

## Συμπεράσματα –Προτάσεις Ημερίδας:

« Συντονισμένη εποπτεία και διαχείριση της ασφάλειας και ιδιωτικότητας στον Ελλαδικό χώρο»

<http://athina.cs.unipi.gr/imerida/index.php>

### Οργανωτές

	<b>Πανεπιστήμιο Πειραιώς</b>	Καθ. Χρήστος Δουληγέρης, <a href="mailto:cdoulig@unipi.gr">cdoulig@unipi.gr</a> Επικ. Καθ. Νινέτα Πολέμη, <a href="mailto:dpolemi@unipi.gr">dpolemi@unipi.gr</a>
	<b>Οικονομικό Πανεπιστήμιο Αθηνών</b>	Καθ. Δημήτρης Γκρίτζαλης, <a href="mailto:dgrit@aueb.gr">dgrit@aueb.gr</a> Καθ. Διομήδης Σπινέλης, <a href="mailto:dds@aueb.gr">dds@aueb.gr</a>
	<b>Εθνικό Μετσόβειο Πολυτεχνείο</b>	Καθ. Μίλτος Αναγνώστου, <a href="mailto:miltos@central.ntua.gr">miltos@central.ntua.gr</a> Καθ. Νικόλαος Μήτρου, <a href="mailto:mitrou@cs.ntua.gr">mitrou@cs.ntua.gr</a>
	<b>Πανεπιστήμιο Πατρών</b>	Καθ. Παύλος Σπυράκης, <a href="mailto:spirakis@cti.gr">spirakis@cti.gr</a> Αναπλ. Καθ. Γιάννης Σταματίου, <a href="mailto:stamatiu@ceid.upatras.gr">stamatiu@ceid.upatras.gr</a>

**Rapporteur Ημερίδας:** Δρ. Παναγιώτης Κοτζανικολάου, Λέκτορας Πανεπιστημίου Πειραιώς

**Επιστημονική και Τεχνική Υποστήριξη:** Υ.Δ. Κ. Δέλλιος, Α. Σάσσαλος, Δ. Παράς

## *A. Συμπεράσματα*

Από τις παρουσιάσεις της ημερίδας (<http://athina.cs.unipi.gr/imerida>) και τις απαντήσεις που λάβαμε από το ερωτηματολόγιο (επισυνάπτεται στο παράρτημα) προέκυψαν τα εξής συμπεράσματα:

### *A1. Αποτύπωση Δράσεων, Διαδικασιών, Ροών Εργασιών, Πληροφορίας*

- 1) επικαιροποιήθηκε ο πίνακας καταγραφής των φορέων που σχετίζονται με την ασφάλεια και την ιδιωτικότητα, καθώς και τα πεδία δράσης τους. Η αρχική καταγραφή των φορέων και των αρμοδιοτήτων πραγματοποιήθηκε το 2004 στο πλαίσιο της ομάδας εργασίας ΣΤ3 του e-business forum (<http://www.ebusinessforum.gr/teams/teamsall/view/index.php?ctn=76&language=el>) και ανανεώθηκε το 2008 (ομάδας εργασίας CICIP, eGovernment Forum, <http://e-governmentforum.gr/index.php?/ell/content/view/full/273>). Από την ανανέωση των αρμοδιοτήτων προκύπτει ο παρακάτω πίνακας:
- 2) Το νομοθετικό πλαίσιο της ίδρυσης των παραπάνω φορέων είναι δεσμευτικό ως προς τις αρμοδιότητες κάθε φορέα.
- 3) Δεν υπάρχουν συγκεκριμένες, προτυποποιημένες και θεσμοθετημένες (π.χ. από εσωτερικούς κανονισμούς) διαδικασίες, οι οποίες χρησιμοποιούνται για την υλοποίηση των παραπάνω δράσεων.
- 4) Δεν απαιτείται από το προσωπικό των φορέων να είναι πιστοποιημένοι ελεγκτές / επιθεωρητές ασφάλειας, σύμφωνα με κάποιο πρότυπο.

