****

**Εθνική Στρατηγική Κυβερνοασφάλειας 2026 – 2030**

**Ερωτηματολόγιο Διαβούλευσης**

**Γενική Διεύθυνση Επιτελικού Σχεδιασμού**

**Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας**

**Οκτώβριος 2025**

Πίνακας Περιεχομένων

[Μήνυμα Διοικητή Εθνικής Αρχής Κυβερνοασφάλειας 3](#_Toc209090158)

[Εισαγωγή 5](#_Toc209090159)

[Εθνική Στρατηγική Κυβερνοασφάλειας 2026 - 2030 5](#_Toc209090160)

[Στόχοι της Δημόσιας Διαβούλευσης 6](#_Toc209090161)

[Οδηγίες Συμπλήρωσης 7](#_Toc209090162)

[Εμπιστευτικότητα 8](#_Toc209090163)

[Ερωτηματολόγιο Διαβούλευσης ΕΣΚ 2026 - 2030 9](#_Toc209090164)

[Τμήμα Α: Στοιχεία Επικοινωνίας 9](#_Toc209090165)

[Τμήμα Β: Ερωτήσεις 9](#_Toc209090166)

[Θεματική Ενότητα 1: Στρατηγικές Κατευθύνσεις και Διακυβέρνηση 9](#_Toc209090167)

[Θεματική Ενότητα 2: Νομοθεσία, Ρυθμιστικά Μέτρα και Συμμόρφωση 10](#_Toc209090168)

[Θεματική Ενότητα 3: Τεχνολογικές Προκλήσεις και Καινοτομία 11](#_Toc209090169)

[Θεματική Ενότητα 4: Δεξιότητες, Εκπαίδευση και Ανθρώπινο Δυναμικό 12](#_Toc209090170)

[Θεματική Ενότητα 5: Συνεργασίες, Οικοσύστημα και Διεθνής Διάσταση 12](#_Toc209090171)

[Ανοικτή Ερώτηση 13](#_Toc209090172)

# Μήνυμα Διοικητή Εθνικής Αρχής Κυβερνοασφάλειας

Η κυβερνοασφάλεια αποτελεί στρατηγικό πυλώνα της εθνικής ανθεκτικότητας και της ψηφιακής ασφάλειας της χώρας μας, διασφαλίζοντας την απρόσκοπτη λειτουργία της δημόσιας διοίκησης, την προστασία των κρίσιμων υποδομών, την ομαλή λειτουργία της οικονομίας και την ενίσχυση της εμπιστοσύνης των πολιτών στην ψηφιακή διακυβέρνηση. Η περίοδος 2020 –2025 σηματοδότησε τη μετάβαση από αποσπασματικές πρωτοβουλίες σε μία συνεκτική, θεσμοθετημένη και επιχειρησιακά οργανωμένη εθνική στρατηγική. Η θεσμική ενδυνάμωση της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ), αρχικά με τους ν. 4635/2019 και 4961/2022, αλλά κυρίως με τον ιδρυτικό της νόμο 5086/2024, καθώς και η πλήρης σύγκλιση με το ευρωπαϊκό κανονιστικό πλαίσιο μέσω της ενσωμάτωσης της Οδηγίας 2022/2555 (Οδηγία NIS2) με το νόμο 5160/2024, δημιούργησαν ένα στιβαρό θεσμικό θεμέλιο πολιτικής και διακυβέρνησης στον τομέα της κυβερνοασφάλειας. Πλέον, η κυβερνοασφάλεια αποτελεί για τη χώρα μας μία διακριτή δημόσια πολιτική, με οριζόντιο χαρακτήρα και υψηλή πολιτική προτεραιότητα.

