

NIS2.

Από την απαίτηση στην πράξη.

Κατανοήστε το πλαίσιο. Εντοπίστε τα κενά.
Οργανώστε ένα πλάνο με υπευθύνους και τεκμήρια.

ΑΠΑΙΤΗΣΕΙΣ

10 θεματικές.
Συγκεκριμένα τεκμήρια.

- Διακυβέρνηση
- Περιστατικά
- Ανθεκτικότητα



01 / ΤΟ ΠΛΑΙΣΙΟ

Η ετοιμότητα θέλει οργάνωση.

Η NIS2 αφορά τεχνικά μέτρα, διαδικασίες και αποφάσεις διοίκησης. Μία χρήσιμη αφετηρία είναι η πραγματική εικόνα του οργανισμού σας.

ΔΙΟΙΚΗΣΗ

Ποιος εγκρίνει και εποπτεύει τα μέτρα;

ΕΦΑΡΜΟΓΗ

Ποιοι έλεγχοι λειτουργούν στην πράξη;

ΤΕΚΜΗΡΙΑ

Ποια στοιχεία αποδεικνύουν την εφαρμογή;

ΠΡΩΤΑ ΕΠΙΒΕΒΑΙΩΣΤΕ ΤΗΝ ΥΠΑΓΩΓΗ

Ο τομέας και η συγκεκριμένη υπηρεσία, το μέγεθος και οι ειδικές διατάξεις εξετάζονται μαζί. Υπάρχουν περιπτώσεις ανεξαρτήτως μεγέθους. Ένας αριθμός εργαζομένων μόνος του δεν αρκεί για οριστικό συμπέρασμα.

A**Τομέας & υπηρεσία**

Ελέγξτε τα Παραρτήματα I και II του Ν. 5160/2024.

B**Μέγεθος & σχέσεις**

Εξετάστε προσωπικό, οικονομικά στοιχεία και συνδεδεμένες επιχειρήσεις.

Γ**Ειδικές περιπτώσεις**

Ελέγξτε ειδικούς κανόνες για υπηρεσίες ή φορείς ανεξαρτήτως μεγέθους.

Για τις υπόχρεες οντότητες προβλέπεται εγγραφή στην ΕΑΚ. Ελέγξτε την επίσημη πλατφόρμα και τις οδηγίες της αρχής: nis2register.cyber.gov.gr

02 / ΑΠΑΙΤΗΣΕΙΣ & ΤΕΚΜΗΡΙΑ

Οι 10 θεματικές στην πράξη.

Άρθρο 21 της NIS2 / άρθρο 15 Ν. 5160/2024. Τα προτεινόμενα τεκμήρια είναι πρακτικά παραδείγματα οργάνωσης.

01

Ανάλυση κινδύνων & πολιτικές ασφάλειας

Πολιτικές ανάλυσης κινδύνων και ασφάλειας πληροφοριακών συστημάτων.

Τεκμήριο: Μητρώο κινδύνων με υπεύθυνο, αξιολόγηση, μέτρα αντιμετώπισης και ημερομηνία επανεξέτασης.

02

Διαχείριση περιστατικών

Οργανωμένη ανίχνευση, χειρισμός και αντιμετώπιση περιστατικών.

Τεκμήριο: Σχέδιο απόκρισης, στοιχεία επικοινωνίας, χρονολόγιο άσκησης και πρότυπα αναφοράς.

03

Επιχειρησιακή συνέχεια & ανάκαμψη

Αντίγραφα ασφαλείας, ανάκαμψη από καταστροφές και διαχείριση κρίσεων.

Τεκμήριο: Σχέδιο συνέχειας, στόχοι RTO/RPO και πρακτικό επιτυχημένης δοκιμής επαναφοράς.

04

Ασφάλεια εφοδιαστικής αλυσίδας

Ασφάλεια σχέσεων με άμεσους προμηθευτές και παρόχους υπηρεσιών.

Τεκμήριο: Μητρώο κρίσιμων προμηθευτών, έλεγχοι αξιολόγησης και συμφωνημένες απαιτήσεις ασφάλειας.

05

Ασφαλής κύκλος ζωής συστημάτων

Ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση, με χειρισμό ευπαθειών.

Τεκμήριο: Απογραφή εκδόσεων, αρχείο ενημερώσεων, αξιολόγηση ευπαθειών και έλεγχος αλλαγών.