**Πίνακας 1: Εποπτικοί/Κανονιστικοί/ Ρυθμιστικοί Φορείς Ασφάλειας**

Φορέας	Ειδικές Αρχές / Διευθύνσεις Ασφάλειας	Πεδίο δράσης	Ρόλοι						
			Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Computer Forensics	Πιστοποίηση προϊόντων & υπηρεσιών ασφαλείας	Παροχή Προϊόντων Υποδομών Ασφάλειας	Συμβουλευτικές Υπηρεσίες Ασφάλειας	Εκπαίδευση σε θέματα ασφαλείας
ΓΓΕΘΑ - Εθνική Αρχή Ασφάλειας	Διεύθυνση Πληροφορικής/Τμήμα Ασφάλειας Συστημάτων Πληροφορικής	1) Αποτελεί την Εθνική Αρχή Ασφάλειας 2) Έκδοση του Εθνικού Κανονισμού Ασφαλείας (ΕΚΑ) (σε συνεργασία με την ΕΥΠ): Αφορά στην ασφάλεια των ηλεκτρονικά επεξεργασμένων, διαβαθμισμένων, εθνικά ευαίσθητων πληροφοριών και εφαρμόζεται σε όλους τους δημόσιους φορείς. 3) Το ΔΠΛΗ/Τμήμα Ασφάλειας Συστημάτων Πληροφορικής υλοποιεί το Κέντρο Συντονισμού Αντιμετώπισης Περιστατικών Ασφαλείας ( CIRC). 4) Το ΔΕΠ/Τμήμα Ασφάλειας Επικοινωνιών είναι ο τεχνικός σύμβουλος της Εθνικής Αρχής Πιστοποίησης Ασφάλειας.	✓		✓				
	Διεύθυνση Επικοινωνιών / Τμήμα Ασφάλειας Επικοινωνιών								
	Διεύθυνση Επικοινωνιών/Τμήμα Ηλεκτρονικού Πολέμου								
	Διεύθυνση Κυβερνοάμυνας								
ΕΥΠ	Αρχή Ασφάλειας Πληροφοριών (INFOSEC) (Τεχνικής φύσεως)	1) Ασφάλεια Εθνικών Επικοινωνιών-Πληροφορικής (σύνταξη κανονισμών, πιστοποίηση συστημάτων) 2) Πρόληψη και Αντιμετώπιση Ηλεκτρονικών Επιθέσεων. 3) Συντάξη, με βάση τις πληροφορίες που διαθέτει, πληροφοριακών δελτίων, μελετών και εκθέσεων τις οποίες και διαβιβάζει στις κατά περίπτωση αρμόδιες αρχές. 4) Συμμετοχή στη σύνταξη του ΕΚΑ. Συγκεκριμένα είναι επιφορτισμένη με το τεχνικό μέρος του κανονισμού. 5) Έλεγχος της τήρησης του τεχνικού μέρους του ΕΚΑ από ΔΔ. 6) Συντονίζει, στο πλαίσιο των αποφάσεων του ΚΥ.Σ.Ε.Α., τη δράση των υπηρεσιών πληροφοριών και ασφαλείας της Χώρας στον τομέα συλλογής και διάθεσης των πληροφοριών, που έχουν σχέση με το αντικείμενο της αποστολής της.  Παράλληλα, συνεργάζεται και ενημερώνει τη Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (Δ.Δ.Σ.Π.) και τις υπηρεσίες πληροφοριών των Επιτελείων που εποπτεύονται από αυτήν, για θέματα της αρμοδιότητάς τους.	✓			✓		✓	
	Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT)								