Ωστόσο, το ταχέως εξελισσόμενο τοπίο απειλών και τεχνολογιών απαιτεί μία ακόμη πιο φιλόδοξη προσέγγιση για την περίοδο 2026–2030. Η εντεινόμενη χρήση της τεχνητής νοημοσύνης, ο κρίσιμος ρόλος και η ασφάλεια της εφοδιαστικής αλυσίδας, οι υβριδικές επιθέσεις που συνδυάζουν κυβερνοαπειλές με επιχειρήσεις παραπληροφόρησης, καθώς και οι γεωπολιτικές ανακατατάξεις, επιτάσσουν με εμφατικό τρόπο την ριζική αναθεώρηση και λειτουργική αναβάθμιση των υφιστάμενων δομών και εργαλείων. Τα ανωτέρω σκιαγραφούν ενδεικτικά το σύνθετο πλαίσιο διακυβέρνησης μέσα στο οποίο καλείται η χώρα μας να λειτουργήσει και να ανταποκριθεί στις ολοένα αυξανόμενες απειλές, αξιοποιώντας τον επιτελικό και επιχειρησιακό ρόλο της Εθνικής Αρχής Κυβερνοασφάλειας.

Η νέα στρατηγική έχει ως σκοπό να εστιάσει:

* Στη θεσμική συνέπεια και συνέχεια, με ενίσχυση του επιτελικού ρόλου της ΕΑΚ, τη συνέργεια και συνεργασία με άλλες κρίσιμες Αρχές και Φορείς και την υιοθέτηση σαφών μηχανισμών συντονισμού σε περιόδους κρίσης.
* Στην αναβάθμιση κρίσιμων υποδομών και υπηρεσιών, αξιοποιώντας τεχνολογίες αιχμής και εφαρμογές προγνωστικής ανάλυσης με χρήση τεχνητής νοημοσύνης για πρόληψη και έγκαιρη απόκριση σε επιθέσεις.
* Στην προσαρμογή της χώρας στο ευρωπαϊκό και διεθνές πλαίσιο, ενσωματώνοντας και εφαρμόζοντας πλήρως τις πολυάριθμες ευρωπαϊκές ρυθμιστικές πρωτοβουλίες, όπως ενδεικτικά την Πράξη για την Ανθεκτικότητα στον Κυβερνοχώρο (Cyber Resilience Act), την Πράξη για την Αλληλεγγύη στον Κυβερνοχώρο (Cyber Solidarity Act) και την Πράξη για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα (Digital Operational Resilience Act).
* Στην ανάπτυξη δεξιοτήτων και ερευνητικής αριστείας, μέσω επενδύσεων σε εκπαίδευση, κατάρτιση και R&D, ώστε να οικοδομηθεί ένα εθνικό οικοσύστημα καινοτομίας στην κυβερνοασφάλεια.
* Στην καλλιέργεια μιας ώριμης κοινωνικής και επιχειρησιακής κουλτούρας κυβερνοασφάλειας, τόσο για κρίσιμους οργανισμούς όσο και για το σύνολο της κοινωνίας μέσω εκστρατειών ενημέρωσης και προσαρμοσμένων εκπαιδευτικών εργαλείων για πολίτες, δημόσιους φορείς και ΜΜΕ.

Η περίοδος 2026–2030 δεν αφορά μόνο στην προσαρμογή σε νέες συνθήκες, αλλά και στη διαμόρφωση ενός μακροπρόθεσμου στρατηγικού σχεδιασμού που θα θωρακίσει τη χώρα απέναντι σε μελλοντικές απειλές, θα ενισχύσει την ψηφιακή της αυτονομία και θα την καταστήσει αξιόπιστο εταίρο στο ευρωπαϊκό και διεθνές πεδίο της κυβερνοασφάλειας.

Η στρατηγική καλείται να διασφαλίσει ότι η Ελλάδα θα παραμείνει όχι απλώς συμμορφούμενη με τις διεθνείς και ευρωπαϊκές υποχρεώσεις της, αλλά και πρωτοπόρος σε θέματα κυβερνοασφάλειας, προωθώντας ένα εθνικό μοντέλο που συνδυάζει θεσμική ισχύ, τεχνολογική καινοτομία και ευρύτερη κοινωνική συμμετοχή.

