

				Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P23				Τίτλος εγγράφου: <b>Πολιτική Συγχρονισμού Χρόνου</b>							
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

<p><b>Νομική σημείωση (πνευματικά δικαιώματα και περιορισμοί χρήσης)</b> (C) 2025 Clarysec LLC. All rights reserved.</p> <p>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: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
--

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρα 8	-
ISO/IEC 27002:2022	Έλεγχος 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
ΓΚΠΔ της ΕΕ	Άρθρο 32	-
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(e)	-
Κανονισμός DORA της ΕΕ	Άρθρα 9, 10	-
COBIT 2019	DSS05.04, MEA	-

## 1. Σκοπός

1.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίσει ότι όλα τα συστήματα, οι εφαρμογές, οι συσκευές και οι υπηρεσίες νέφους του οργανισμού διατηρούν συνεπείς και ακριβείς ρυθμίσεις χρόνου μέσω συγχρονισμού με καθορισμένες και αξιόπιστες πηγές χρόνου.

1.2 Ο ακριβής συγχρονισμός χρόνου είναι ουσιώδης για την αξιόπιστη καταγραφή συμβάντων, τις ασφαλείς επικοινωνίες, την ιχνηλασιμότητα ελέγχου, την απόκριση σε περιστατικά και την εγκληματολογική διερεύνηση. Η απόκλιση χρόνου μπορεί να οδηγήσει σε μη συσχετίσιμα αρχεία καταγραφής, αποτυχημένη αυθεντικοποίηση και ελλιπή κανονιστική αναφορά.

1.3 Η παρούσα πολιτική υποστηρίζει τον Έλεγχο 8.17 του Παραρτήματος Α του ISO/IEC 27001 και συναφή διεθνή πρότυπα, επιβάλλοντας ακρίβεια χρόνου και ανίχνευση απόκλισης ρολογιού σε όλη την υποδομή πληροφορικής του οργανισμού.

## 2. Πεδίο εφαρμογής

### 2.1 Η παρούσα πολιτική εφαρμόζεται στα εξής:

2.1.1 Σε όλα τα στοιχεία της υποδομής, συμπεριλαμβανομένων διακομιστών, σταθμών εργασίας, συσκευών δικτύου, τειχών προστασίας και συστημάτων Διαδικτύου των Πραγμάτων (IoT)

2.1.2 Σε εικονικά περιβάλλοντα και περιβάλλοντα νέφους (π.χ. AWS, Azure, Google Cloud)

2.1.3 Σε όλα τα συστήματα που συμμετέχουν στην καταγραφή, την αυθεντικοποίηση, την επεξεργασία συναλλαγών ή τη συσχέτιση συμβάντων ασφάλειας

2.1.4 Σε εσωτερικούς εργαζομένους, εργολάβους και τρίτους παρόχους υπηρεσιών που έχουν ευθύνη για συστήματα ευαίσθητα στον χρόνο

2.2 Συστήματα που παράγουν ή χρησιμοποιούν αρχεία με χρονοσήμανση — όπως καταχωρίσεις αρχείων καταγραφής, ειδοποιήσεις, αρχεία δραστηριότητας χρηστών ή ψηφιακά πειστήρια — θεωρούνται εντός πεδίου εφαρμογής.

## 3. Στόχοι

3.1 Να καθοριστεί συνεπής και κεντρικά διαχειριζόμενη αρχιτεκτονική συγχρονισμού χρόνου με χρήση εγκεκριμένων πηγών NTP ή ισοδύναμων μηχανισμών.

3.2 Να διασφαλίζεται ότι όλα τα συστήματα συγχρονίζουν τα ρολόγια τους σε καθορισμένα χρονικά διαστήματα και ότι κάθε απόκλιση ανιχνεύεται και διορθώνεται αυτόματα ή με ελάχιστη παρέμβαση.

**3.3 Να διατηρείται η ακρίβεια χρόνου σε υβριδικά, επιτόπια και νεφοϋπολογιστικά περιβάλλοντα, ώστε να υποστηρίζονται:**

3.3.1 Η αξιόπιστη συσχέτιση συμβάντων και η απόκριση σε περιστατικά

3.3.2 Η κανονιστική συμμόρφωση με πρότυπα όπως το ISO 27001, ο ΓΚΠΔ, η NIS2 και ο DORA

3.3.3 Η προστασία από επιθέσεις επανάληψης και αστοχίες αυθεντικοποίησης που βασίζονται στον χρόνο

3.4 Να καθοριστούν σαφείς ρόλοι, διαδικασίες διαχείρισης εξαιρέσεων και μηχανισμοί ελέγχου για τη διατήρηση της εφαρμογής της πολιτικής.

