



ΗΔΙΚΑ

ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ
ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

59 ΜΕΡΕΣ ΠΡΙΝ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ GDPR (ΕΕ 2016/679)

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΕΤΟΙΜΟΤΗΤΑΣ - ΗΔΙΚΑ ΑΕ.

26/03/2018

Τμήμα Ασφ. Συστ. & Δικτύων - ΔΤΥ&ΑΣ

Agenda

- Παρουσίαση της ΗΔΙΚΑ ΑΕ
- Υφιστάμενη υποδομή Datacenter
- Μέτρα Ασφάλειας ΠΣ ΗΔΙΚΑ ΑΕ
- Νομοθετικό πλαίσιο (ΕΕ 2016/679 GDPR)
- Σχετικές Δράσεις ΗΔΙΚΑ ΑΕ
- Προκλήσεις

ΠΑΡΟΥΣΙΑΣΗ ΗΔΙΚΑ ΑΕ

Συνοπτική παρουσίαση της ΗΔΙΚΑ ΑΕ

Η Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης (Η.ΔΙ.Κ.Α. Α.Ε.) συστάθηκε με τον Ν.3607/2007 (ως μετατροπή του ΝΠΙΔ Κ.Η.Υ.Κ.Υ. ν.δ.390/1969 ΦΕΚ 283/Α΄), και είναι κρατικός φορέας (ΔΕΚΟ) με αποστολή:

- να παρέχει ολοκληρωμένες λύσεις υψηλής ποιότητας στον τομέα της **Πληροφορικής και Επικοινωνιών**, οι οποίες θα υποστηρίζουν την ορθή, πλήρη και αποτελεσματική λειτουργία των **φορέων κοινωνικής ασφάλισης και παροχής υγείας** σε βάθος χρόνου και την **εξυπηρέτηση των πολιτών**, **μέσω της παροχής σύγχρονων ηλεκτρονικών υπηρεσιών και πληροφοριών**
- να διασφαλίζει και υποστηρίζει τη **διαλειτουργικότητα των Συστημάτων Πληροφορικής και Επικοινωνιών** των φορέων που δραστηριοποιούνται σε θέματα ασφάλισης, υγείας, πρόνοιας και κοινωνικής πολιτικής

Υπηρεσίες στους Φορείς Κοινωνικής Ασφάλισης, Πρόνοιας και Υγείας

- **Διασφάλιση και υποστήριξη της διαλειτουργικότητας των Πληροφοριακών Συστημάτων** των ΦΚΑ καθώς και φορέων που δραστηριοποιούνται σε θέματα υγείας, πρόνοιας και κοινωνικής πολιτικής
- **Ενοποίηση πληροφορίας** στο χώρο της Κοινωνικής Ασφάλισης και της Υγείας στην Ελλάδα
- **Παροχή συμβουλών για θέματα ΤΠΕ** προς τους Φορείς Κοινωνικής Ασφάλισης
- **Εθνικό σημείο πρόσβασης για διασύνδεση με αντίστοιχους φορείς της Ευρωπαϊκής Ένωσης** στην Κοινωνική Ασφάλιση (EESSI) και Υγεία (NCReHealth)
- **Παροχή πληροφοριών στατιστικών ή άλλου τύπου και αξιολογήσεων** για την Κοινωνική Ασφάλιση και την Υγεία στην Ελλάδα

Ποιους εξυπηρετεί...

- 10 εκ. Ασφαλισμένους (ΑΜΚΑ, ΑΤΛΑΣ, Σύστημα Ηλ. Συνταγογράφησης κλπ)
- 2,66 εκ συνταξιούχους για τη μηνιαία πληρωμή 4,49 εκ συντάξεων
- 1,85 εκατομμύρια ασφαλισμένους σε ΟΓΑ, ΟΑΕΕ, ΤΑΝ, ΕΤΑΠ-ΜΜΕ
- 50.000 Ιατρούς
- 12.000 Φαρμακοποιούς
- 37.000 Μισθοδοτούμενους
- 500.000 Νοσηλευόμενους

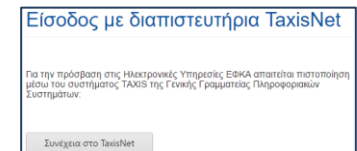
Εφαρμογές Υγείας ...

- Υλοποίησε και λειτουργεί το έργο της Ηλεκτρονικής Συνταγογράφησης
- Συντηρεί 14 εγκαταστάσεις Πληροφοριακών Συστημάτων Νοσοκομείων
- Εκδίδει τη μισθοδοσία (εφημερίες, βάρδιες) σε περισσότερα από 60 νοσοκομεία
- Ολοκληρώνει το ΟΠΣΥ για 31 Νοσοκομεία (εκτός Γ' ΚΠΣ)
- Υλοποίησε και λειτουργεί το Εθνικό Σύστημα Ηλεκτρονικών Ραντεβού με τις μονάδες υγείας
- Αναπτύσσει πλατφόρμα για την υποστήριξη των δόμων της Πρωτοβάθμιας Φροντίδας Υγείας
 - Ιατρικός Φάκελος Α'-βάθμιας
 - Πρόσβαση και Συγκατάθεση Ασθενούς



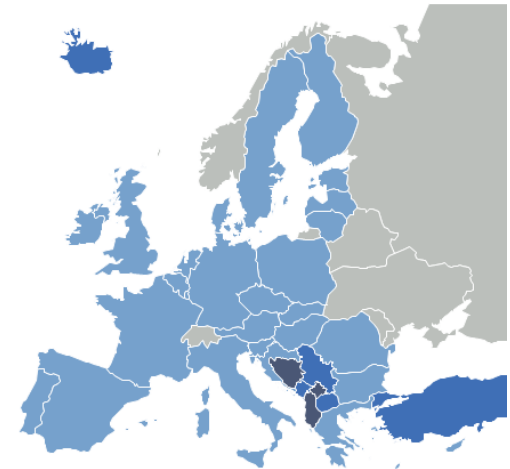
Εφαρμογές Κοινωνικής Ασφάλισης & Αλληλεγγύης ...

- Διαθέτει και συντηρεί το μοναδικό ηλεκτρονικό **μητρώο πολιτών (ΑΜΚΑ)** του Ελληνικού Κράτους
- Εκδίδει τις **συντάξεις** όλων των συνταξιούχων κάθε μήνα
- Διαθέτει ως υπηρεσία το **Ασφαλιστικό Βιογραφικό** και την **Ασφαλιστική Ικανότητα** καθενός μας και υποστηρίζει επί χρόνια τα Ασφαλιστικά Ταμεία
- Δημιούργησε τις **Ηλεκτρονικές Υπηρεσίες**, το **ενιαίο μητρώο ασφαλισμένων και συνταξιούχων**, καθώς και το Σύστημα Υπολογισμού, Είσπραξης και Εκκαθάρισης **Εισφορών Μη-Μισθωτών** του ΕΦΚΑ
- Δημιούργησε το μηχανογραφικό σύστημα που υποστηρίζει το **Κοινωνικό Εισόδημα Αλληλεγγύης (ΚΕΑ)**
- Υλοποίησε τις **απαραίτητες διασυνδέσεις** με άλλα πληροφοριακά συστήματα (ΕΦΚΑ, ΑΑΔΕ, ΟΑΕΔ) για την αυτοματοποιημένη διενέργεια διαδικασιών και ελέγχων



Εφαρμογές Εθνικού κόμβου διασυνοριακών εφαρμογών ...

- Εξασφάλισε χρηματοδότηση (CEF) για δημιουργία και λειτουργία υποδομών ως Εθνικός Κόμβος:
 - Πρόσβασης για Ηλεκτρονικές Υπηρεσίες για την Υγεία (**NCP eHealth**), και
 - Πρόσβασης για Ηλεκτρονικές Υπηρεσίες για την Ασφάλιση (**EESSI**)
- Συμμετέχει στο σχεδιασμό των υποδομών **eID** (πανευρωπαϊκή ταυτοποίηση χρηστών) και **HEALTHeID** (ταυτοποίηση ασθενών)



Η Ολοκληρωμένη πλατφόρμα αιτήσεων της ΗΔΙΚΑ

- <https://www.idika.gr/athenacard/>
- <https://www.idika.gr/kot/>
- <https://keaprogram.gr/>
- <https://www.koinonikomerisma.gr/>

Μια πρόκληση για νέα προσέγγιση με
τον πολίτη



Χαρακτηριστικά πλατφόρμας αιτήσεων ΗΔΙΚΑ

- Σύστημα διαχείρισης **κριτηρίων** (οικογένεια, φιλοξενούμενος, νοικοκυριό, κοκ)
- Διαχείριση αιτήσεων **ένταξης** και/ή μεταβολής στοιχείων (ατομικά, οικογένειας, νοικοκυριού, κοκ)
- **On-line** έγκριση/απόρριψη της αίτησης
- Διαχείριση **πληρωμών** σε δικαιούχους
- Πληθώρα **analytics** σε εθνικό επίπεδο, επίπεδο δήμου, κα
- Πολλαπλά "**κανάλια υποβολής**" αιτήσεων
- **Έλεγχοι** ορθότητας και πληρότητας στοιχείων

Επιπλέον Χαρακτηριστικά πλατφόρμας αιτήσεων ΗΔΙΚΑ

- Κλειστό ή και συνεχώς «ανοιχτό» πρόγραμμα (δεν υπάρχει συγκεκριμένη περίοδος αιτήσεων)
- Ευρύ φάσμα **on-line** διασταυρώσεων κατά:
 - την αίτηση
 - σε μηνιαία βάση
 - αλλά και **κατασταλτικά**. Ενδεικτικά: ΑΑΔΕ, ΑΜΚΑ, ΕΜΑΠΣ, Εργόσημο, ΟΑΕΔ, ΕΦΚΑ
- Τεχνικά χαρακτηριστικά:
 - Σύστημα υψηλής διαθεσιμότητας
 - Φιλικότητα προς τον χρήστη (responsive UI)
 - Ελαχιστοποίηση των καταχωρούμενων στοιχείων
- Πιστεύουμε τον πολίτη, αλλά ελέγχουμε

1^ο Χαρακτηριστικό – άμεση έγκριση

- Η αίτηση κρίνεται με την υποβολή της
- Δεκάδες ή εκατοντάδες χιλιάδες αιτήσεις την μέρα!