**Ο Διοικητής**

**Μιχαήλ Μπλέτσας**

# Εισαγωγή

## Εθνική Στρατηγική Κυβερνοασφάλειας 2026 - 2030

Η Εθνική Στρατηγική Κυβερνοασφάλειας (Ε.Σ.Κ.), σύμφωνα με το άρθρο 7 του ν. 5160/2024, αποτελεί το ανώτατο συνεκτικό πλαίσιο πολιτικής της χώρας για την ενίσχυση της κυβερνοανθεκτικότητας και την προστασία του εθνικού κυβερνοχώρου. Διαμορφώνεται από την Εθνική Αρχή Κυβερνοασφάλειας και θεσπίζεται στο πλαίσιο της Στρατηγικής Εθνικής Ασφάλειας, καθορίζοντας τους στρατηγικούς στόχους, τις προτεραιότητες, τους αναγκαίους πόρους και τα μέτρα πολιτικής και ρύθμισης για την επίτευξή τους. Η Ε.Σ.Κ. περιλαμβάνει το πλαίσιο διακυβέρνησης που προσδιορίζει τους ρόλους και τις αρμοδιότητες των συναρμόδιων αρχών και εμπλεκομένων μερών, καθώς και τους μηχανισμούς συνεργασίας και συντονισμού σε εθνικό και ευρωπαϊκό επίπεδο. Παράλληλα, προβλέπει δράσεις εκτίμησης κινδύνων, ετοιμότητας, απόκρισης και αποκατάστασης από κυβερνοπεριστατικά. Επιπλέον, περιλαμβάνονται μέτρα που αποσκοπούν στην ανάπτυξη δεξιοτήτων, την ευαισθητοποίηση πολιτών και επιχειρήσεων, και την προώθηση της έρευνας και της καινοτομίας. Με τον τρόπο αυτό, η Ε.Σ.Κ. λειτουργεί ως ολοκληρωμένο στρατηγικό πλαίσιο που διασφαλίζει τη συνοχή των εθνικών πολιτικών με τις ευρωπαϊκές και διεθνείς εξελίξεις, ενισχύει την κυβερνοανθεκτικότητα της χώρας και καλλιεργεί την εμπιστοσύνη στην ψηφιακή οικονομία και κοινωνία.

Η Εθνική Στρατηγική Κυβερνοασφάλειας αποτελεί το βασικό πλαίσιο της δημόσιας πολιτικής, ώστε η χώρα να ανταπεξέλθει στις εξαιρετικά δυναμικές και ταχέως εξελισσόμενες προκλήσεις στον τομέα. Η κυβερνοασφάλεια αποτελεί τον ακρογωνιαίο λίθο για την επιτυχή ψηφιακή μετάβαση, καθώς και τη διασφάλιση των υπηρεσιών που παρέχονται από το κράτος, τις κρίσιμες υποδομές, καθώς και τον ιδιωτικό τομέα και την αγορά εν γένει. Η αξία της αναδεικνύεται ιδιαίτερα από το γεγονός ότι κρίσιμες υπηρεσίες για το κοινωνικό σύνολο και την εθνική οικονομία παρέχονται και εξαρτώνται, όλο και περισσότερο, από την ομαλή και αδιάλειπτη λειτουργία των ψηφιακών υποδομών. Ενδεικτικά, η ίδια η λειτουργία του δημόσιου τομέα, καθώς και η παροχή υπηρεσιών σε κρίσιμους τομείς, όπως η υγεία, οι μεταφορές, η ενέργεια, η εφοδιαστική αλυσίδα, οι τηλεπικοινωνίες, ο κλάδος των κατασκευών, ο χρηματοπιστωτικός τομέας, παρέχονται πλέον κυρίως μέσω ψηφιακών υποδομών. Ταυτόχρονα, η κυβερνοασφάλεια, ως μια κατάσταση ομαλότητας και «ευταξίας» στον κυβερνοχώρο, αποτελεί προϋπόθεση για την άσκηση και διασφάλιση σειράς θεμελιωδών ατομικών δικαιωμάτων στον ψηφιακό κόσμο: από την προστασία των προσωπικών δεδομένων, το απόρρητο των τηλεπικοινωνιών, τo δικαίωμα στην πληροφόρηση και συμμετοχής στην κοινωνία της πληροφορίας, έως την ελεύθερη ανάπτυξη της προσωπικότητας και συμμετοχής στην κοινωνική, οικονομική και πολιτική ζωή της Xώρας. Η διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας, ιδίως της κρίσιμης εθνικής ψηφιακής υποδομής, συνιστά υποχρέωση της Πολιτείας και των φορέων, του δημόσιου και ιδιωτικού τομέα που τις διαχειρίζονται, αλλά και υπόθεση όλων μας.