3.5 Να διασφαλίζεται ότι ανωμαλίες σχετικές με τον χρόνο καταγράφονται, παράγουν ειδοποιήσεις και κλιμακώνονται όταν υπερβαίνουν τα επιτρεπτά όρια.

#### **4. Ρόλοι και αρμοδιότητες**

##### **4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)**

4.1.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει την ευθυγράμμιση της με τους επιχειρησιακούς ελέγχους του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) και τις κανονιστικές υποχρεώσεις.

4.1.2 Εγκρίνει την επιλογή εταιρικών πηγών χρόνου και επικυρώνει τις διαδικασίες αναφοράς συγχρονισμού χρόνου.

##### **4.2 Υπεύθυνος Υπηρεσιών Υποδομής / Επικεφαλής Μηχανικής Δικτύων**

4.2.1 Συντηρεί τους πρωτεύοντες και δευτερεύοντες διακομιστές NTP του οργανισμού ή την καθορισμένη διάταξη πηγών χρόνου.

4.2.2 Διασφαλίζει ότι όλες οι δικτυωμένες συσκευές και οι εικονικές παρουσίες συγχρονίζουν τον χρόνο σε κατάλληλα χρονικά διαστήματα.

4.2.3 Παρακολουθεί τα αρχεία καταγραφής συγχρονισμού χρόνου, τις ειδοποιήσεις απόκλισης ρολογιού και τις συνθήκες αστοχίας.

[ ... 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 υπό τις ακόλουθες συνθήκες:**

9.1.1 Εντοπισμός επιθέσεων που βασίζονται στον χρόνο ή αστοχιών καταγραφής

9.1.2 Αλλαγές στη βασική υποδομή χρόνου (π.χ. νέοι εταιρικοί διακομιστές NTP ή επικαιροποιήσεις πρωτοκόλλων)

9.1.3 Αποκλίσεις χρόνου σε πλατφόρμες νέφους ή περιφερειακές αλλαγές υπηρεσιών

9.1.4 Ευρήματα μετά από περιστατικό που εντοπίζουν την ασυμφωνία χρόνου ως συντελεστικό παράγοντα

9.2 Η ανασκόπηση πρέπει να συντονίζεται από τον Επικεφαλής Υποδομών, με απαιτούμενη συνεισφορά από το SOC, την Ασφάλεια Εφαρμογών και τα ενδιαφερόμενα μέρη συμμόρφωσης.

9.3 Οι αναθεωρήσεις πρέπει να τεκμηριώνονται στο Μητρώο Εγγράφων του ΣΔΑΠ και να γνωστοποιούνται στα επηρεαζόμενα εσωτερικά ενδιαφερόμενα μέρη και στα ενδιαφερόμενα μέρη τρίτων μερών.

9.4 Οι ιστορικές εκδόσεις της πολιτικής πρέπει να αρχειοθετούνται με ασφάλεια, να υπόκεινται σε έλεγχο εκδόσεων και να είναι διαθέσιμες για αιτήματα ελέγχου συμμόρφωσης ή νομικού ελέγχου.

#### **10. Συναφείς πολιτικές και διασυνδέσεις**

10.1 P1 – Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει τη συνολική εντολή για τη διασφάλιση της ακεραιότητας και της ιχνηλασιμότητας όλων των πληροφοριακών συστημάτων, για την οποία η ακρίβεια χρόνου αποτελεί θεμελιώδη προϋπόθεση.

10.2 P5 – Πολιτική Διαχείρισης Αλλαγών. Διέπει τις τροποποιήσεις στις ρυθμίσεις συστημάτων, συμπεριλαμβανομένων των προσαρμογών πηγών χρόνου, διασφαλίζοντας κατάλληλη τεκμηρίωση, δοκιμές και σχέδια επαναφοράς.

10.3 P22 – Πολιτική Καταγραφής και Παρακολούθησης. Εξαρτάται άμεσα από τον συγχρονισμένο χρόνο, ώστε να διασφαλίζεται η αλληλουχία συμβάντων, η συσχέτιση αρχείων καταγραφής και η ακεραιότητα της διερεύνησης περιστατικών σε ετερογενή συστήματα.