Στοιχεία της 1/2/2017 16:30				
	Πολίτες	ΚΕΠ	Δημοι	Σύνολο
Εγκεκριμένες	1.126	42	91	
Νέα Αίτηση	19.777	871	411	
Ακύρωση από χρήστη	716	6	17	
ολοκληρωμενη που δεν έχει υποβληθεί	481	17	22	
Μη Έγκριση	94		3	
Αντικατάσταση από άλλη (τροποποίηση)	14		1	
σύνολα	22.208	936	545	23.689
Ακυρώσεις λόγω αστοχίας επικοινωνίας με 3α συστήματα	11.050	328	453	
σύνολα	33.258	1.264	998	35.520

2^ο Χαρακτηριστικό – online διασταυρώσεις

- Ευρεία χρήση πληροφοριών που «ζουν» σε τρίτα συστήματα
 - ΑΑΔΕ: Ε1 (Έλεγχος ΑΦΜ, Προσωπικών στοιχείων, Μελών νοικοκυριού, Εισόδημα, Κινητή περιουσία, Στοιχεία Κατοικίας, Καταθέσεις), Ε2 (Ενοίκια), Ε9 (Ακίνητη Περιουσία)
 - ΗΔΙΚΑ: ΑΜΚΑ (Έλεγχος εμφάνιση ατομικών προσωπικών στοιχείων), Συντάξεις (Εισόδημα-“ΗΛΙΟΣ”), ΑΤΛΑΣ (Ασφαλιστικό Ιστορικό – Ασφαλιστική Ικανότητα), Εργόσημο, Επιδόματα
 - ΟΑΕΔ: (Επιδόματα, Ανεργίας κ.ά.)
- Δεν ζητάμε «γνωστά» στοιχεία
- Είμαστε φειδωλοί στα στοιχεία
- Προ-συμπληρώνουμε στοιχεία

3^ο Χαρακτηριστικό – εμπιστοσύνη

- Ο πολίτης καλείται να αποδείξει κάτι μόνο αν διαφωνεί με αυτό που έχουμε βρει από διασταυρώσεις
- Κατακόρυφη μείωση της γραφειοκρατίας
- Ελαχιστοποίηση συναλλαγής πολίτη με υπάλληλο

4^ο Χαρακτηριστικό – φιλικό στον χρήστη

- Σύγχρονο User Interface
- Responsive design (ταμπλέτες, κινητά, μεγάλες οθόνες)
- Καθαρό User Interface με βοήθεια εκεί που ακριβώς χρειάζεται

Οικονομικά Στοιχεία- Εισοδήματα τελευταίων 6 μηνών: 01-09-2016 - 28-02-2017

Προσοχή: Παρακαλούμε ενημερώστε τον πολίτη ότι οφείλει να υποβάλει τα στοιχεία σωστά ανεξάρτητα αν έχουν βρεθεί από τις διασταυρώσεις την ώρα της αίτησης. ×

Οι διασταυρώσεις είναι συνεχείς και αν διαπιστωθεί υποβολή αίτησης με μη αληθή στοιχεία τα στοιχεία διαβιβάζονται στη Διεύθυνση Καταπολέμησης της Φτώχειας και εφόσον διαπιστωθεί ότι η καταβολή έγινε χωρίς να πληρούνται οι νόμιμες προϋποθέσεις εκδίδεται πράξη διακοπής της καταβολής. Σε αυτή την περίπτωση, το νοικοκυριό δικαιούται να επανυποβάλει αίτηση για το πρόγραμμα μετά την πάροδο ενός έτους, από την ημερομηνία έκδοσης της πράξης διακοπής και με την προϋπόθεση ότι έχουν επιστραφεί τα αχρεωστήτως καταβληθέντα.

Μισθοί	742,88 ⬇	Συντάξεις	0,00 ⬇
0,00 ?		0,00 ?	

Αφορά το σύνολο από μισθούς, ημερομίσθια κτλ το τελευταίο έμμηνο 01-09-2016 - 28-02-2017 (& αλλοδαπής προέλευσης).
Πρέπει να καταχωρηθεί το συνολικό ποσό και αυτόματα θα εξαιρεθεί το 20% στους υπολογισμούς

Αντιστοιχεί στο άθροισμα των πεδίων [301], [389], [391], [393], [255], [251], [263], [311], [343], [325] του εντύπου Ε1:
Αν απουσία είναι η σύζυγος, τα πεδία είναι τα αντίστοιχα της συζύγου δηλαδή τα: [302], [390], [392], [394], [256], [252], [264], [312], [344], [326]

Αγροτική δραστηριότητα	0,00 ?	Επιχειρήσεις, Ελ. Επαγγέλματα	0,00 ?
------------------------	---------------------	-------------------------------	---------------------

5^ο Χαρακτηριστικό – Έλεγχοι

➤ Έλεγχοι (auditing), το λέμε και το εννοούμε

Ιστορικό Αίτηση: 170-225-1111111111, Κατάσταση: Ανενεργή					
Ημερομηνία/Ωρα	Ενέργεια	Χρήστης		Κανάλι	Λεπτομέρειες Χρήστη
24-02-2017 09:16:33	Δημιουργία	afn	44	Πολίτης/TaxisNet	ΑΦΜ: 1'
24-02-2017 09:16:33	Νέα Αίτηση	afn	44	Πολίτης/TaxisNet	ΑΦΜ: 1'
25-02-2017 09:13:56	Ολοκλήρωση	std	gmail.com	Δήμος	ΓΕΩΡΓΙ
25-02-2017 09:14:15	Υποβολή	std	gmail.com	Δήμος	ΓΕΩΡΓΙ
25-02-2017 09:14:15	Έγκριση	std	gmail.com	Δήμος	ΓΕΩΡΓΙ
28-02-2017 23:59:59	Απενεργοποίηση	sys:audit			
01-03-2017 18:39:13	Τελευταία Μεταβολή				

Λόγος Μη Έγκρισης / Παρατηρήσεις: Από τις διασταυρώσεις, προέκυψε ότι μένετε στο ίδιο σπίτι με τα εξής πρόσωπα: 170-225-1111111111 που έχουν υποβάλει επίσης αίτηση για το ΚΕΑ: (170-225-1111111111). Παρακαλούμε να ανακαλέσετε άμεσα όλες τις αιτήσεις σας και υποβάλλετε κοινή αίτηση ως ενιαίο νοικο

Analytics σε εθνικό επίπεδο ή επίπεδο δήμου

Dashboard

(Επικράτεια)

20.838

Draft Αιτήσεις

155.834

Εγκεκριμένες ή
Ενεργές Αιτήσεις

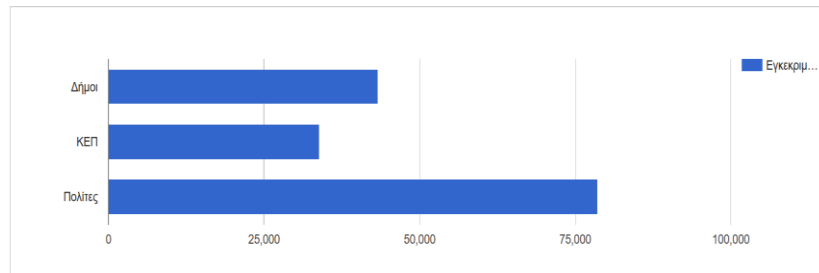
€34.070.998

Μηνιαίο
Προϋπολογιζόμενο
κόστος

€218

Μέσο κόστος ανά
αίτηση

Διασπορά αιτήσεων ανά κανάλι



Δήμοι
ΚΕΠ
Πολίτες

Κανάλι	Αιτήσεις
Δήμοι	43,278
ΚΕΠ	33,902
Πολίτες	78,654

Dashboard

ΖΑΚΥΝΘΟΥ

66

Draft Αιτήσεις

392

Εγκεκριμένες ή
Ενεργές Αιτήσεις

€82.993

Μηνιαίο
Προϋπολογιζόμενο
κόστος

€211

Μέσο κόστος ανά
αίτηση

Διασπορά αιτήσεων ανά κανάλι

Διασπορά αιτήσεων ανά κατάσταση

Πληροφορίες εγκεκριμένων & ενεργών αιτήσεων

Πληροφορίες νοικοκυριών

206

Νοικοκυριά με μηδέν
εισόδημα

87

Νοικοκυριά με εισόδημα
από Επίδομα

184

Νοικοκυριά με ακίνητα

Τι χρειάστηκε για την επίτευξη αυτών;

Με χρώμα αυτά που μας προβλημάτισαν ιδιαίτερα...