## Στόχοι της Δημόσιας Διαβούλευσης

Σκοπός του παρόντος ερωτηματολογίου είναι η προαγωγή της δημόσιας διαβούλευσης και η ενεργή και ουσιαστική συμμετοχή όλων των εμπλεκόμενων φορέων και των πολιτών στη διαμόρφωση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030. Η κυβερνοασφάλεια συνιστά κρίσιμο πυλώνα της ψηφιακής ανθεκτικότητας της χώρας και απαιτεί συνεκτική, πολυεπίπεδη και πρωτίστως συμμετοχική προσέγγιση.

Μέσα από τη διαδικασία διαβούλευσης επιδιώκονται:

1. **Η συλλογική νομιμοποίηση και συναίνεση**

Η κυβερνοασφάλεια δεν αποτελεί υπόθεση μόνο του κράτους και των ρυθμιστικών αρχών. Αφορά την κοινωνία, τις επιχειρήσεις, τους φορείς υποδομών, την ακαδημαϊκή και ερευνητική κοινότητα. Η διαβούλευση οικοδομεί κοινή γλώσσα και σταθερή συνεργασία για την υλοποίηση της στρατηγικής.

1. **Η ρεαλιστική προσαρμογή του “Σχεδίου Δράσης”**

Μέσα από τη διαβούλευση διαπιστώνουμε κατά πόσο οι προτεινόμενες δράσεις είναι ρεαλιστικές, εφαρμόσιμες και κατάλληλα στοχευμένες. Οι απόψεις των φορέων θα συμβάλουν καθοριστικά στη διαμόρφωση της στρατηγικής σε πρακτικό επίπεδο.

1. **Ο εντοπισμός κενών και ειδικών αναγκών**

Πολλές ανάγκες σε επίπεδο τομέων, ενδέχεται να μην είναι ορατές σε κεντρικό επίπεδο. Η διαβούλευση αναμένεται να αναδείξει αυτά τα σημείακαι να τα ενσωματώσει στο τελικό κείμενο της στρατηγικής.

1. **Η ενίσχυση της εμπιστοσύνης και της διαφάνειας**

Η ανοικτή διαβούλευση συμβάλλει στην ενίσχυση της διαφάνειας και της δημοκρατικής λογοδοσίας, στο πλαίσιο διαμόρφωσης μιας εθνικής πολιτικής που επηρεάζει ουσιωδώς την ασφάλεια και την ευημερία πολιτών και επιχειρήσεων.