02 / ΑΠΑΙΤΗΣΕΙΣ & ΤΕΚΜΗΡΙΑ

Οι 10 θεματικές στην πράξη.

Άρθρο 21 της NIS2 / άρθρο 15 Ν. 5160/2024. Τα προτεινόμενα τεκμήρια είναι πρακτικά παραδείγματα οργάνωσης.

06

Αξιολόγηση αποτελεσματικότητας μέτρων

Πολιτικές και διαδικασίες αξιολόγησης των μέτρων διαχείρισης κινδύνων.

Τεκμήριο: Αποτελέσματα ελέγχων, δείκτες, διορθωτικές ενέργειες και ανασκόπηση από τη διοίκηση.

07

Κυβερνοϋγιεινή & εκπαίδευση

Βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση κυβερνοασφάλειας.

Τεκμήριο: Πρόγραμμα εκπαίδευσης, συμμετοχές και αποτελέσματα ασκήσεων προσαρμοσμένων στους ρόλους.

08

Κρυπτογραφία & κρυπτογράφηση

Πολιτικές χρήσης κρυπτογραφίας και, όπου ενδείκνυται, κρυπτογράφησης.

Τεκμήριο: Καταγραφή χρήσεων κρυπτογράφησης, υπευθύνων και κανόνων διαχείρισης κλειδιών.

09

Προσωπικό, πρόσβαση & περιουσιακά στοιχεία

Ασφάλεια ανθρώπινων πόρων, έλεγχος πρόσβασης και διαχείριση περιουσιακών στοιχείων.

Τεκμήριο: Απογραφή συστημάτων και διαδικασία ένταξης, αλλαγής ρόλου, αποχώρησης και επανελέγχου δικαιωμάτων.

10

Ισχυρή ταυτοποίηση & ασφαλείς επικοινωνίες

MFA ή συνεχής ταυτοποίηση και ασφαλείς επικοινωνίες, κατά περίπτωση.

Τεκμήριο: Καταγραφή κάλυψης MFA και ασφαλών καναλιών επικοινωνίας, με τεκμηριωμένες εξαιρέσεις.

03 / ΣΗΜΑΝΤΙΚΑ ΠΕΡΙΣΤΑΤΙΚΑ

Προετοιμαστείτε πριν συμβεί.

Ο γενικός κανόνας προβλέπει προειδοποίηση και κοινοποίηση χωρίς αδικαιολόγητη καθυστέρηση, εντός των ανώτατων ορίων που ακολουθούν.

24

ΩΡΕΣ

Έγκαιρη προειδοποίηση

Από τη στιγμή που έγινε αντιληπτό το σημαντικό περιστατικό. Αρχική ενημέρωση προς την ΕΑΚ.

72

ΩΡΕΣ

Κοινοποίηση περιστατικού

Από τη γνώση του σημαντικού περιστατικού. Αρχική εκτίμηση σοβαρότητας, επιπτώσεων και διαθέσιμων ενδείξεων παραβίασης.

1

ΜΗΝΑΣ

Τελική έκθεση

Από την κοινοποίηση περιστατικού. Περιγραφή, πιθανή αιτία, επιπτώσεις και μέτρα αντιμετώπισης.

Υπάρχουν ειδικές ρυθμίσεις: ενδιάμεση έκθεση κατόπιν αιτήματος, περιστατικά σε εξέλιξη και κοινοποίηση ορισμένων περιστατικών παρόχων υπηρεσιών εμπιστοσύνης εντός 24 ωρών. Ελέγξτε το άρθρο 16 και τις ισχύουσες οδηγίες της ΕΑΚ.

ΤΙ ΝΑ ΕΧΕΤΕ ΕΤΟΙΜΟ

Ομάδα απόκρισης / στοιχεία επικοινωνίας / σαφή κριτήρια αξιολόγησης / πρότυπα αναφοράς / χρονολόγιο / διαθέσιμα τεκμήρια / δοκιμή της διαδικασίας.

Μία σαφής σειρά ενεργειών.

Προσαρμόστε τη σειρά εργασιών στις υποδομές, στις υπηρεσίες και στις υποχρεώσεις σας. Οι φάσεις είναι πρόταση οργάνωσης, όχι κανονιστικές προθεσμίες.

01

Επιβεβαιώστε

Καταγράψτε νομική οντότητα, υπηρεσίες και υποχρεώσεις. Ελέγξτε υπαγωγή, κατηγορία οντότητας και εγγραφή στην ΕΑΚ.