- Άνθρωποι και ομαδικό πνεύμα
- Υλικοτεχνική υποδομή (HW)
- System SW (Άδειες Λογισμικού)
- Δίκτυα (ναι και DRS)
- Ανάπτυξη Εφαρμογών (Software)
- Λειτουργία - Παρακολούθηση
- Υποστήριξη - Help Desk
- Υποδομή ψηφιακής πιστοποίησης του πολίτη

ΥΦΙΣΤΑΜΕΝΗ ΥΠΟΔΟΜΗ DATA CENTER ΗΔΙΚΑ

Κτιριακές υποδομές

- Η ΗΔΙΚΑ, μέσω του σύγχρονου Κέντρο Δεδομένων που έχει κατασκευαστεί το 2015 επί της οδού Λυκούργου 10, 105 51 Αθήνα, παρέχει υπηρεσίες φιλοξενίας δικτυακών υποδομών υψηλών προδιαγραφών εξασφαλίζοντας την μέγιστη διαθεσιμότητα και την ασφάλεια τους και την παροχή υπηρεσιών υπολογιστικού νέφους (cloud computing) στους Φορείς Κοινωνικής Ασφάλισης, Πρόνοιας, Υγείας και λοιπούς φορείς που υποστηρίζει.
- Το Κέντρο Δεδομένων καλύπτει επιφάνεια **465 τ.μ.** του κτιρίου και αποτελείται από:
 - Δύο ανεξάρτητους χώρους Computer Room
 - Χώρο Μονάδας Η/Ζ
 - Ξεχωριστό Χώρο Διαχειριστών C.R. (και εισαγωγής τηλεπικοινωνιών)
 - Χώρο UPS (με ξεχωριστό χώρο για τις μπαταρίες του)
 - Χώρο Δεξαμενής Καυσίμου
 - Άλλους Βοηθητικούς χώρους

Εξοπλισμός κτιριακών υποδομών

- **Σύστημα Πυρασφάλειας-Πυρανίχνευσης:**
 - περιλαμβάνει τοπικούς πίνακες κατάσβεσης με FM200
 - φωτισμό ασφαλείας και σήμανση οδεύσεων διαφυγής
 - Διπλές ζώνες πυρανίχνευσης (CROSS ZONING)
- **Κλιματισμός:**
 - Διπλά συστήματα ανά Computer Room
 - Αυτόνομο σύστημα για τα γραφεία υπαλλήλων
- **UPS/αδιάλειπτη παροχή τροφοδοσίας:**
 - συστοιχία 2 UPS / 160 KVA έκαστο (32 & 27 KVA με χρήση ψηφιακών φίλτρων)
 - γεννήτριας πετρελαίου μεγέθους 450 KVA
 - υποσταθμό της ΔΕΗ
- **Έλεγχος φυσικής πρόσβασης:**
 - Access control (διπλές θύρες – πάντα μια κλειστή)
 - IP CCTV (24x7 καταγραφή - κεντρικό σημείο παρακολούθησης)
- **Building Management System (BMS)**
 - 24x7 με συμβεβλημένο κέντρο παρακολούθησης κτιρίου

Υποδομές Πληροφορικής

- 40 και πλέον RACKs που φιλοξενούν:
 - Servers (επί το πλείστον τεχνολογίας Blade Servers)
 - SAN storages (FC-Fabric),
 - Tape Backup Libraries,
 - Network & Security systems, κλπ
- Physical servers > 170
- Virtual servers > 320

Τεχνολογίες Υποδομών Πληροφορικής

➤ Τεχνολογίες virtualization

- MS HyperV
- Oracle VM
- VMWare

➤ Λειτουργικά συστήματα

- Oracle Enterprise Linux
- CentOS
- Solaris
- IBM AIX
- MS Windows (Server 2008, Server 2012, Server 2016)

Ποσοστά κάλυψης Υποδομών Πληροφορικής

- Χωρική κάλυψη > 55 %
- Υπολογιστική ισχύς
(physical CPU cores > 62 %)
- Storage > 74 %
- Δικτυακά > 40 %

ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Νομοθετικό πλαίσιο προ GDPR

- Ενοποιημένη απόδοση Συνθήκης για την Ευρωπαϊκή Ένωση Άρθρο 39.
- Συνθήκη για την Λειτουργία της Ευρωπαϊκής Ένωσης Άρθρο 16.
- Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ Άρθρα 7 & 8.
- Ελληνικό Σύνταγμα, Άρθρα 9, 9^Α, & 19.
- Οδηγία 95/46/ΕΚ-24.10.1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για την ελεύθερη κυκλοφορία αυτών των δεδομένων.
- Νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Οδηγία 2002/58/ΕΚ-12.07.2002 σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.
- Νόμος 3471/2006 για την προστασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν.2472/1997.

ΜΕΤΡΑ ΣΥΜΟΡΦΩΣΗΣ

- Διοικητικά
- Οργανωτικά
- Τεχνικά
- Συλλογή ψηφιακών πειστηρίων

ΔΙΟΙΚΗΤΙΚΑ ΜΕΤΡΑ

Διοικητικά μέτρα

- «Μελέτη Ασφάλειας Πληροφοριακών Συστημάτων ΚΗΥΚΥ»
(Σύμβαση 30/2002 & ΠΠ1-13/06/2005 & ΠΠ2-29/05/2007)
 - Έγγραφο ΑΠ:117/09.01.2003 ΚΗΥΚΥ, Θέμα: «Μικροεξοπλισμός Χρηστών»
 - Έγγραφο ΑΠ:118/09.01.2003 ΚΗΥΚΥ, Θέμα: «Νομιμότητα Χρήσης Λογισμικού»
 - Έγγραφο ΑΠ:2127/07.03.2003 ΚΗΥΚΥ, Θέμα: «Κανόνες Σύνδεσης στο Τοπικό Δίκτυο ΚΗΥΚΥ»
- «Πολιτική Ασφαλείας» της ΗΔΙΚΑ ΑΕ με έγκριση της Διοίκησης
(ΑΠ:8763/19.06.2013)
- Εγχειρίδιο Βασικών Αρχών Ασφαλείας (διανέμεται σε όλους τους υπαλλήλους χρήστες της ΗΔΙΚΑ ΑΕ καθώς και στους συνεργάτες)
- Σύστημα Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων (κατάλογος ελεγχόμενων εντύπων)

Πολιτική Ασφαλείας

- **Σκοπός:** «...να καθορίσει την συμπεριφορά των χρηστών σε θέματα προστασίας ΠΣ και να μετατρέψει τους υπαλλήλους της ΗΔΙΚΑ σε ενεργά μέλη ασφαλείας»
«Περιλαμβάνει όλες τις διατάξεις πρόληψης και προστασίας που εφαρμόζονται για την μείωση ή την εξάλειψη των κινδύνων και των συνεπειών από πράξεις, εσωτερικές ή εξωτερικές, σκόπιμες ή μη και τυχαίες που μπορεί να είναι επιζήμιες για την περιουσία της ΗΔΙΚΑ»
- **Στόχος:** «... προστασία της περιουσίας της ΗΔΙΚΑ από κινδύνους ζημίας, αποκάλυψης απόρρητων πληροφοριών ή παράνομης τροποποίησης σε συνάρτηση με τον ευαίσθητο χαρακτήρα των πληροφοριακών συστημάτων.»

Πολιτική Ασφαλείας-Πεδίο δράσης

- Χρήστες ΠΣ – Όλο το προσωπικό της ΗΔΙΚΑ ΑΕ
- Όλα τα ΠΣ (διαχείρισης, ανάπτυξης, επεξεργασίας κλπ)
- Όλο το Υλικό (HW), Λογισμικό (SW), Δίκτυα, κλπ
- Όλες τις πληροφορίες, τεχνικού, βιομηχανικού, εμπορικού, και προσωπικού περιεχομένου που αποθηκεύονται ή μεταδίδονται προς τα ΠΣ της ΗΔΙΚΑ ΑΕ

Πολιτική Ασφαλείας - Περιεχόμενο

- Οργανωτικές αρχές και αρμοδιότητες
- Εκπαίδευση
- Διαβάθμιση Πληροφοριακών Συστημάτων
- Ασφάλεια Πληροφοριακών Συστημάτων
- Οριζόμενες διαδικασίες ΠΣ
- Διαχείριση των Κωδικών Ασφαλείας
- Χρήση των υπηρεσιών του Internet
- Ανίχνευση και αντιμετώπιση κακόβουλου λογισμικού
- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Αναφορά περιστατικών ασφαλείας στο Τμ. Ασφ.