Η διαδικασία της διαβούλευσης στοχεύει, ειδικότερα:

1. **Στην τελική διαμόρφωση της Εθνικής Στρατηγικής Κυβερνοασφάλειας,** σύμφωνα με τις ανάγκες των επιμέρους φορέων. Μια στρατηγική οριζόντιας εφαρμογής, προκειμένου να είναι αποτελεσματική, δεν μπορεί να είναι αποκομμένη από την κοινωνική και θεσμική πραγματικότητα. Η διαβούλευση αποτελεί βασικό εργαλείο για τη διερεύνηση της αντιστοίχισης μεταξύ στρατηγικών στόχων και πραγματικών αναγκών.
2. **Στην προτεραιοποίηση δράσεων με βάση τις τρέχουσες ανάγκες και την ετοιμότητα υλοποίησης.** Μέσα από τη διαβούλευση εντοπίζονται οι «ώριμες» και επείγουσες παρεμβάσεις προς άμεση υλοποίηση, όσο κι εκείνες που απαιτούν σταδιακή εφαρμογή και αποτελεσματικό συντονισμό σε βάθος χρόνου.
3. **Στην ανάδειξη των δυνατοτήτων συνεργειών μεταξύ φορέων και καλών πρακτικών** που έχουν εφαρμοστεί επιτυχώς σε εθνικό ή ευρωπαϊκό επίπεδο, καθώς και στην προώθηση του ρόλου των διαθέσιμων εθνικών και ευρωπαϊκών εργαλείων και προγραμμάτων. Η καταγραφή σχετικών δράσεων θα επιτρέψει την αξιοποίησή τους ως πρότυπα ή ως μοχλούς επιτάχυνσης και κλιμάκωσης για την υλοποίηση της νέας στρατηγικής.
4. **Στην αποτελεσματική εφαρμογή των δράσεων,** σε συνέχεια της δημοσίευσης της Εθνικής Στρατηγικής. Η ενεργός συμμετοχή των φορέων κατά το στάδιο της διαμόρφωσης της ΕΣΚ, συμβάλλει στη διαμόρφωση ενός σταθερού πλαισίου συνεργασίας, που προάγει την κοινή δέσμευση και ενισχύει την προσήλωση στην αποτελεσματική υλοποίηση δράσεων.

Συμπερασματικά, η διαβούλευση δεν συνιστά απλώς μία τυπική διαδικασία. Πρόκειται για έναν ουσιαστικό και αναγκαίο μηχανισμό που διασφαλίζει την ποιότητα, την ευρύτερη αποδοχή και, εν τέλει, την αποτελεσματική υλοποίηση της στρατηγικής.

Για το λόγο αυτό, καλούνται όλοι οι εμπλεκόμενοι φορείς, καθώς και όλοι οι ενδιαφερόμενοι πολίτες να συνεισφέρουν με συγκεκριμένες παρατηρήσεις και προτάσεις, απαντώντας στα σχετικά ερωτήματα ανά θεματικό άξονα. Οι συμβολές αυτές θα είναι καθοριστικές για τη διαμόρφωση μιας στρατηγικής με γνώμονα τη συνέχεια, τη συνέπεια και κυρίως την αποτελεσματικότητα με πραγματικό αντίκτυπο.

# Οδηγίες Συμπλήρωσης

Στο πλαίσιο της διαδικασίας διαμόρφωσης της νέας ΕΣΚ 2026 - 2030, η Εθνική Αρχή Κυβερνοασφάλειας καλεί τους ενδιαφερόμενους φορείς και τους πολίτες να συμβάλουν με τις απόψεις και τις προτάσεις τους, μέσω του παρόντος ερωτηματολογίου.

Το ερωτηματολόγιο περιλαμβάνει ερωτήσεις ανοιχτού τύπου, ώστε να δοθεί η δυνατότητα για ουσιαστικές και στοχευμένες τοποθετήσεις. Η συμπλήρωσή του δεν απαιτεί την υποχρεωτική απάντηση σε όλες τις ερωτήσεις. Οι ερωτώμενοι μπορούν να επιλέξουν σε ποιες ερωτήσεις θα απαντήσουν, ανάλογα με τον τομέα δραστηριότητας, τις αρμοδιότητες, την εξειδίκευση και τις γνώσεις τους.