Φορέας	Ειδικές Αρχές / Διευθύνσεις Ασφάλειας	Πεδίο δράσης	Ρόλοι							
			Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Computer Forensics	Πιστοποίηση προϊόντων & υπηρεσιών ασφαλείας	Παροχή Προϊόντων Υποδομών Ασφάλειας	Συμβουλευτικές Υπηρεσίες Ασφάλειας	Εκπαίδευση σε θέματα ασφαλείας	
ΕΛΑΣ	Διεύθυνση Εγκληματολογικών Ερευνών – Τμήμα εξέτασης ψηφιακών πειστηρίων	1) Εξέταση ψηφιακών πειστηρίων. 2) Παρέχει υποστήριξη στις διοικητικές Αρχές της χώρας.		✓	✓				✓	
	Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος	1) Διενέργεια προανακριτικών ελέγχων που αφορούν το ηλεκτρονικό έγκλημα.								
Υπουργείο Μεταφορών και Επικοινωνιών	Γενική Γραμματεία Επικοινωνιών (ΓΓΕ)	1) Αποτελεί την Αρχή Τηλεπικοινωνιών. 2) Χάραξη Πολιτικής Ασφάλειας (Εθνική Στρατηγική Ασφάλειας). 3) Έκδοση του Εθνικού σχεδίου αριθμοδότησης (Ε.Σ.Α.).	✓			✓				
	ΓΓΕ(Γενική Γραμματεία Επικοινωνιών)/Διεύθυνση Πιστοποίησης (Τμήμα Τυποποίησης και Πιστοποίησης)	4) Η Διεύθυνση Πιστοποίησης της Γενικής Γραμματείας Επικοινωνιών του ΥΜΕ έχει αρμοδιότητες για τα θέματα αναρμόνισης της οδηγίας RTTE στη χώρα μας. (Οδηγία 99/5/ΕΚ) 5) Υλοποίηση Πολιτικής για την Ασφάλεια Δημοσίων Δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.								
Τράπεζα Ελλάδος	Διεύθυνση Εποπτείας Πιστωτικού Συστήματος	1) Έκδοση συγκεκριμένων αρχών / κανονισμών ασφαλείας 2) Έλεγχος εφαρμογής των παραπάνω κανονισμών 3) Αξιολόγηση συστημάτων εσωτερικού ελέγχου	✓	✓						
Υπουργείο Εσωτερικών	Δ/ση Πολιτικής Σχεδίασης Έκτακτης Ανάγκης	1) Προπαρασκευή και ετοιμότητα των υπηρεσιών με σκοπό την ομαλή μετάπτωση από ειρηνική περίοδο σε πολεμική. 2) Σχέδια επικινδυνότητας / επιχειρησιακής συνέχειας	✓	✓					✓	
	ΓΓΔΔ&ΗΔ (Γενική Γραμματεία Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης)/Υπηρεσία Ανάπτυξης Πληροφορικής	1) Αρχή Πιστοποίησης Ελληνικού Δημοσίου – ΑΠΕΔ. 2) Διαθεσιμότητα πληροφοριών στη ΔΔ/Σχέδια ανάκαμψης καταστροφών. 3) Καθορισμός Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης <ul style="list-style-type: none"> <li>Ανάπτυξη διαδικτυακών τόπων και συστημάτων ΔΔ όπως επίσης και υπηρεσιών της ΔΔ.</li> <li>Διασφάλιση Διαλειτουργικότητας των ΠΣ της ΔΔ.</li> </ul>	✓	✓		✓	✓	✓		

Φορέας	Ειδικές Αρχές / Διευθύνσεις Ασφάλειας	Πεδίο δράσης	Ρόλοι						
			Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Computer Forensics	Πιστοποίηση προϊόντων & υπηρεσιών ασφαλείας	Παροχή Προϊόντων Υποδομών Ασφάλειας	Συμβουλευτικές Υπηρεσίες Ασφάλειας	Εκπαίδευση σε θέματα ασφαλείας
Υπουργείο Οικονομικών	ΓΓΠΣ (Γενική Γραμματεία Πληροφοριακών Συστημάτων)/Γραφείο Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων & Υποδομών	<ol style="list-style-type: none"> <li>1) Σύνταξη προτύπων σχεδιασμού, ανάπτυξης και λειτουργίας πληροφοριακού συστήματος ασφαλείας και ποιοτικού ελέγχου (Στα ΠΣ του ΥΠΟΙΟ?).</li> <li>2) Έλεγχος και διερεύνηση των επεισοδίων ασφαλείας στις ηλεκτρονικές υπηρεσίες της ΓΓΠΣ.</li> <li>3) Έλεγχος ΠΣ για αξιολόγηση του βαθμού ασφαλείας.</li> <li>4) Εκπαίδευση προσωπικού σε θέματα ασφαλείας ΠΣ.</li> </ol>		✓		✓			✓
ΑΠΔΠΧ	Ανεξάρτητη Αρχή	<ol style="list-style-type: none"> <li>1) Προστασία προσωπικών δεδομένων</li> <li>2) Αρχείο Γνωστοποιήσεων – Έκδοση Αδειών</li> <li>3) Διενέργεια Διοικητικών Ελέγχων</li> <li>4) Εξέταση προσφυγών / καταγγελιών / ερωτημάτων</li> <li>5) Έκδοση οδηγιών και κανονιστικών πράξεων</li> <li>6) Απευθύνει συστάσεις και υποδείξεις</li> </ol>	✓	✓				✓	
ΑΔΑΕ	Ανεξάρτητη Αρχή	<ol style="list-style-type: none"> <li>1) Προστασία απορρήτου επικοινωνιών</li> <li>2) Διενέργεια τακτικών και έκτακτων ελέγχων</li> <li>3) Έκδοση κανονιστικών πράξεων</li> <li>4) Γνωμοδοτεί και απευθύνει συστάσεις</li> <li>5) Εξέταση καταγγελιών</li> <li>6) Προβαίνει σε κατάσχεση μέσω παραβίασης του απορρήτου.</li> </ol>	✓	✓				✓	
ΕΕΤΤ	Ανεξάρτητη Αρχή	<ol style="list-style-type: none"> <li>1) Αποτελεί την Εθνική Ρυθμιστική Αρχή Επικοινωνιών</li> <li>2) Ρύθμιση θεμάτων τηλεπικοινωνιών</li> <li>3) Υπεύθυνη αρχή για την εφαρμογή της Οδηγίας RTTE</li> </ol>	✓	✓					
GRNET CERT		<ol style="list-style-type: none"> <li>1) Προϊόντα και Υπηρεσίες ασφαλείας συστημάτων</li> <li>2) Πληροφόρηση στους χρήστες του ΕΔΕΤ σε θέματα ασφαλείας.</li> <li>3) Εκπαίδευση χρηστών σε θέματα ασφαλείας υπολογιστών και διαφύλαξης προσωπικού απορρήτου.</li> </ol>					✓	✓	✓
ENISA		<ol style="list-style-type: none"> <li>1) Παροχή συμβουλών και υποστήριξης στην ΕΕ και στα ΚΜ για την ασφαλεία πληροφοριών.</li> <li>2) Συλλογή και ανάλυση δεδομένων σχετικά με περιστατικά ασφαλείας στη Ευρώπη.</li> <li>3) Προώθηση μεθόδων αποτίμησης και διαχείρισης ρίσκου για τη βελτίωση της αντιμετώπισης απειλών σε θέματα ασφαλείας.</li> </ol>						✓	