Πολιτική Ασφαλείας - Ορισμοί

- Ιδιοκτήτης πληροφοριακού συστήματος
- Χρήστης πληροφοριακού συστήματος
- Πληροφοριακό Σύστημα
- Δεδομένα
- Πληροφορίες

Εξασφάλιση Εμπιστευτικότητας & Εχεμύθειας

- «**ΚΩΔΙΚΑΣ ΔΕΟΝΤΟΛΟΓΙΑΣ**» εξουσιοδοτημένων χρηστών Πληροφοριακών Συστημάτων της ΗΔΙΚΑ ΑΕ
- «**ΙΔΙΩΤΙΚΟ ΣΥΜΦΩΝΗΤΙΚΟ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ & ΕΧΕΜΥΘΕΙΑΣ**» μεταξύ ΗΔΙΚΑ ΑΕ και Εξωτερικών Συνεργατών
- **ΣΥΜΒΑΣΕΙΣ ΕΡΓΩΝ** (συμπεριλαμβάνονται όροι Εμπιστευτικότητα & Εχεμύθειας με τους συμβαλλόμενους Αναδόχους των Έργων)

ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ

Κατάλληλο Οργανόγραμμα

- Λειτουργία «Διεύθυνσης Τεχνικής Υποστήριξης και Ασφάλειας Συστημάτων»
- Λειτουργία «Τμήματος Ασφάλειας Συστημάτων & Δικτύων» κάτω από την Διεύθυνση Τεχνικής Υποστήριξης & Ασφάλειας Συστημάτων
- «Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων»

Αρμοδιότητες Υπεύθυνου Ασφαλείας

- Ο ορισμός ενός ιδιοκτήτη για κάθε ΠΣ (παράδοση έντυπου ταυτότητας ΠΣ)
- Η δημιουργία αποτελεσματικού τρόπου διαβάθμισης των ΠΣ
- Η δημιουργία οδηγιών για τα ΛΣ, τις υπηρεσίες και τις εφαρμογές των ΠΣ
- Η δημιουργία ενός προγράμματος εποπτείας για την αποτελεσματικότητα των μέτρων προστασίας και της ΠΑ
- Η δημιουργία ενός προγράμματος εποπτείας για την αποτελεσματικότητα των κωδικών ασφαλείας των ΠΣ της ΗΔΙΚΑ
- Η δημιουργία ενός προγράμματος εποπτείας τήρησης της ΠΑ και των διαδικασιών από τους ιδιοκτήτες των ΠΣ
- Η δημιουργία μιας αποτελεσματικής διαδικασίας αντιμετώπισης περιστατικών ασφαλείας
- Ο συντονισμός και προγραμματισμός των ενεργειών του Τμ. Ασφάλειας
- Ο εμπλουτισμός των ήδη υπαρχόντων μέτρων ασφαλείας
- Ο συντονισμός της εκπαίδευσης των υπαλλήλων του Τμ. Ασφάλειας ΠΣ σε θέματα ασφαλείας
- Η ενημέρωση, η σύνταξη πορισμάτων και οι γνωμοδοτήσεις σε θέματα ασφαλείας ΠΣ

Αρμοδιότητες Τμ. Ασφαλείας

- Υλοποίηση Σχεδίου ασφαλείας για κάθε νέο ΠΣ
- Υλοποίηση αρχιτεκτονικής ασφαλείας του δικτύου, και επιλογή των λογισμικών ασφαλείας και παρακολούθηση των περιστατικών ασφαλείας
- Δημιουργία διαδικασίας ενημέρωσης antivirus με το τελευταίο αρχείο ανίχνευσης και αντιμετώπισης ιών
- Τον έλεγχο των απαραίτητων μέτρων προστασίας κάθε ΠΣ πριν συνδεθεί στο δίκτυο και σε τακτά/απρόοπτα χρονικά διαστήματα
- Την εκπαίδευση των χρηστών σε θέματα ασφαλείας ΠΣ
- Την εποπτεία για την αποτελεσματικότητα των μέτρων προστασίας και την ΠΑ
- Την παρακολούθηση και την αποστολή των νέων service packs και security hot fixed των ΠΣ προς τους ιδιοκτήτες αυτών
- Τον έλεγχο της αποτελεσματικότητας των κωδικών ασφαλείας των ΠΣ
- Την εποπτεία τήρησης της ΠΑ και των διαδικασιών από τους ιδιοκτήτες των ΠΣ
- Την παρακολούθηση νέων τρωτών σημείων που ανακοινώνονται από τους κατασκευαστές των ΠΣ και την δημιουργία μέτρων προστασίας από αυτά
- Την αντιμετώπιση περιστατικών ασφαλείας.

Ευθύνη Ιδιοκτητών ΠΣ

- Στην διαβάθμιση των πληροφοριακών συστημάτων τους
- Στην εφαρμογή και την διαχείριση των μέτρων προστασίας όπως περιγράφονται στην ΠΑ ή σύμφωνα με τις οδηγίες που θα τους δοθούν από το Τμ. Ασφ.
- Στην εγκατάσταση των service packs και security hot fixes που θα τους δοθούν από το Τμ. Ασφ.
- Στην διαχείριση του Πληροφοριακού Συστήματος ευθύνης τους
- Στην εποπτεία των γεγονότων ασφαλείας στο ΠΣ που έχουν στην ευθύνη τους
- Στην ενημέρωση του Τμ. Ασφ. πριν την σύνδεση του ΠΣ που έχουν στην ευθύνη τους στο δίκτυο
- Στην δημιουργία και την παράδοση των απαραίτητων οδηγιών χρήσης στους χρήστες του συγκεκριμένου ΠΣ
- Να μπορούν να αποδείξουν στο Τμ. Ασφ. όποτε ζητηθεί, ότι τηρούν τους κανόνες ασφαλείας
- Στον ορισμό έγγραφων διαδικασιών όπως αυτές καθορίζονται από την ΠΑ
- Στην συμπλήρωση της ταυτότητας του ΠΣ που θα λάβουν από τον υπεύθυνο ασφαλείας και την παράδοση ενός υπογεγραμμένου αντιγράφου σε αυτόν
- Για να ενημερώσουν τον υπεύθυνο ασφαλείας για οποιαδήποτε αλλαγή στην ταυτότητα του ΠΣ ευθύνης τους ώστε να δημιουργηθεί η νέα ταυτότητα ΠΣ
- Για την άμεση ενημέρωση του Τμ. Ασφαλείας σε οποιοδήποτε περιστατικό ασφαλείας πέσει στην αντίληψή τους σύμφωνα με την πολιτική αντιμετώπισης περιστατικών ασφαλείας

Ευθύνη Χρηστών ΠΣ

- Στην τήρηση των κανόνων ασφαλείας όπως αυτοί περιγράφονται στο «**εγχειρίδιο ασφαλείας**»
- Για την αίτηση πρόσβασης προς τον ιδιοκτήτη των ΠΣ στα οποία θέλουν να αποκτήσουν πρόσβαση
- Να χρησιμοποιούν τα ΠΣ μόνο για την νόμιμη χρήση που τους έχει εξουσιοδοτηθεί από τον ιδιοκτήτη αυτών
- Να υπακούουν στους κανόνες και στα μέτρα προστασίας που έχει ορίσει ο ιδιοκτήτης για το κάθε ΠΣ
- Να προστατεύουν τον λογαριασμό τους (**user account**) και τον κωδικό ασφαλείας (**password**) τους σύμφωνα με το «**εγχειρίδιο ασφαλείας**»
- Να αναφέρουν στο Τμ. Ασφ. οποιοδήποτε περιστατικό ασφαλείας υποπέσει στην αντίληψη τους και θεωρούν ότι είναι ύποπτο

Διαβάθμιση Πληροφοριακών Συστημάτων

- Η «Διαβάθμιση» απευθύνεται στους ιδιοκτήτες των ΠΣ για τα ΠΣ
- Οι ιδιοκτήτες των ΠΣ ταξινομούν αυτά σύμφωνα με τα κριτήρια διαθεσιμότητας και ευαισθησίας σε:
 - Διαβάθμιση διαθεσιμότητας: 80%, 95%, 99.5% και 99.9%
 - Downtime ανά περιστατικό: 1 εβδομάδα, 1 ημέρα, 1 ώρα, 1 ώρα
 - Διαθεσιμότητα σε ημέρες: εργάσιμες, εργάσιμες, εργάσιμες, 7
 - Διαθεσιμότητα σε ώρες: - , - , 07:00 με 18:00, 24 ώρες
 - Διαβάθμιση ευαισθησίας (εμπιστευτικότητα και ακεραιότητα)
 - Επίπεδο-1: δημόσια μη εμπιστευτικού χαρακτήρα
 - Επίπεδο-2: για εσωτερικούς μόνο χρήστες
 - Επίπεδο-3: εμπιστευτικού χαρακτήρα
 - Επίπεδο 4: απόρρητου χαρακτήρα