Για τη βέλτιστη αξιοποίηση των απαντήσεων, παρακαλούμε:

* Να καταγραφούν τα στοιχεία του φορέα που εκπροσωπείτε στο Τμήμα Α.
* Να διατυπώνονται οι απόψεις με σαφήνεια και, όπου είναι δυνατόν, με συγκεκριμένα παραδείγματα ή προτάσεις.
* Να καταχωρούνται οι απαντήσεις στο δυναμικό πεδίο που ακολουθεί κάθε ερώτηση.

Η υποβολή των απαντήσεων θα πρέπει να γίνει ως εξής:

* Οι απαντήσεις να αποθηκευτούν και να αποσταλούν σε μορφή PDF.
* Η υποβολή να πραγματοποιηθεί έως την 31η Οκτωβρίου 2025 στη διεύθυνση: [dir.strategy@cyber.gov.gr](mailto:dir.strategy@cyber.gov.gr)
* Στο θέμα του email να αναγράφεται: *«Απάντηση στο Ερωτηματολόγιο – Εθνική Στρατηγική Κυβερνοασφάλειας 2026 - 2030»*.

# Εμπιστευτικότητα

Τα στοιχεία που θα δηλωθούν στο Τμήμα Α (ονοματεπώνυμο, φορέας, θέση, στοιχεία επικοινωνίας), θα χρησιμοποιηθούν αποκλειστικά για σκοπούς επικοινωνίας και κατηγοριοποίησης των απαντήσεων. Δεν θα δημοσιοποιηθούν, ούτε θα διαβιβαστούν σε τρίτους. Οποιαδήποτε δημοσίευση των αποτελεσμάτων της διαβούλευσης, θα είναι σε ανωνυμοποιημένη και σε συγκεντρωτική μορφή.

# Ερωτηματολόγιο Διαβούλευσης ΕΣΚ 2026 - 2030

## Τμήμα Α: Στοιχεία Επικοινωνίας

Παρακαλούμε συμπληρώστε τα παρακάτω στοιχεία. Οι πληροφορίες θα χρησιμοποιηθούν αποκλειστικά για την επεξεργασία των απαντήσεων και τη διασφάλιση της αντιπροσωπευτικότητας της διαβούλευσης.

1. Ονοματεπώνυμο: Click or tap here to enter text.
2. Οργανισμός / Φορέας που δραστηριοποιήστε: Click or tap here to enter text.
3. Θέση / Ρόλος στον οργανισμό: Click or tap here to enter text.
4. Τομέας δραστηριότητας του φορέα: Click or tap here to enter text.  
    Δημόσιος φορέας  
    Ιδιωτικός φορέας  
    Ένωση / Επιμελητήριο  
    Οργάνωση της Κοινωνίας των Πολιτών  
    Ακαδημαϊκός / Ερευνητικός φορέας  
    Άλλο (παρακαλώ διευκρινίστε): Click or tap here to enter text.
5. Στοιχεία επικοινωνίας (email): Click or tap here to enter text.

## Τμήμα Β: Ερωτήσεις

## Θεματική Ενότητα 1: Στρατηγικές Κατευθύνσεις και Διακυβέρνηση

1. Ποιες ιδέες και δράσεις θεωρείτε ότι θα πρέπει να συμπεριλαμβάνει η Εθνική Στρατηγική Κυβερνοασφάλειας, προκειμένου η Ελλάδα να βελτιώσει σημαντικά το συνολικό επίπεδο της ανθεκτικότητάς της στον κυβερνοχώρο έως το 2030;

Click or tap here to enter text.

1. Ποιες είναι οι ιδιαίτερες ανάγκες και προκλήσεις που αντιμετωπίζει ο τομέας δραστηριότητάς σας στο πεδίο της κυβερνοασφάλειας και ποιες στοχευμένες τομεακές δράσεις θα μπορούσαν να συμβάλλουν στην αντιμετώπισή τους;

Click or tap here to enter text.