10.4 P30 – Πολιτική Αντιμετώπισης Περιστατικών (P30). Βασίζεται σε ακριβείς χρονοσημάνσεις για εγκληματολογικές διερευνήσεις, χρονογραμμές περιστατικών και αποδεικτικά στοιχεία αλυσίδας επιμέλειας. Ο ανακριβής χρόνος υπονομεύει την αξιοπιστία των αναφορών περιστατικών.

10.5 P20 – Πολιτική Προστασίας Τερματικών / Κακόβουλου Λογισμικού. Απαιτεί ακριβή χρονικά ευθυγραμμισμένη ειδοποίηση και ανάλυση συμπεριφοράς για την ανίχνευση εξάπλωσης κακόβουλου λογισμικού, πλευρικής κίνησης και ανωμαλιών πρόσβασης.

10.6 P6 – Πολιτική Διαχείρισης Κινδύνων. Ορίζει την αντιμετώπιση του αποσυγχρονισμού ως δυνητικού λειτουργικού και εγκληματολογικού κινδύνου, απαιτώντας τις δικλίδες που ορίζονται στην παρούσα πολιτική για τον μετριασμό του αντίκτυπου.

## **11. Πρότυπα και πλαίσια αναφοράς**

### **11.1 ISO/IEC 27001**

11.1.1 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί την ενσωμάτωση ακριβών τεχνικών ελέγχων, όπως ο συγχρονισμός χρόνου συστημάτων, για αξιόπιστη επιχειρησιακή εκτέλεση.

### **11.2 ISO/IEC 27002:2022 – Έλεγχος 8**

11.2.1 Ενισχύει την ακρίβεια ρολογιού και επιβάλλει τη συνεπή διαχείριση του χρόνου συστήματος σε επίπεδο οργανισμού, ώστε να διευκολύνεται η σύγκριση αρχείων καταγραφής, η διερεύνηση και η επικύρωση ασφαλών συναλλαγών.

### **11.3 NIST SP 800-53 Rev.5**

11.3.1 SC-45 – Συγχρονισμός χρόνου συστήματος: Απαιτεί συγχρονισμό χρόνου με χρήση έγκυρων πηγών σε όλα τα στοιχεία εντός του ορίου ελέγχου ενός συστήματος.

11.3.2 AU-8 – Χρονοσημάνσεις: Διασφαλίζει ότι τα συμβάντα φέρουν ακριβείς χρονοσημάνσεις και παρέχει ιχνηλασιμότητα για έλεγχο και απόκριση σε περιστατικά.

### **11.4 ΓΚΠΔ της ΕΕ (2016/679)**

11.4.1 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Αν και δεν αναφέρεται ρητά στον χρόνο, επιβάλλει τη χρήση κατάλληλων τεχνικών μέτρων — συμπεριλαμβανομένων διαδρομών ελέγχου και αρχείων καταγραφής — τα οποία εξαρτώνται εγγενώς από συγχρονισμένες χρονοσημάνσεις για την εγκυρότητα και την ακεραιότητά τους.

### **11.5 Οδηγία NIS2 της ΕΕ (2022/2555)**

11.5.1 Άρθρο 21(2)(e): Απαιτεί δυνατότητες καταγραφής και ανίχνευσης, οι οποίες προϋποθέτουν ακριβή συγχρονισμό χρόνου για διασυστημική συσχέτιση και έγκαιρη απόκριση.

### **11.6 Κανονισμός DORA της ΕΕ (2022/2554)**

11.6.1 Άρθρο 9 – Διαχείριση κινδύνων ΤΠΕ: Επιβάλλει ακριβή τηλεμετρία συστημάτων για την παρακολούθηση κινδύνων και την ανίχνευση ανωμαλιών, η οποία εξαρτάται από ακριβή συγχρονισμό ρολογιών.

11.6.2 Άρθρο 10 – Επιχειρησιακή συνέχεια ΤΠΕ: Επιβάλλει ελέγχους που διασφαλίζουν την ακεραιότητα των συστημάτων κατά τη διάρκεια διαταραχών, συμπεριλαμβανομένων χρονικά ευθυγραμμισμένων αρχείων συμβάντων.

### **11.7 COBIT 2019**

11.7.1 DSS05.04 – Παρακολούθηση περιστατικών ασφάλειας: Απαιτεί ακεραιότητα χρονοσημάνσεων για αποτελεσματική ανάλυση αρχείων καταγραφής και ανίχνευση απειλών.

11.7.2 ΜΕΑ03 – Παρακολούθηση, αξιολόγηση και εκτίμηση της συμμόρφωσης: Ο συγχρονισμός χρόνου υποστηρίζει ακριβή έλεγχο συμμόρφωσης και κύκλους αναφοράς.