Ασφάλεια Πληροφοριακών Συστημάτων

- Εξαρτάται από το είδος των δεδομένων που επεξεργάζεται και αποθηκεύει το ΠΣ καθώς και την διαβάθμισή του
- Σκοπός είναι να δημιουργηθούν τα κατάλληλα μέτρα προστασίας του ΠΣ σε συνδυασμό με την διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα, των δεδομένων
 - Backups (retention period, restore tests, off-premises copies, DRS, κα)
 - Λειτουργικό περιβάλλον (H/Z, UPS, κλιματισμός, πυρασφάλεια, κα)
 - Οργάνωση (Συμβόλαιο Συντήρησης, Υποστήριξης, SPs, Hot Fixes, κα)
 - Πλεονασμός (H/W, S/W, RAID, Clusters, Mirroring, ανταλλακτικά, κα)
 - Μοναδικά user accounts, και καθορισμός δικαιωμάτων πρόσβασης
 - Κρυπτογράφηση δεδομένων, και auditing

Ασφάλεια Δικτύων 1

- Καθορίζονται τα μέτρα προστασίας που εφαρμόζονται στα δίκτυα δεδομένων και οι απαραίτητοι πόροι λειτουργίας αυτών
- Κάθε δίκτυο διαβαθμίζεται σύμφωνα με τις πληροφορίες που διέρχονται από αυτό:
 - **Συνδέσεις με ασφαλή εξωτερικά δίκτυα** («οτιδήποτε δεν απαγορεύεται επιτρέπεται»)
 - **Συνδέσεις με μη προστατευμένα δίκτυα ή προέκταση σε άλλο οργανισμό** («όλα απαγορεύονται εκτός από αυτά που ρητώς επιτρέπονται»)
 - **Συνδέσεις απομακρυσμένων δικτύων μέσω ασφαλούς μέσου μεταφοράς** («οτιδήποτε δεν απαγορεύεται επιτρέπεται»)
 - **Συνδέσεις απομακρυσμένων δικτύων μέσω ανασφαλούς δικτύου/internet** («όλα απαγορεύονται εκτός από αυτά που ρητώς επιτρέπονται»)

Ασφάλεια Δικτύων 2

- Γενικοί έλεγχοι που διενεργούνται κατά την μεταφορά δεδομένων:
 - Της ταυτότητας το πόρου απ όπου πραγματοποιήθηκε η κλήση (IP address)
 - Της ταυτότητας του καλούμενου πόρου (IP address, DNS name)
 - Η ώρα και ημερομηνία σύνδεσης (timestamp)
 - Ο Λόγος τυχόν απόρριψης της σύνδεσης (audit log)
 - Η αναγνώριση του χρήστη εάν αυτό είναι δυνατόν (user-ID)
 - Το πρωτόκολλο επικοινωνίας (tcp, udp, κα)
 - Η υπηρεσία (http, https, ftp, rdp, ssh, telnet, κα)

Διαχείριση κωδικών ασφαλείας

- Ο παρόν κανονισμός έχει σαν σκοπό να παρουσιάσει στους ιδιοκτήτες των ΠΣ ποιους κανόνες πρέπει να ακολουθούν για την δημιουργία και διαχείριση των κωδικών ασφαλείας:
 - Οι κωδικοί ασφαλείας (*password*) θα αποτελούνται από τουλάχιστον 6 ή περισσότερους χαρακτήρες
 - Οι κωδικοί ασφαλείας θα πρέπει να προέρχονται από την μίξη γραμμάτων και αριθμών σε τυχαία σύνταξη και σε καμία περίπτωση δεν θα πρέπει να είναι ονόματα, τηλέφωνα, ημερομηνίες
 - Οι κωδικοί ασφαλείας (*password*) θα πρέπει να αλλάζουν ανά 2 μήνες
 - Ένας κωδικός ασφαλείας (*password*) θα πρέπει να ξαναχρησιμοποιείται μετά από 10 τουλάχιστον αλλαγές κωδικού ασφαλείας (*password*)

Χρήση υπηρεσιών Internet

- Ο παρόν κανονισμός απευθύνεται σε όλους τους χρήστες της ΗΔΙΚΑ και έχει σαν σκοπό να τους ενημερώσει για τους κινδύνους του Internet και πως πρέπει να χρησιμοποιούν τις υπηρεσίες του:

- ***Μη εξουσιοδοτημένη χρήση***

- ***Εξουσιοδοτημένη χρήση***

Μη εξουσιοδοτημένη χρήση υπηρεσιών Internet

- **Οι χρήστες ΔΕΝ πρέπει να χρησιμοποιούν την υποδομή πρόσβασης στο Internet για:**
- Αντιγραφή, αποκάλυψη, μεταφορά, εξέταση, αλλαγή ονομασίας, ανάγνωση ή διαγραφή πληροφοριών ή προγραμμάτων που ανήκουν στην ΗΔΙΚΑ χωρίς έγκριση
- Παραβίαση ή παράκαμψη των μηχανισμών ασφαλείας που έχει η ΗΔΙΚΑ για προστασία από το Internet
- Χρήση της internet πρόσβασης για την απόκτηση παράνομης πρόσβασης σε άλλο υπολογιστικό σύστημα ή υπηρεσία
- Αντιγραφή οποιουδήποτε προγράμματος ή πληροφορίας μέσω Internet από μη αναγνωρισμένα Internet Site
- Δεν επιτρέπεται να χρησιμοποιείται η προσφερόμενη πρόσβαση στο Internet με τέτοιο τρόπο ώστε να παρουσιάζετε τον εαυτό σας σαν κάποιο άλλο πρόσωπο, πραγματικό ή φανταστικό
- Άνοιγμα κάθε είδους αρχείου προερχομένου από το Internet χωρίς virus scan
- Εγκατάσταση οποιουδήποτε προγράμματος ή συσκευής χωρίς την έγκριση από κάποιον αρμόδιο
- Σύνδεση σε Internet sites με μη επαγγελματικό περιεχόμενο
- Δημιουργία Internet account με ίδιο user name και password με αυτό που έχετε στην ΗΔΙΚΑ

Εξουσιοδοτημένη χρήση υπηρεσιών Internet

- Σύνδεση σε οποιοδήποτε Web Site για επαγγελματικούς λόγους
- Download εγκεκριμένων αρχείων από την ΗΔΙΚΑ και αφού έχει υλοποιηθεί ο απαραίτητος έλεγχος για ιούς
- Σύνδεση και χρήση των υπηρεσιών του Internet μόνο με το λογισμικό και το υλικό το οποίο έχει καθοριστεί από την ΗΔΙΚΑ

Ανίχνευση και αντιμετώπιση Κακόβουλου Λογισμικού

- Η Πολιτική αντιμετώπισης «Κακόβουλου λογισμικού» έχει σαν σκοπό την μείωση των περιστατικών ασφαλείας λόγω της μόλυνσης ενός συστήματος από ιό.
- **Κίνδυνοι:**
 - Κάθε μεταφορά αρχείων περικλείει τον κίνδυνο μόλυνσης του υπολογιστή σας από κακόβουλο κώδικα.
 - Ο κακόβουλος κώδικας μπορεί να είναι ιός (virus), σκουλήκι (worm) ή και δούρειος ίππος (Trojan horse)
- **Μέτρα προστασίας:**
 - Αντίγραφα ασφαλείας
 - Χρήση λογισμικού ανίχνευσης κακόβουλου λογισμικού (ΠΟΤΕ ΜΗΝ απενεργοποιείτε το λογισμικό αυτό)

Ασφάλεια ηλεκτρονικού ταχυδρομείου (e-Mail)

- Σκοπός αυτής της Πολιτικής είναι η δημιουργία των απαραίτητων μέτρων προστασίας του ηλεκτρονικού ταχυδρομείου επιπλέον από τα μέτρα προστασίας των πληροφοριακών συστημάτων
- **Κίνδυνοι:**
 - Κάθε μεταφορά αρχείων με ηλεκτρονικό ταχυδρομείο περικλείει τον κίνδυνο μόλυνσης του υπολογιστή σας από κακόβουλο κώδικα.
 - Ο κακόβουλος κώδικας μπορεί να είναι ιός (virus), σκουλήκι (worm) ή και δούρειος ίππος (Trojan horse)
- **Μέτρα προστασίας:**
 - Για κάθε σύστημα ηλεκτρονικού ταχυδρομείου θα υπάρχει λογισμικό ανίχνευσης ιών το οποίο θα ελέγχει για κακόβουλο κώδικα στα e-mail πριν αυτά παραδοθούν στους χρήστες
 - Δεν επιτρέπεται η χρήση του εξυπηρετητή ηλεκτρονικού ταχυδρομείου για αποστολή Email σε παραλήπτες εκτός των χρηστών της ΗΔΙΚΑ
 - Καθορίζεται ανώτατο όριο μεγέθους ηλεκτρονικού μηνύματος
 - Καθορίζεται ανώτατο όριο αποθήκευσης ηλεκτρονικών μηνυμάτων (γραμματοκιβώτιο)