1. Σε ποιες ενέργειες θα πρέπει να προβεί η Πολιτεία, προκειμένου να ενισχυθεί η ανταλλαγή πληροφοριών (intelligence sharing) ανάμεσα στις οντότητες σχετικά με τις κυβερνοαπειλές;

Click or tap here to enter text.

1. Πώς μπορούν να δημιουργηθούν κίνητρα για τις οντότητες προκειμένου να αναφέρουν εγκαίρως σημαντικά κυβερνοπεριστατικά που αντιμετωπίζουν;

Click or tap here to enter text.

1. Θα πρέπει η Πολιτεία να εξετάσει τη δυνατότητα θεσμοθέτησης ενιαίας ψηφιακής πύλης αναφοράς για όλα τα περιστατικά κυβερνοασφάλειας, με στόχο την εναρμόνιση των υφιστάμενων υποχρεώσεων που σήμερα απαιτούν ξεχωριστές αναφορές σε πολλαπλές ρυθμιστικές αρχές;

Click or tap here to enter text.

## Θεματική Ενότητα 2: Νομοθεσία, Ρυθμιστικά Μέτρα και Συμμόρφωση

1. Ποια νομοθετικά ή κανονιστικά μέτρα θα πρέπει να προωθήσει η Πολιτεία, προκειμένου να ενισχύσει την κυβερνοανθεκτικότητα σε όλο το εύρος της ψηφιακής οικονομίας;

Click or tap here to enter text.

1. Υπάρχουν πεδία ρυθμιστικής παρέμβασης στην ισχύουσα εθνική νομοθεσία για την κυβερνοασφάλεια τα οποία δεν έχουν αντιμετωπιστεί επαρκώς ή καθόλου, ή χρήζουν περαιτέρω επεξεργασίας και εξειδίκευσης;

Click or tap here to enter text.

1. Ποιες πρωτοβουλίες από την πλευρά της Πολιτείας θα διευκόλυναν ή θα παρακινούσαν τους φορείς να εφαρμόζουν αποτελεσματικά την ισχύουσα νομοθεσία κυβερνοασφάλειας;

Click or tap here to enter text.

1. Πώς μπορεί να ενισχυθεί η ευαισθητοποίηση σε θέματα κυβερνοασφάλειας στα ανώτερα ιεραρχικά επίπεδα λήψης αποφάσεων των οργανισμών;

Click or tap here to enter text.

1. Πώς μπορεί η Πολιτεία να περιορίσει τα διοικητικά βάρη που προκύπτουν για τις επιχειρήσεις από την εφαρμογή της νομοθεσίας για την κυβερνοασφάλεια; Υπάρχουν πεδία όπου το κανονιστικό πλαίσιο μπορεί να γίνει απλούστερο και πιο αποτελεσματικό;

Click or tap here to enter text.

1. Ποια ρυθμιστικά μέτρα μπορούν να ληφθούν για την αντιμετώπιση συγκεκριμένων κυβερνοαπειλών (π.χ. ransomware), οι οποίες εμφανίζουν υψηλό ρίσκο για τον τομέα δραστηριότητάς σας;

Click or tap here to enter text.

1. Πώς μπορεί να προωθηθεί η υιοθέτηση μη δεσμευτικών προτύπων διαχείρισης της κυβερνοασφάλειας (π.χ. ISO, NIST CSF, ENISA guidelines);

Click or tap here to enter text.

1. Ποιες παρεμβάσεις απαιτούνται προκειμένου οι δημόσιες συμβάσεις να αποτελέσουν ουσιαστικό εργαλείο για τη βελτίωση του επιπέδου κυβερνοασφάλειας των δημόσιων οργανισμών;

Click or tap here to enter text.