## *A2. Συνέργειες με άλλους φορείς*

- 1) Η συνεργασία των φορέων δεν είναι θεσμοθετημένη από τον κανονισμό λειτουργίας τους. Η επικοινωνία πραγματοποιείται σε εθελοντική βάση και με ad hoc τρόπο. Δεν υπάρχει συστηματική, δομημένη, συνεργασία και καθορισμένα και σταθερά κανάλια επικοινωνίας.
- 2) Δεν υπάρχουν δομημένες, συνεχείς, συνεργατικές δραστηριότητες μεταξύ των φορέων.
- 3) Δεν υπάρχει ενιαίο κανονιστικό πλαίσιο το οποίο να διευκολύνει την συντονισμένη λειτουργία των φορέων. Οι κανονισμοί και τα πλαίσια που διέπουν την λειτουργία τους είναι (σε μερικές περιπτώσεις) επικαλυπτόμενα ενώ δεν προβλέπουν / αναδεικνύουν την συνεργασία τους.
- 4) Η πολυνομία προκαλεί έλλειψη συντονισμού των ελεγκτικών μηχανισμών μεταξύ των φορέων και αποθαρρύνει την ηλεκτρονική/κινητή διακυβέρνηση και επιχειρηματικότητα στην Ελλάδα.

## *A3. Ενημέρωση- Εκπαίδευση –Πιστοποίηση*

- 1) Δεν υπάρχει συντονισμένη ενημέρωση μεταξύ των φορέων για αλληλοενημέρωση σχετικά με θέματα αρμοδιότητας άλλου φορέα.
- 2) Δεν υπάρχουν δομημένα κανάλια ενημέρωσης για τους χρήστες (παρόχους, οργανισμούς, εταιρείες, διαχειριστές) για θέματα που προκύπτουν (και τους αφορούν).
- 3) Δεν υπάρχουν συντονισμένες συγκεκριμένες/δομημένες δράσεις συνεχούς εκπαίδευσης, επιμόρφωσης σε θέματα ασφάλειας και ιδιωτικότητας και πιστοποίησης.