Αναφορά περιστατικών ασφαλείας

- Σκοπός της Πολιτικής διαχείρισης περιστατικών ασφαλείας Πληροφοριακών Συστημάτων είναι η κεντρική αναφορά των περιστατικών ασφαλείας των ΠΣ της ΗΔΙΚΑ προς το Τμ. Ασφαλείας.
- **Περιστατικό Ασφαλείας** θεωρείται κάθε μη εξουσιοδοτημένη χρήση πόρων ή Πληροφοριακού Συστήματος, όπως ιοί, χρήση μη εξουσιοδοτημένου λογαριασμού και κωδικού ασφαλείας, προσπάθειες εισβολής, κλπ
- Οι εισβολές έχουν ποικίλες μορφές και περιλαμβάνουν:
 - Άρνηση υπηρεσιών (DoS, DDoS)
 - Μη εξουσιοδοτημένη πρόσβαση (διαρροή, αλλαγή, ή καταστροφή δεδομένων)
 - Μεταβολή ιστοσελίδας (αλλαγή περιεχομένου)
 - Ανίχνευση τρωτών σημείων (Vulnerability scanning)
 - Απόπειρα ανεύρεσης λογαριασμών και κωδικών ασφαλείας (user names/passwords)
 - Social Engineering (fishing κλπ)

Διαδικασία Αναφοράς Περιστατικών Ασφαλείας

- **ΠΡΟΣΟΧΗ:** Αναφέρετε το οποιοδήποτε περιστατικό ασφαλείας των πληροφοριακών συστημάτων της ΗΔΙΚΑ ακόμη και εάν μετά αποδειχτεί απλό λάθος.
- **Διαδικασία:**
 - Ενημερώστε αμέσως τους υπευθύνους της ΗΔΙΚΑ και το Τμήμα Ασφαλείας
 - Συμπληρώστε την φόρμα (έντυπο) ανίχνευσης περιστατικών ασφαλείας και παραδώστε την στους υπευθύνους της ΗΔΙΚΑ (και το Τμ. Ασφ.)
 - Ακολουθήστε πιστά τις οδηγίες του Τμήματος Ασφαλείας της ΗΔΙΚΑ.
 - Μην αναφέρετε το περιστατικό ασφαλείας στους συναδέλφους σας (και εκτός ΗΔΙΚΑ) εκτός και αν σας δοθεί σχετική οδηγία από το Τμ. Ασφαλείας της ΗΔΙΚΑ.


Λειτουργία «Συστήματος διαχείρισης ασφάλειας»

- Διαχείριση αγαθών,
- Ασφάλεια Προσωπικού,
- Φυσική & Περιβαλλοντική Ασφάλεια,
- Λειτουργίες Οργανισμού και επικοινωνίες,
- Έλεγχος Πρόσβασης,
- Ασφάλεια κατά την κτήση, ανάπτυξη και συντήρηση λογισμικού,
- Διαχείριση περιστατικών ασφαλείας Πληροφοριακών Συστημάτων,
- Διαχείριση επιχειρησιακής συνέχειας,
- Συμμόρφωση με πρότυπα.


Έντυπα Διαχείρισης Ασφάλειας

- Έντυπα Πολιτικών
- Έντυπα Διαδικασιών
- Έντυπα Οδηγιών
- Έντυπα χρέωσης πόρων


Έντυπα Διαχείρισης Ασφάλειας

	Πολιτική Έλεγχος Πρόσβασης	no : Αναθ		
Συντάκτης:	Έγκριση:			
ΣΚΟΠΟΣ:	Ο έλεγχος της πρόσβασης στις πληροφορίες της ι απαγόρευση της μη εξουσιοδοτημένης πρόσβασης.			
ΠΕΡΙΓΡΑΦΗ:				
Πεδίο εφαρμογής				
Αυτή η πολιτική βρίσκεται εφαρμογή σε όλο το προσωπικό που έχει πρόσβαση στα συστήματα της Εταιρείας.				
Πολιτική				
<ul style="list-style-type: none">Τα δικαιώματα πρόσβασης των χρηστών περιγράφονται στον κατάλογο με τις χρήστών (EH_4292)Οι απαιτήσεις ασφαλείας καθώς και οι πληροφορίες για κάθε σύστημα περιγράφονται στην επικινδυνότητα του.Τα δικαιώματα πρόσβασης για κάθε σύστημα δίδονται από τις ακόλουθες αρχές:<ul style="list-style-type: none">Αρχικά απαγορεύονται τα πάντα και στη συνέχεια επιτρέπονται οι απαραίτητες.Αλλαγές στα δικαιώματα των χρηστών, γίνονται από τη ΔΤΥ&ΑΣΟι αλλαγές στα δικαιώματα πρόσβασης καταγράφονται.Παρέχονται τα ελάχιστα δικαιώματα ανά ρόλο.Η Εταιρεία τηρεί ασφαλείς διαδικασίες για τη προσθήκη νέων χρηστών, της επέμβασης πρόσβασης των χρηστών και στην διαγραφή των χρηστών.Οι μηχανισμοί ελέγχου πρόσβασης διασφαλίζουν ότι υπάρχει δυνατότητα των ατόμων που πραγματοποιήσε μία ενέργεια. Η αρχή αυτή ισχύει τόσο για τους διαχειριστές.Οι χρήστες λαμβάνουν οδηγίες για την επιλογή και διαχείριση των συνθηκών.Η εταιρεία έχει θεσπίσει για κάθε ρόλο τα απαραίτητα δικαιώματα που περιγράφονται στο αρχείο ρόλων των χρηστώνΟι χρήστες δεν επιτρέπεται να αλλάζουν τα δικαιώματα πρόσβασης τους.				

Εμπιστευτικό

	Πολιτική Αποδεκτή Χρήση του δικτύου δεδομένων	no : Αναθ		
Συντάκτης:	Έγκριση:			
ΣΚΟΠΟΣ:	Η πολιτική αποδεκτής χρήσης του δικτύου δεδομένων επιτρέπει και μη επιτρεπόμενες χρήσεις του δικτύου της Εταιρείας.			
ΠΕΡΙΓΡΑΦΗ:				
Πεδίο εφαρμογής				
Η πολιτική αποδεκτής χρήσης του δικτύου δεδομένων καλύπτει κάθε χρήση δεδομένων της Εταιρείας.				
Πολιτική				
Αποδεκτή χρήση				
<ul style="list-style-type: none">Η πρόσβαση στις υπηρεσίες της Εταιρείας μέσα από το δίκτυο επαγγελματικών σκοπούς της Εταιρείας.Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους, ηθικώς και του Συντάγματος.Η διασφάλιση του απόρρητου των επικοινωνιών και η προστασία των δεδομένων.Η άμεση ενημέρωση του υπεύθυνου ασφαλείας αν υποπέσει σε οποιοδήποτε κενό ασφαλείας				
Μη αποδεκτή χρήση				
<ul style="list-style-type: none">Επεμβάσεις στον μηχανογραφικό εξοπλισμό που αποτελεί το δίκτυο ή εισαγωγή εξοπλισμού στο δίκτυο.Ενέργειες που συνιστούν προσπάθεια παραβίασης (επιτυχής ή μη) συστημάτων μέσα από το δίκτυο δεδομένων της Εταιρείας. Σε εντάσσονται και ενέργειες που υποβαθμίζουν το επίπεδο συστήματος.				


Εμπιστευτικό

	Πολιτική Αποδεκτή χρήση σταθμών εργασίας	no : 4251 Αναθεώρηση: 00		
Συντάκτης:	Έγκριση:			
ΣΚΟΠΟΣ:	Η προστασία των σταθμών εργασίας της Εταιρείας			
ΠΕΡΙΓΡΑΦΗ:				
Πεδίο εφαρμογής				
Αυτή η πολιτική βρίσκεται εφαρμογή σε όλους τους σταθμούς εργασίας (desktop, laptops) για εντός ή εκτός του δικτύου της Εταιρείας. Κάθε υπάλληλος που χρειάζεται εξοπλισμό (desktop computer, laptop κ.τ.λ.) ορίζεται ως ιδιοκτήτης του και είναι υπεύθυνος για να εφαρμόσει τις οδηγίες που περιγράφονται στην πολιτική αυτή.				
Πολιτική				
Αποδεκτή χρήση				
<ul style="list-style-type: none">Το κλείσιμο του Η/Υ και του περιφερειακού εξοπλισμού μετά το πέρας της εργασίας του κάθε υπαλλήλου της Εταιρείας.Η ενεργοποίηση του screen saver υποχρεωτικά με χρήση συνθηματικού σε περίπτωση απομάκρυνσης του υπαλλήλου για αρκετό χρονικό διάστημα από τον Η/Υ.Ο τεμαχισμός των συνδέσεων όταν απομακρυνθείτε από τον Η/Υ ή όταν δεν είναι απαραίτητες.Η χρήση μόνο εξουσιοδοτημένου υλικού και λογισμικού.Η δημιουργία εφεδρικών αντιγράφων των αρχείων που έχετε αποθηκεύσει στον ηλεκτρονικό υπολογιστή σας.				
Μη αποδεκτή χρήση				
<ul style="list-style-type: none">Η εγκατάσταση παράνομου ή μη εξουσιοδοτημένου λογισμικού.Η απομακρυσμένη πρόσβαση στους σταθμούς εργασίας των χρηστών της Εταιρείας.Η παραμετροποίηση του δικτύου και του Internet Explorer από μη εξουσιοδοτημένο προσωπικό της Εταιρείας.Η απενεργοποίηση ή απεγκατάσταση του λογισμικού που έχει εγκατασταθεί από το εξουσιοδοτημένο προσωπικό της Εταιρείας.				