## Θεματική Ενότητα 3: Τεχνολογικές Προκλήσεις και Καινοτομία

1. Ποια καθιερωμένα πρότυπα και βέλτιστες πρακτικές προτείνετε για την υλοποίηση αυτοματοποιημένων μηχανισμών ανίχνευσης και αντιμετώπισης απειλών σε μεγάλη κλίμακα, με στόχο την αξιόπιστη, αποδοτική και επεκτάσιμη προστασία πληροφοριακών συστημάτων και υποδομών;

Click or tap here to enter text.

1. Ποιες δράσεις θα μπορούσαν να ενταχθούν στην Εθνική Στρατηγική Κυβερνοασφάλειας για την αντιμετώπιση των προκλήσεων που θέτουν οι αναδυόμενες τεχνολογίες (π.χ. AI, IoT, κβαντικοί υπολογιστές) και την προαγωγή της αρχής “security by design”;

Click or tap here to enter text.

1. Ποιες είναι οι προϋποθέσεις (θεσμικές, οικονομικές ή/και ερευνητικές) που θα πρέπει να διαμορφωθούν ώστε να αυξηθεί ο αριθμός των ελληνικών επιχειρήσεων που αναπτύσσουν και προσφέρουν καινοτόμες λύσεις κυβερνοασφάλειας στην ελληνική και ευρωπαϊκή/διεθνή αγορά;

Click or tap here to enter text.

## Θεματική Ενότητα 4: Δεξιότητες, Εκπαίδευση και Ανθρώπινο Δυναμικό

1. Πώς θα μπορούσε η κυβερνοασφάλεια να ενταχθεί αποτελεσματικά στα προγράμματα σπουδών της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης;

Click or tap here to enter text.

1. Ποιες δράσεις από την πλευρά της Πολιτείας θεωρείτε ότι θα είχαν ισχυρό αντίκτυπο στη μείωση του «χάσματος δεξιοτήτων» κυβερνοασφάλειας και στην κάλυψη της αυξημένης ζήτησης σε εξειδικευμένα στελέχη (στον δημόσιο και/ή ιδιωτικό τομέα);

Click or tap here to enter text.

1. Τα υπάρχοντα προγράμματα εκπαίδευσης και κατάρτισης στην κυβερνοασφάλεια που προσφέρονται στην Ελλάδα, ανταποκρίνονται στις τρέχουσες ανάγκες της αγοράς; Ποιες δράσεις θα επέτρεπαν την καλύτερη ευθυγράμμιση της εκπαίδευσης με τις ανάγκες των οντοτήτων;

Click or tap here to enter text.

## Θεματική Ενότητα 5: Συνεργασίες, Οικοσύστημα και Διεθνής Διάσταση

1. Ποια πεδία εντός του τομέα της κυβερνοασφάλειας θεωρείτε πιο πρόσφορα για την ανάπτυξη συμπράξεων δημόσιου και ιδιωτικού τομέα;

Click or tap here to enter text.

1. Τι είδους υποστήριξη θα πρέπει να προσφέρει η Πολιτεία σε πολύ μικρές και μικρές επιχειρήσεις για την ενίσχυση του επιπέδου της κυβερνοασφάλειάς τους και την αποτελεσματική αντιμετώπιση των κυβερνοαπειλών;

Click or tap here to enter text.

1. Πώς μπορεί η Ελλάδα να ενισχύσει την συνολική κυβερνοανθεκτικότητα των υποδομών της, αξιοποιώντας τις διμερείς και πολυμερείς σχέσεις της Ποια πεδία εντοπίζετε για συνεργασία με τρίτες χώρες στον τομέα της κυβερνοασφάλειας;

Click or tap here to enter text.

## Ανοικτή Ερώτηση

1. Υπάρχει κάποιο/α θέμα/τα που θεωρείτε ιδιαιτέρως κρίσιμα και δεν έχουν αναφερθεί στο παρόν ερωτηματολόγιο; Παρακαλούμε αναπτύξτε ελεύθερα τους προβληματισμούς και τις προτάσεις σας, στο πλαίσιο διαμόρφωσης της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

Click or tap here to enter text.