## B. Προτάσεις

- I. Η ανάγκη Εθνικής Στρατηγικής Ασφάλειας Επικοινωνιών (ΕΣΑΕ) είναι επιτακτική ώστε να δημιουργηθεί συντονισμένη διαχείριση της ασφάλειας και ιδιωτικότητας στην Ελλάδα και να ενθαρρύνει την ηλεκτρονική διακυβέρνηση και επιχειρηματικότητα. Όπως αναφέρθηκε και στην εισήγηση του Γενικού Γραμματέα Επικοινωνιών στην Ημερίδα, το Υπουργείο Υποδομών Μεταφορών και Δικτύων έχει ήδη αναλάβει δράση προς αυτή την κατεύθυνση.
- II. Η ΕΣΑΕ θα πρέπει να ορίζει και να βελτιστοποιεί τις εσωτερικές διαδικασίες των εμπλεκόμενων φορέων καθώς και τις συντονιστικές τους δράσεις. Συνίσταται η βελτιστοποίηση των εσωτερικών διαδικασιών και των συντονιστικών ενεργειών των εμπλεκόμενων φορέων να ορίζεται με βάση αναγνωρισμένα διεθνή πρότυπα για την επεξεργασία, αποθήκευση και επικοινωνία πληροφοριών.
- III. Προτείνεται η θεσμοθέτηση (μέσω της ΕΣΑΕ) συνεργατικών δράσεων μεταξύ των φορέων με σκοπό την καλύτερη και αποδοτικότερη ενημέρωση των πολιτών και οργανισμών, ως προς τις αρμοδιότητες και δράσεις κάθε φορέα, με τη βοήθεια νέων τεχνολογιών (για παράδειγμα κοινό portal για την ενημέρωση των ενδιαφερομένων σχετικά με το σύνολο των φορέων και των αρμοδιοτήτων τους).
- IV. Η ΕΣΑΕ θα πρέπει να ορίζει στόχους αλλά και μέτρα/διαδικασίες υλοποίησης των στόχων ώστε να υπάρχει αποτελεσματικότητα κατά την εφαρμογή της. Στο πλαίσιο της ΕΣΑΕ συνίσταται να περιλαμβάνονται μέτρα και διαδικασίες υλοποίησης προς της επίτευξη των ακόλουθων στόχων:
  - Ενιαίο νομοθετικό/ρυθμιστικό πλαίσιο για την συνεργατική λειτουργία των εποπτικών, ελεγκτικών και ρυθμιστικών αρχών.
  - Ρύθμιση θεμάτων ελεγκτικών αρμοδιοτήτων και συναρμοδιοτήτων φορέων.
  - Προτυποποιημένη αποτελεσματική ενδο-διαχείριση και επικοινωνία των συμβάντων ασφάλειας/ιδιωτικότητας
  - Προτυποποιημένη καταγραφή, αποθήκευση και από κοινού αξιοποίηση των περιστατικών και μέτρων αντιμετώπισης με χρήση κοινών προτύπων.

- Προτυποποιημένη αποτελεσματική επικοινωνία των συμβάντων ασφάλειας/ιδιωτικότητας μεταξύ των φορέων.
- Συστηματική και δομημένη επικοινωνία με τους ενδιαφερόμενους οργανισμούς και τους πολίτες.
- Συντονισμένη και συνεχής εκπαίδευση των φορέων σε τρέχοντα επιτεύγματα από τον διεθνή χώρο, και αξιοποίηση της διεθνούς εμπειρίας.
- Συνεργατικές δράσεις φορέων προς την κατεύθυνση της εκπαίδευσης και πιστοποίησης του ειδικευμένου προσωπικού των φορέων (π.χ. ελεγκτών) σε κοινού ενδιαφέροντος θέματα ασφάλειας, για την επίτευξη οικονομικών κλίμακας.



**Ερωτηματολόγιο Ημερίδας**

---

**«Συντονισμένη εποπτεία και διαχείριση της ασφάλειας και ιδιωτικότητας στον Ελλαδικό χώρο»**

---

**Οργανισμός:** \_\_\_\_\_  
**Όνομα:** \_\_\_\_\_  
**Θέση:** \_\_\_\_\_  
**e-mail:** \_\_\_\_\_

**A. Αποτύπωση Δράσεων, Διαδικασιών, Ροών Εργασιών, Πληροφορίας**

1) Στα πλαίσια των εργασιών της θεματικής ομάδας «[Προστασία Κρίσιμων Πληροφοριακών και Τηλεπικοινωνιακών Υποδομών της Δημόσιας Διοίκησης](http://www.e-governmentforum.gov.gr/index.php?ell/content/view/full/273)» του eGovernment Forum (<http://www.e-governmentforum.gov.gr/index.php?ell/content/view/full/273>, κεφ.4 του παραδοτέου) παρουσιάστηκαν συνοπτικά (όπως δείχνουν οι Πίνακες 1, 2) οι Δημόσιοι Φορείς που λειτουργούν ως: (α) Ρυθμιστικοί/Κανονιστικοί και (β) Εποπτικοί (δεν αναφέρθηκαν οι φορείς που έχουν ενημερωτικό ρόλο)

- i. Συμφωνείτε με την συγκεκριμένη αποτύπωση:      ΝΑΙ       ΟΧΙ
- ii. Αναφέρετε τυχόν φορείς που έχουν κατά τη γνώμη σας παραλειφθεί

Φορέας	
Πεδίο δράσης	
Ρόλος	

- iii. Σχολιάστε όπως νομίζετε τους Πίνακες 1 και 2 (π.χ. τυχόν διορθώσεις, παραλείψεις ανά φορέα κλπ.).