Εμπιστευτικό

Σελίδες 1/2

Έντυπα Διαχείρισης Ασφάλειας

	Πολιτική Εξωτερικοί συνεργάτες και πελάτες	ΠΟ : 424
Συντάκτης:	Έγκριση:	Ανοθεώ:
ΣΚΟΠΟΣ:	Η διασφάλιση των πληροφοριών και των πλήρως συστημάτων από την πρόσβαση, την επεξεργασία ή τη χρήση εξωτερικών συνεργάτες και πελάτες της Εταιρείας.	
ΠΕΡΙΓΡΑΦΗ:		
Πεδίο εφαρμογής		
Η πολιτική αυτή εφαρμόζεται για όλους τους εξωτερικούς συνεργάτες και πελάτες της Εταιρείας.		
Πολιτική		
Εμπιστευτικότητα		
<ul style="list-style-type: none">Οι εξωτερικοί συνεργάτες και οι πελάτες υπογράφουν σύμβαση εμπιστευτικού προστασία των πληροφοριών της Εταιρείας ή των πελατών της από μη εξουσιοδότηση.Η πρότυπη σύμβαση μεταξύ της Εταιρείας και των εξωτερικών συνεργατών ή ελέγχεται από τον νομικό σύμβουλο της Εταιρείας.Οι εξωτερικοί συνεργάτες λαμβάνουν όλα τα πιθανά προληπτικά μέτρα από την ώστε να διασφαλισθεί η εμπιστευτικότητα των πληροφοριών της Εταιρείας ή των πελατών.Το προσωπικό των συνεργατών που εργάζεται, προσωρινά ή μόνιμα, στις εγκαταστάσεις της Εταιρείας δεν αποκλύπτει καμία πληροφορία της Εταιρείας που έχει αποκλειστική παρουσία στην Εταιρεία.		
Ασφάλεια Πληροφοριών και Ενήμερωση		
<ul style="list-style-type: none">Το προσωπικό των εξωτερικών συνεργατών που εργάζεται για την Εταιρεία, ενημερώνεται υπεύθυνο ασφάλειας για την Πολιτική Ασφάλειας της Εταιρείας.Οι εξωτερικοί συνεργάτες που εργάζονται για την Εταιρεία, συμμορφώνονται με την Πολιτική Ασφάλειας.		
Συμμόρφωση με την Πολιτική Ασφάλειας		
Οι εξωτερικοί συνεργάτες και οι πελάτες έχουν πρόσβαση μόνο στις εφαρμογές, στις πληροφορίες συστημάτων και στα συστήματα για τις ανάγκες και τον σκοπό της για το χρονικό διάστημα που ορίζεται στην σύμβαση. Οποιαδήποτε κατάχρηση των πληροφοριών ή μη εξουσιοδοτημένη πρόσβαση σε άλλα συστήματα και δεδομένα χαρακτηρίζεται ως συμμόρφωση με την πολιτική ασφάλειας της Εταιρείας και επιφέρει τις νόμιμες συνέπειες.		

Εμπιστευτικό

	Έντυπο Παράδοση voucher για WIFI	
Συντάκτης: Καραγιάννη Α.Α.	Έγκριση: Τζωρτζής Γ.	
ΠΑΡΑΔΟΣΗ VOUCHER ΓΙΑ WIFI – IDIKA GU		
Στοιχεία χρήστη		
Όνοματεπώνυμο:	Ημερομηνία:	
ΑΔΤ/Διαβατηρίου:		
Εταιρεία/Τμήμα:	Τηλ.:	e-mail:
	Κιν:	
Συνθηματικό (Voucher):		
Σκοπός χρήσης:		
Παρατηρήσεις:		
<input type="checkbox"/> * Έχω λάβει γνώση και αποδέχομαι τους όρους χρήσης του ασύρματου δικτύου Η.Δ.Κ.Α. Α.Ε. που περιγράφονται στη επόμενη σελίδα.		
(*) Υπογραφή Χρήστη	Ημερομηνία Παράδοσης	Υπογραφή Διαχειριστή

Εμπιστευτικό




Εγχειρίδιο Βασικών Αρχών Ασφαλείας



ΜΗΝ ΞΕΧΝΑΙΕΤΕ ΠΟΤΕ ΤΙ ΠΡΟΣΤΑΤΕΥΟΥΜΕ

Προστατεύουμε πριν από όλα την προσωπική μας εργασία
Προστατεύουμε την ομαλή λειτουργία της εταιρείας.

Έντυπα Διαχείρισης Ασφάλειας

 ΗΔΙΚΑ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΧΕΙΡΙΣΤΙΚΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.	Έντυπο Δήλωση Υπεύθυνων Διαχείρισης Συστημάτων & Εφαρμογών	Σύντάκτης: Καραχάλιου Έγκριση: Τζωρτζή
--	---	---


Καταγραφή στοιχείων υπευθύνου			
Όνομα		Επώνυμο	
Δ/ση & Τμήμα			
Γραφείο		Τηλ.	

Καταγραφή Πληροφοριακού Συστήματος ή εφαρμογής	
Όνομασία	
Τύπος	
IP (για Π.Σ.) μήνυμα εγκατ./σης (για εφαρ.)	
Φυσική θέση	
Σκοπός λειτουργίας	
Ημ. Ανάληψης ευθύνης	
Αναπληρωτές υπεύθυνοι	

Καταγραφή Πληροφοριακού Συστήματος ή εφαρμογής	
Όνομασία	
Τύπος	
IP (για Π.Σ.) / μήνυμα εγκατ./σης (για εφαρ.)	
Φυσική θέση	
Σκοπός λειτουργίας	
Ημ. Ανάληψης ευθύνης	
Αναπληρωτές υπεύθυνοι	

Υπογραφή υπεύθυνου	Ημερομηνία

Εμπιστευτικό

 HΔΙΚΑ <small>ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΔΙΚΑΣΙΑ ΚΕΡΤΑΝΣΗΣ ΑΣΦΑΛΙΣΤΗ ΑΔ</small>	Έντυπο	EN : 4298
	Δήλωση νέου χρήστη	Αναθεώρηση
Συντάκτης: Καραχάλιου Αλ.	Έγκριση: Τζώρτζης Γ.	

ΔΗΛΩΣΗ ΝΕΟΥ ΧΡΗΣΤΗ		
Στοιχεία χρήστη		
Όνοματεπώνυμο:	Ημερομηνία:	
Τηλ.:	e-mail:	Τμήμα:

Όνομα χρήση:

Προσωρινός Κωδικός χρήστη:

E-mail:


Παρατηρήσεις

☐ Έχω λάβει γνώση και αποδέχομαι να τηρώ τους κανόνες Ασφαλείας που περιγράφονται εν συντομία στο Εγχειρίδιο Βασικών Αρχών Ασφαλείας της Η.Μ.Α.

Υπογραφή Χρήστη	Ημερομηνία	Υπογραφή Διαχειριστή	Ημερομηνία
-----------------	------------	----------------------	------------

Υπογραφή Χρήστη	Ημερομηνία	Υπογραφή Διαχειριστή	Ημερομηνία
-----------------	------------	----------------------	------------

Εμπιστευτικό

 ΗΔΙΚΑ <small>ΗΛΕΚΤΡΟΝΙΚΟ ΔΙΑΔΙΚΤΥΟ ΚΟΙΝΩΝΙΚΗΣ ΕΚΔΟΣΗΣ Α.Ε.</small>	Έντυπο Ρόλος των χρηστών	EN : 42112
	Συντάκτης:	Έγκριση:

[illegible]

Εμπιστευτικό

Σελίδα 1/1

ΤΕΧΝΙΚΑ ΜΕΤΡΑ

Αδιάλειπτη παροχή Δικτύων και Τηλεπικοινωνιών

- Πρόσφατη οπτική σύνδεση με το ΕΔΕΤ στα 10G - που μπορεί να προσφέρει εναλλακτική πρόσβαση σε Φορείς που ανήκουν σε αυτό το δίκτυο.
- Διπλές οπτικές συνδέσεις (διπλή όδευση / διπλή εισαγωγή) στα 1 Gbps στο Εθνικό Δίκτυο Δημόσιας Διοίκησης ΣΥΖΕΥΞΙΣ.
- Διπλός ενεργός εξοπλισμός ΣΥΖΕΥΞΙΣ και ΗΔΙΚΑ ΑΕ για υψηλή διαθεσιμότητα.
- Όλο το LAN της ΗΔΙΚΑ ΑΕ, βασίζεται σε 10 Gbps backbone με διπλά 10Gbit Uplinks στα περισσότερα RACKs με Servers.
- Το LAN της ΗΔΙΚΑ ΑΕ απομονώνεται από τα WANs Φορέων με διπλά FireWalls (σε διάταξη active/standby).
- Το LAN της ΗΔΙΚΑ ΑΕ απομονώνεται από το Δίκτυο ΣΥΖΕΥΞΙΣ & INTERNET με διπλά FireWalls (σε διάταξη active/standby).
- Όλες οι εξωτερικές συνδέσεις της ΗΔΙΚΑ ΑΕ ελέγχονται από διπλά IPS/IDS (σε διάταξη active/standby) .

