενα μέρη που επηρεάζονται, ιδίως σε όσους διαθέτουν πρόσβαση σε επίπεδο συστήματος

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζει άμεσα και υποστηρίζεται από τις ακόλουθες πολιτικές ασφάλειας πληροφοριών για ΜΜΕ:

10.1.1 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι τα δεδομένα καταγραφής που περιέχουν προσωπικές πληροφορίες διαχειρίζονται με δικλίδες ακεραιότητας, διατήρησης και πρόσβασης σύμφωνα με τις απαιτήσεις του ΓΚΠΔ της ΕΕ.

10.1.2 P21S – Πολιτική Ασφάλειας Δικτύου: Παρέχει τη βάση για τη συλλογή αρχείων καταγραφής που σχετίζονται με τείχη προστασίας, ασύρματη πρόσβαση, VPN και παρακολούθηση της τμηματοποίησης.

10.1.3 P24S – Πολιτική Ασφαλούς Ανάπτυξης: Διασφαλίζει ότι τα αρχεία καταγραφής εφαρμογών (π.χ. για απόπειρες σύνδεσης, σφάλματα και εξαιρέσεις) ενσωματώνονται στον σχεδιασμό και στη λειτουργία του λογισμικού.

10.1.4 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Βασίζεται σε ακριβή και πλήρη δεδομένα καταγραφής για τον εντοπισμό, την ανάλυση και την απόκριση σε συμβάντα ασφάλειας πληροφοριών.

10.1.5 P23S – Πολιτική Συγχρονισμού Χρόνου: Διασφαλίζει συνεπείς και ιχνηλάσιμες χρονοσημάνσεις σε όλα τα συστήματα, επιτρέποντας τη συσχέτιση των αρχείων καταγραφής κατά τις διερευνήσεις.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 8.1 – Απαιτεί την εφαρμογή επιχειρησιακών ελέγχων για τον μετριασμό κινδύνων ασφάλειας πληροφοριών, συμπεριλαμβανομένης της καταγραφής.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 8.15 – Απαιτεί καταγραφή συμβάντων για την υποστήριξη της ανίχνευσης ανωμαλιών και της λογοδοσίας.

11.2.2 Έλεγχος 8.16 – Απαιτεί την προστασία των αρχείων καταγραφής από παραποίηση και μη εξουσιοδοτημένη πρόσβαση.

11.2.3 Έλεγχος 8.17 – Απαιτεί την παρακολούθηση συστημάτων για ασυνήθιστη δραστηριότητα και την επιβεβαίωση της αποτελεσματικότητας των ελέγχων παρακολούθησης.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 έως AU-12 – Καλύπτουν το περιεχόμενο των αρχείων ελέγχου, την ανασκόπηση, τη διατήρηση και τις αυτοματοποιημένες ειδοποιήσεις.

11.3.2 SI-4 – Απαιτεί την ανίχνευση ανωμαλιών συστήματος και την αναφορά ύποπτων συμβάντων.

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 5(1)(f) – Απαιτεί την ακεραιότητα και εμπιστευτικότητα των προσωπικών δεδομένων, η οποία περιλαμβάνει την καταγραφή της πρόσβασης.

11.4.2 Άρθρο 32 – Επιβάλλει τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της ασφάλειας, συμπεριλαμβανομένων της καταγραφής και της παρακολούθησης.

11.4.3 Άρθρο 33 – Απαιτεί έγκαιρη γνωστοποίηση παραβίασης, υποστηριζόμενη από αρχεία καταγραφής που επιτρέπουν ανάλυση βασικής αιτίας.

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(d) – Απαιτεί μηχανισμούς καταγραφής που ανιχνεύουν ανωμαλίες και παρέχουν υποστήριξη κατά τις διερευνήσεις περιστατικών.

11.5.2 Άρθρο 23 – Επιβάλλει την αναφορά περιστατικών εντός 24 ωρών, η οποία εξαρτάται από ακριβή και έγκαιρα δεδομένα καταγραφής.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 10 – Απαιτεί ψηφιακή λειτουργική ανθεκτικότητα, συμπεριλαμβανομένης της ιχνηλασιμότητας περιστατικών που σχετίζονται με ΤΠΕ μέσω καταγραφής.

11.6.2 Άρθρο 15 – Επιβάλλει την παρακολούθηση παρόχων υπηρεσιών, συμπεριλαμβανομένης της πρόσβασης σε αρχεία καταγραφής και των δικαιωμάτων ανασκόπησης.

11.7 COBIT 2019

11.7.1 DSS01.03 – Απαιτεί ιχνηλασιμότητα της δραστηριότητας συστημάτων μέσω καταγραφής και παρακολούθησης.

11.7.2 DSS05.02 – Αντιμετωπίζει την καταγραφή ως βασικό έλεγχο για την προστασία από κακόβουλο λογισμικό και άλλη μη εξουσιοδοτημένη δραστηριότητα.