**Πίνακας 1: Εποπτικοί/Κανονιστικοί Φορείς Ασφάλειας στην Ελλάδα**

Φορέας	Πεδίο δράσης	Ρόλοι				
		Ειδικές Αρχές Ασφάλειας	Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Computer Forensics	Πιστοποίηση προϊόντων & υπηρεσιών ασφαλείας
<b>ΓΕΕΘΑ</b>	Έκδοση εθνικών κανονισμών ασφαλείας	ΣΥΖΕΥΞΙΣ ΑΠ	X			
<b>ΕΥΠ</b>	Ασφάλεια Εθνικών Επικοινωνιών Πληροφορικής	INFOSEC, CERT για ΔΔ	X			X
<b>ΕΛΑΣ</b>	Εξέταση ψηφιακών πειστηρίων				X	
<b>Υπ. Μεταφορών Επικοινωνιών</b>	Χάραξη Πολιτικής Ασφάλειας		X			
<b>Τράπεζα Ελλάδος</b>	Έκδοση συγκεκριμένων κανονισμών ασφαλείας		X	X		
<b>Δ/ση Πολιτικής Σχεδίασης Έκτακτης Ανάγκης ΥΠΕΣ</b>	Σχέδια επικινδυνότητας /επιχειρησιακής συνέχειας		X	X		

<b>Υπηρεσία Ανάπτυξης Πληροφορικής, ΥΠΕΣ</b>	Διαθεσιμότητα πληροφοριών στη ΔΔ/Σχέδια ανάκαμψης καταστροφών	ΑΠΕΔ X				X
<b>Υπουργείο Εσωτερικών</b>		ΣΥΖΕΥΞΙΣ ΑΠ				
<b>Υπ.Υγείας</b>		ΣΥΖΕΥΞΙΣ ΑΠ				
<b>Υπ. Οικονομίας</b>		ΣΥΖΕΥΞΙΣ ΑΠ	X	X		

**Πίνακας 2: Ρυθμιστικοί/Ελεγκτικοί Φορείς Ασφάλειας**

Φορέας	Πεδίο δράσης	Ρόλοι			
		Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Παροχή προϊόντων/ υποδομών ασφαλείας	Πιστοποίηση προϊόντων & υπηρεσιών ασφαλείας
<b>ΑΠΠΑ</b>	Προστασία προσωπικών δεδομένων	X	X		X
<b>ΑΔΑΕ</b>	Προστασία απορρήτου επικοινωνιών	X	X		X
<b>ΕΕΤΤ</b>	Ρύθμιση θεμάτων τηλεπικοινωνιών	X	X	X	X
<b>ΕΦΤΑ</b>	Πρόληψη τηλεπικοινωνιακής απάτης	X		X	
<b>GRNET CERT</b>	Υπηρεσίες ασφαλείας συστημάτων			X	

2) Υπάρχουν συγκεκριμένες, θεσμοθετημένες/προτυποποιημένες διαδικασίες που χρησιμοποιείτε για την υλοποίηση των παραπάνω δράσεων;

- ΟΧΙ  
 ΝΑΙ – ακολουθούν ερωτήσεις 2α, 2β

2α. Ποιές διαδικασίες χρησιμοποιείτε για την υλοποίηση των παραπάνω δράσεων; (αναφέρετε τις διαδικασίες αναλυτικά για την κάθε δράση)

2 β. Υπάρχουν πρότυπα / δομημένα έντυπα που χρησιμοποιείτε στις παραπάνω διαδικασίες και σε ποιά μορφή;

**B. Συνέργειες με άλλους φορείς**

5) Στα πεδία δράσης (των παραπάνω πινάκων) του φορέα σας συνεργάζεστε με κάποιον άλλο από τους φορείς που αναφέρονται;

ΝΑΙ – ακολουθούν οι ερωτήσεις

1α, 1β

ΟΧΙ

1α. Αναφέρετε τους οργανισμούς που συνεργάζεστε και εξηγήστε την μορφή συνεργασίας για κάθε μια από τις παραπάνω δράσεις σας.