Αδιάλειπτη παροχή Υπηρεσιών Πληροφοριακών Συστημάτων

- Τα περισσότερα Πληροφοριακά Συστήματα της ΗΔΙΚΑ ΑΕ (κυρίως τα ΠΣ ΕΣΠΑ) εφαρμόζουν τεχνολογίες Private Cloud (virtualization & clustering).
- Διαθέτουν δικά τους dedicated SAN storages & tape backup libraries
- Διαθέτουν διπλές δικτυακές οδεύσεις με το backbone core δίκτυο.
- Κάποια διαθέτουν δικές τους υποδομές εξοπλισμού ασφαλείας (FireWalls, IDS/IPS, Networks, Antivirus κλπ).
- Κάποια ΠΣ έχουν και αλλού σημείο παρουσίας Disaster Recovery Site

Υποδομές Ασφάλειας

- Διπλοί network Firewalls με πολλές DMZs
- Διπλά IDS/IPS
- Διπλοί Web Application Firewalls
- Mail Gateway (Virtual Appliance)
- Web Gateway (Virtual Appliance)
- Total Endpoint Protection/Antivirus
- Αυτόνομο Guests WiFi (Captive Portal)

Κανόνες Ασφάλειας

- Έλεγχος πρόσβασης χρηστών στα ΠΣ της ΗΔΙΚΑ ΑΕ με την χρήση MS Active Directory (με γνωστοποίηση & αποδοχή της ΠΑ).
- Σύνθετα passwords (ελάχιστου πλήθους χαρακτήρων).
- Αλλαγή των passwords σε τακτά χρονικά διαστήματα.
- Κλείδωμα password σε αριθμό ανεπιτυχών προσπαθειών.
- Όλη η κίνηση προς το Internet γίνεται μέσω Web Proxy (με ελεγχόμενους κανόνες).
- Όλη η εξωτερική διακίνηση emails γίνεται μέσω Mail Gateway, και ελεγχόμενους κανόνες από Mail Security Software (transport layer).
- Endpoint Protection (Virus & Spyware protection, Proactive Threat protection, Network & Host Exploit Mitigation).
- Κρυπτογραφημένη ανταλλαγή αρχείων με Φορείς-SFTP Server
- Αυτόνομο Guests WiFi (Captive Portal) για επισκέπτες.

Ασφάλεια Δεδομένων

- Τα περισσότερα ΠΣ (κυρίως τα ΕΣΠΑ) της ΗΔΙΚΑ ΑΕ αποτελούν ανεξάρτητες νησίδες με ελεγχόμενους κανόνες διαλειτουργικότητας με άλλα ΠΣ (web services/APIs)
 - Διαθέτουν δικό τους tape backup library και ορισμένα έχουν ενεργοποιημένη κρυπτογράφηση δεδομένων.
 - Οι περισσότερες βάσεις δεδομένων (DBs) έχουν ήδη ενεργοποιημένη την δυνατότητα κρυπτογράφησης δεδομένων (Advanced Security Option).
 - Στις περισσότερες βάσεις δεδομένων (DBs) υπάρχει η δυνατότητα ενεργοποίησης του option Data Masking (αλλά χρειάζεται η προμήθεια της σχετικής άδειας ενεργοποίησης).
 - Σε όλες τις βάσεις δεδομένων γίνεται καταγραφή πρόσβασης των χρηστών διαχείρισης και λειτουργίας (DBs).
- Δεδομένα σε άλλη μορφή (π.χ. έντυπη) φυλάσσονται σε ελεγχόμενους χώρους.

ΣΥΛΛΟΓΗ ΠΕΙΣΤΗΡΙΩΝ

Καταγραφή logs

- Όλες οι συσκευές ασφαλείας (FWs, IDS/IPS, κλπ) στέλνουν logs συμβάντων σε κεντρικό Σύστημα Syslog Server και σε SIEM.
- Όλοι οι servers ΠΣ στέλνουν logs συμβάντων σε κεντρικό Σύστημα Syslog Server (μερικοί και σε SIEM)
- Όλες οι δικτυακές συσκευές στέλνουν logs σε NMS (μερικές και σε SIEM).
- Όλοι οι WAFs κρατούν τα logs τοπικά και τα στέλνουν και σε κεντρικό Σύστημα Syslog Server (μερικοί και σε SIEM).
- Το SIEM παρακολουθείται 24x7 από συμβεβλημένο SOC (με σχετική Σύμβαση).

ΤΙ ΕΙΝΑΙ Ο (ΕΕ) 2016/679 – GDPR

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΤΙ ΧΡΕΙΑΖΕΤΑΙ Ο GDPR;

- Διοικητικά μέτρα
- Οργανωτικά μέτρα
- Τεχνικά μέτρα
- Λογοδοσία
 - Αρμόδιες Αρχές Προστασίας Δεδομένων
 - Υποκείμενα των Δεδομένων
 - Χρονικούς περιορισμούς ειδοποίησης παραβίαση

ΤΙ ΘΕΛΕΙ Ο GDPR;

- Νόμιμη Επεξεργασία
- Προσδιορισμός του σκοπού
- Ελαχιστοποίηση Δεδομένων
- Σχετικότητα Δεδομένων
- Ακρίβεια Δεδομένων
- Περιορισμένη Διατήρηση Δεδομένων
- Θεμιτή Επεξεργασία

Συναφή έργα σε εξέλιξη

- Υπάρχει ήδη σε εξέλιξη το έργο της «Αναδιοργάνωσης της ΗΔΙΚΑ ΑΕ» που περιλαμβάνει:
 1. Το νέο οργανόγραμμα της ΗΔΙΚΑ ΑΕ με πρόταση του αναδόχου για:
 - δημιουργία «Ανεξάρτητου Γραφείου Ασφάλειας Πληροφοριακών Συστημάτων», που θα λογοδοτεί στο Γραφείο Διοίκησης (Διευθύνων Σύμβουλο)
 - δημιουργία «Ανεξάρτητου Γραφείου Ασφάλειας Δεδομένων» (DPO), που θα λογοδοτεί στο Διοικητικό Συμβούλιο της ΗΔΙΚΑ ΑΕ
 2. Την πιστοποίηση της ΗΔΙΚΑ ΑΕ με ISO-27001, ISO-20000, και ISO-9001

Επόμενα έργα

Υπάρχει σε εξέλιξη διαδικασία προκήρυξης έργου με τίτλο «Παροχή υπηρεσιών τεχνικής υποστήριξης της ΗΔΙΚΑ ΑΕ από εξωτερικό ανάδοχο για το Σχεδιασμό Προγράμματος Συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR - 2016/679) της ΕΕ»

Φυσικό αντικείμενο του έργου θα είναι:

- ΦΑΣΗ Α: Καταγραφή και χαρτογράφηση των προσωπικών δεδομένων
- ΦΑΣΗ Β: Διενέργεια «Εκτίμησης Αντικτύπου» σχετικά με την «Προστασία Δεδομένων» (DPIA)
- ΦΑΣΗ Γ: Μελέτη αποτίμησης αποκλίσεων (Gap analysis)
- ΦΑΣΗ Δ: Σχεδιασμός προγράμματος συμμόρφωσης (Compliance plan)

Δημιουργία & Τήρηση Μητρώου Προσωπικών Δεδομένων

- Συλλογή στοιχείων από το Γραφείο Προστασίας Δεδομένων
- Εντοπισμός όλων των τύπων δεδομένων
- Καταγραφή όλων των ειδών δεδομένων
- Καθιέρωση μιας διαδικασίας συντήρησης του Μητρώου Προσωπικών Δεδομένων

Ενημέρωση Προσωπικού- Εκπαιδεύσεις

- Έχουν ήδη γίνει κάποιες εκπαιδεύσεις προσωπικού σε θέματα:
 - GDPR,
 - DPO, και
 - Συμμετοχή υπαλλήλων στο «Καινοτόμο Εργαστήριο για τον ΓΚΠΔ» του ΕΚΔΔΑ
- Δρομολογείται Ενημέρωση όλου του Προσωπικού
 - Για δημιουργία κουλτούρας Προστασίας Δεδομένων

Προκλήσεις

- Να δοθούν κεντρικές κατευθυντήριες γραμμές από τους αρμόδιους θεσμοθετημένους Φορείς στους Φορείς εφαρμογής του GDPR (όλο το Δημόσιο)
- Ουσιαστική υποστήριξη των Διοικήσεων των Φορέων στους υπαλλήλους που θα ορίσουν DPO
- Να ξεκαθαρίσει το τοπίο στις Νομικές ευθύνες των υπαλλήλων DPO των Φορέων



59 ΜΕΡΕΣ ΠΡΙΝ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ GDPR ΤΕΛΙΚΑ ΠΟΣΟ ΕΤΟΙΜΟΙ ΕΙΜΑΣΤΕ;

Ευχαριστώ για την προσοχή σας!

Γεώργιος Τζώρτζης
Μηχανικός Η/Υ Συστημάτων
MSc Data Communication Systems