Παραδοτέο: σημείωμα υπαγωγής και υπεύθυνος παρακολούθησης.

02

Αποτυπώστε

Οργανώστε απογραφή κρίσιμων συστημάτων, δεδομένων, υπηρεσιών και προμηθευτών. Αντιστοιχίστε υπευθύνους.

Παραδοτέο: ενημερωμένη απογραφή και βασικές εξαρτήσεις.

03

Ιεραρχήστε

Συνδέστε τους κινδύνους με τις 10 θεματικές. Αναθέστε ενέργειες με ημερομηνία και κριτήριο ολοκλήρωσης.

Παραδοτέο: πλάνο ενεργειών με ιδιοκτησία και προτεραιότητες.

04

Δοκιμάστε & τεκμηριώστε

Εκτελέστε άσκηση περιστατικού και επαναφοράς. Κρατήστε αποτελέσματα ελέγχων και αποφάσεις ανασκόπησης.

Παραδοτέο: φάκελος τεκμηρίων και εικόνα προς τη διοίκηση.

Η λίστα ελέγχου της ομάδας.

Χρησιμοποιήστε τη σε συνάντηση εργασίας. Σημειώστε τι έχει τεκμηριωθεί, ποιος αναλαμβάνει και ποια είναι η επόμενη ημερομηνία ελέγχου.

ΘΕΜΑΤΙΚΗ	ΥΠΕΥΘΥΝΟΣ	ΗΜΕΡΟΜΗΝΙΑ
☐ 01 Ανάλυση κινδύνων & πολιτικές ασφάλειας		
☐ 02 Διαχείριση περιστατικών		
☐ 03 Επιχειρησιακή συνέχεια & ανάκαμψη		
☐ 04 Ασφάλεια εφοδιαστικής αλυσίδας		
☐ 05 Ασφαλής κύκλος ζωής συστημάτων		
☐ 06 Αξιολόγηση αποτελεσματικότητας μέτρων		
☐ 07 Κυβερνοϋγιεινή & εκπαίδευση		
☐ 08 Κρυπτογραφία & κρυπτογράφηση		
☐ 09 Προσωπικό, πρόσβαση & περιουσιακά στοιχεία		
☐ 10 Ισχυρή ταυτοποίηση & ασφαλείς επικοινωνίες		

Η ΠΡΩΤΗ ΜΑΣ ΠΡΟΤΕΡΑΙΟΤΗΤΑ

Επόμενη ανασκόπηση:

06 / ΠΗΓΕΣ & ΣΥΝΕΧΕΙΑ

Από τον οδηγό στην εφαρμογή.

Συνδέστε κάθε απαίτηση με συγκεκριμένο έλεγχο, υπεύθυνο, ενέργεια και τεκμήριο. Επανεξετάζετε την εικόνα σας με βάση πραγματικά στοιχεία.

ΞΕΚΙΝΗΣΤΕ ΜΕ ΤΟ CIVERA

Αποτυπώστε τη σημερινή σας εικόνα.

survey.civera.gr / info@civera.gr

ΑΥΤΟΑΞΙΟΛΟΓΗΣΗ: ΠΩΣ ΔΙΑΒΑΖΕΤΑΙ Ο ΔΕΙΚΤΗΣ

Οι 10 ισοβαρείς απαντήσεις δίνουν 2 βαθμούς για διαθέσιμη τεκμηρίωση, 1 για μερική εφαρμογή και 0 για «όχι / δεν γνωρίζω». Ο δείκτης είναι το άθροισμα / 20×100 . Πρόκειται για δηλώσεις χωρίς επαλήθευση. Ακόμη και 100% δεν αποδεικνύει νομική συμμόρφωση.

ΘΕΣΜΙΚΕΣ ΠΗΓΕΣ

- 01 Ν. 5160/2024 - ΦΕΚ Α' 195/27.11.2024
- 02 Οδηγία (ΕΕ) 2022/2555 - EUR-Lex
- 03 Εγγραφή οντοτήτων - ΕΑΚ
- 04 Συχνές ερωτήσεις εγγραφής - ΕΑΚ

Έκδοση 19 Οκτωβρίου 2026. Συνοπτική παρουσίαση βασικών διατάξεων. Για την εφαρμογή εξετάζονται οι ισχύουσες τροποποιήσεις και οδηγίες της ΕΑΚ. Το ενημερωτικό περιεχόμενο δεν υποκαθιστά εξατομικευμένη νομική ή τεχνική αξιολόγηση.