1β. Με ποιόν τρόπο επικοινωνείτε με τους συνεργαζόμενους φορείς:

*Κανάλια Επικοινωνίας*

Ταχυδρομείο,  
Τηλέφωνο/φαξ

E-mail

Ομάδες εργασίας

Web2.0 (forums, on-line  
conferences, chat)

Συσκευές

Δεν υπάρχει επικοινωνία

6) Συμμετέχετε/οργανώνετε συνεργατικές δραστηριότητες με άλλους εποπτικούς φορείς;

ΝΑΙ – ακολουθούν οι ερωτήσεις

1α, 1β

ΟΧΙ

1α. Τι σκοπούς εξυπηρετούν αυτές οι δραστηριότητες (σημειώστε περισσότερες από έναν αν απαιτείτε)

Ενημερωτικό

Αναβάθμιση διαδικασιών/υπηρεσιών

Εναρμόνιση δραστηριοτήτων/δράσεων

Θεσμικό

---

 Συμμετοχή σε προγράμματα εσωτερικού/εξωτερικού

---

 Συμμετοχή σε ασκήσεις/ ημερίδες/επιστημονικές συναντήσεις εσωτερικού/εξωτερικού

---

 Άλλους (εξηγείστε)

---

1β. Σημειώστε (μια ή περισσότερες δραστηριότητες) που συμμετέχετε :

---

 Ημερίδες, επιστημονικά συνέδρια, ομάδες εργασίας

---

 Πιλοτικά Έργα/Δοκιμές/Ασκήσεις

---

 Διαβουλεύσεις

---

 Forums

---

 Τηλεδιασκέψεις

---

 Ερευνητικά Προγράμματα/ Προγράμματα άλλων φορέων

---

 Άλλες (εξηγείστε)

---

### **Γ. Ενημέρωση- Εκπαίδευση –Πιστοποίηση**

4) Ενημερώνετε τους άλλους φορείς για θέματα που προκύπτουν (και τους αφορούν);

 ΝΑΙ – ακολουθούν οι ερωτήσεις

1α, 1β

 ΟΧΙ

1α. Πως γίνεται η αξιολόγηση των θεμάτων αυτών και πως γίνεται η επιλογή των φορέων που πρέπει να ενημερώσετε? Ποια συγκεκριμένη διαδικασία ακολουθείτε;

1β. Πως ενημερώνετε τους φορείς και με ποιά συχνότητα;

---

*Κανάλια*

*Συχνότητα ενημέρωσης*

*Επικοινωνίας*

---

 Ταχυδρομείο

Σε συγκεκριμένα τακτά, προκαθορισμένα διαστήματα

Όποτε θεωρηθεί απαραίτητο (εξηγείστε)

Δεν υπάρχει επίσημη ενημέρωση

---

 Τηλέφωνο-φαξ

Σε συγκεκριμένα τακτά, προκαθορισμένα διαστήματα

---

	Όποτε θεωρηθεί απαραίτητο (εξηγήστε) <input type="checkbox"/>
	Δεν υπάρχει επίσημη ενημέρωση <input type="checkbox"/>
<input type="checkbox"/> E-mail	Σε συγκεκριμένα τακτά, προκαθορισμένα διαστήματα <input type="checkbox"/>
	Όποτε θεωρηθεί απαραίτητο (εξηγήστε) <input type="checkbox"/>
	Δεν υπάρχει επίσημη ενημέρωση <input type="checkbox"/>
<input type="checkbox"/> Web2.0 (forums, on-line conferences, chat)	Σε συγκεκριμένα τακτά, προκαθορισμένα διαστήματα
	Όποτε θεωρηθεί απαραίτητο (εξηγήστε) <input type="checkbox"/>
	Δεν υπάρχει επίσημη ενημέρωση <input type="checkbox"/>
<input type="checkbox"/> Συσκέψεις/ Τηλεδιασκέψεις	Σε συγκεκριμένα τακτά, προκαθορισμένα διαστήματα <input type="checkbox"/>
	Όποτε θεωρηθεί απαραίτητο (εξηγήστε) <input type="checkbox"/>
	Δεν υπάρχει επίσημη ενημέρωση <input type="checkbox"/>
<input type="checkbox"/> Άλλα (εξηγήστε)	Σε συγκεκριμένα τακτά, προκαθορισμένα διαστήματα <input type="checkbox"/>
	Όποτε θεωρηθεί απαραίτητο(εξηγήστε) <input type="checkbox"/>
	Δεν υπάρχει επίσημη ενημέρωση <input type="checkbox"/>

5) Ενημερώνετε τους χρήστες (παρόχους, οργανισμούς, εταιρείες, διαχειριστές) για θέματα που προκύπτουν (και τους αφορούν);

- ΝΑΙ – ακολουθούν οι ερωτήσεις 1α, 1β
- ΟΧΙ

1α. Πως γίνεται η αξιολόγηση των θεμάτων αυτών και πως γίνεται η επιλογή των χρηστών που πρέπει να ενημερώσετε? Ποια συγκεκριμένη διαδικασία ακολουθείτε;

1β. Πως ενημερώνετε τους χρήστες:

*Κανάλια Επικοινωνίας*

- Ταχυδρομείο
- Τηλέφωνο-φαξ
- E-mail

---

 Web2.0 (forums, on-line conferences, chat)

---

 Συσκευές/  
Τηλεδιασκέψεις

---

 Μέσα Μαζικής  
Ενημέρωσης

---

6) Υπάρχουν συγκεκριμένες/δομημένες δράσεις συνεχούς εκπαίδευσης και επιμόρφωσης σε θέματα ασφάλειας και ιδιωτικότητας που προσφέρει ο φορέας σας;

 ΝΑΙ – ακολουθούν οι ερωτήσεις  
1α, 1β ΟΧΙ

1α. Σε ποιά θέματα ασφάλειας και ιδιωτικότητας υπάρχει συνεχής εκπαίδευση και επιμόρφωση; Ποια εκπαιδευτικά εργαλεία χρησιμοποιούνται;

Θέματα	Ημερίδες Συνέδρια	Η-μάθηση/ Βιβλιογραφία	Εκπαιδευτικά Σεμινάρια/ Διαλέξεις	Μεταπτυχιακά
Μεθοδολογίες/ Εργαλεία/ Πολιτικών Ασφάλειας/Ιδιωτικότητας	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Εργαλεία/ Λογισμικά Ασφάλειας Δικτύων	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Εργαλεία/ Λογισμικά Ψηφιακών Πειστηρίων	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Εργαλεία/ Λογισμικά Διαχείρισης Ασφάλειας	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Τεχνολογίες Υποδομής Δημόσιας Κλείδας και υπηρεσιών	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Τεχνολογίες Ασφάλειας/ Ιδιωτικότητας XML, Υπηρεσιών Ιστού	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Τεχνολογίες Διαχείρισης Ταυτοτήτων	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Κυβερνοάμυνα	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Εργαστηριακές εκπαιδεύσεις στα παραπάνω θέματα	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Θέματα	Ημερίδες Συνέδρια	Η-μάθηση/ Βιβλιογραφία	Εκπαιδευτικά Σεμινάρια/ Διαλέξεις	Μεταπτυχιακά
Άλλα (εξηγείστε)				

1β. Με τι συχνότητα γίνεται η εκπαίδευση;

*Συχνότητα*

- Ετησίως
- Κάθε 2 χρόνια
- Όποτε χρειάζεται  
(εξηγείστε)
- Δεν προσφέρεται  
συγκεκριμένη  
εκπαιδευτική διαδικασία
- Άλλο (εξηγείστε)

7) Απαιτείτε από τον φορέα, τα μέλη της ομάδας σας να έχουν κάποιο πιστοποιητικό ασφάλειας;

- ΝΑΙ – ακολουθούν οι ερωτήσεις  
4α
- ΟΧΙ

4α. Τι πιστοποιητικά απαιτούνται (σημειώστε περισσότερα από ένα αν χρειάζεται) απο το φορέα για μέλη της ομάδας σας;

*Πιστοποιητικά Ασφάλειας*

- CISSP
- CISA
- ISO27001
- NATO
- Άλλο (εξηγείστε)

#### **Δ. Προτάσεις**

Βάση του παραπάνω ερωτηματολογίου θα θέλαμε να καταγράψετε (σε ελεύθερο κείμενο, μέχρι 2 σελίδες) τις προτάσεις σας στους τρεις τομείς που αναφέρθηκαν:



- A. Αποτύπωση Δράσεων, Διαδικασιών, Ροών Εργασιών, Πληροφορίας
- B. Συνέργειες με άλλους φορείς
- Γ. Ενημέρωση, Εκπαίδευση, Πιστοποίηση

που θα βελτίωναν την αποτελεσματικότητα των δράσεων ασφάλειας/ιδιωτικότητας του φορέα σας.

**Ευχαριστούμε πολύ για το χρόνο σας και την συνεργασίας σας**