ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΓΡΑΜΜΑΤΕΙΑ ΣΥΓΚΛΗΤΟΥ
Διεύθυνση: Ερυθρού Σταυρού 28 & Καρυωτάκη, 22131 Τρίπολη
Τηλ.:2710-230000

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ ΣΥΓΚΛΗΤΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΛΟΠΟΝΝΗΣΟΥ
Απόφαση 40 /07.06.2021 Συνεδρίαση 192η

Θέμα: Έγκριση Εσωτερικού Κανονισμού Λειτουργίας και Πολιτική Ασφαλείας Δικτύου

Η ΣΥΓΚΛΗΤΟΣ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΛΟΠΟΝΝΗΣΟΥ

Έχοντας υπόψη:

Την απόφαση του Πρυτανικού Συμβουλίου επί της έγκριση Εσωτερικού Κανονισμού Λειτουργίας και Πολιτική Ασφαλείας Δικτύου του Πανεπιστημίου Πελοποννήσου (Απόφαση 4/18.03.2021, 64η συνεδρίαση)

Εγκρίνει

Τον Εσωτερικό Κανονισμό Λειτουργίας και Πολιτική Ασφαλείας Δικτύου, σύμφωνα με την απόφαση 4/18.03.2021 της 64ης Συνεδρίασης του Πρυτανικού Συμβουλίου του Πανεπιστημίου Πελοποννήσου.
Η απόφαση 4/18.03.2021 της 64ης συνεδρίασης του Πρυτανικού Συμβουλίου του Πανεπιστημίου Πελοποννήσου, επί της 4ης έγκριση Εσωτερικού Κανονισμού Λειτουργίας και Πολιτική Ασφαλείας Δικτύου του Πανεπιστημίου Πελοποννήσου επισυνάπτεται στο Παράρτημα της παρούσας απόφασης, της οποίας αποτελεί αναπόσπαστο μέρος.

Ο Πρύτανης

Καθηγητής Αθανάσιος Κατσής

ΠΑΡΑΡΤΗΜΑ

Απόφασης 3 /07-06-2021, 192η συνεδρίαση Συγκλήτου

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΓΡΑΜΜΑΤΕΙΑ ΠΡΥΤΑΝΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ
Διεύθυνση: Ερυθρού Σταυρού 28 & Καρυωτάκη, 22100 Τρίπολη
Τηλ.:2710-230009
Πληροφορίες: κ. Μαρία Χριστοδημητροπούλου, mchristo@uop.gr

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ ΠΡΥΤΑΝΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΛΟΠΟΝΝΗΣΟΥ
Απόφαση 4/18.03.2021 Συνεδρίαση 64η

Θέμα Έγκριση Εσωτερικού Κανονισμού Λειτουργίας και Πολιτική Ασφαλείας Δικτύου

ΤΟ ΠΡΥΤΑΝΙΚΟ ΣΥΜΒΟΥΛΙΟ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΛΟΠΟΝΝΗΣΟΥ

Έχοντας υπόψη:

1. Τις διατάξεις του Π.Δ. 13/2000 Ίδρυση Πανεπιστημίου Πελοποννήσου (ΦΕΚ 12/Α΄/1-2-2000) όπως ισχύει,
2. Τις διατάξεις του Ν. 4610/2019 (ΦΕΚ 70/Α') «Συνέργειες Πανεπιστημίων και Τ.Ε.Ι., πρόσβαση στην τριτοβάθμια εκπαίδευση, πειραματικά σχολεία, Γενικά Αρχεία του Κράτους και λοιπές διατάξεις»,
3. Τον προτεινόμενο Εσωτερικό Κανονισμό Λειτουργίας και Πολιτική Ασφαλείας Δικτύου
4. Την προφορική εισήγηση του Αντιπρύτανη Οικονομικών, Προγραμματισμού και Ανάπτυξης
5. Τη διεξαχθείσα συζήτηση κατά την 64η συνεδρίαση του Πρυτανικού Συμβουλίου (18-03-2020)

Εγκρίνει

Τον Εσωτερικό Κανονισμό Λειτουργίας και Πολιτική Ασφαλείας Δικτύου του Πανεπιστημίου Πελοποννήσου, το οποίο επισυνάπτεται ως Παράρτημα της παρούσας απόφασης, της οποίας αποτελεί αναπόσπαστο μέρος.

Ο Πρύτανης

Καθηγητής Αθανάσιος Κατσής

Παράρτημα Απόφασης 4/18-03-2021, 64η Συνεδρίαση

Πανεπιστήμιο Πελοποννήσου

Διεύθυνση Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Εσωτερικός Κανονισμός Λειτουργίας και Πολιτική Ασφαλείας Δικτύου

Πίνακας περιεχομένων

1. Κανονισμός Λειτουργίας Δικτύου Δεδομένων

1.1. Εισαγωγή

Το Πανεπιστήμιο Πελοποννήσου (ΠΑΠΕΛ) ιδρύθηκε το 2000 και άρχισε να λειτουργεί το 2002 με έδρα την Τρίπολη. Δραστηριοποιείται στις 5 πρωτεύουσες των Νομών της Περιφέρειας Πελοποννήσου (Τρίπολη, Κόρινθος, Ναύπλιο, Σπάρτη, Καλαμάτα) και στην Πάτρα. Το όραμα και η αποστολή του ΠΑΠΕΛ συνοψίζονται στα παρακάτω σημεία:

Ενίσχυση της επιστημονικής έρευνας και της παραγωγής νέας γνώσης
Αναβάθμιση της εκπαιδευτικής διαδικασίας και των προγραμμάτων σπουδών
Παροχή ενισχυτικών υπηρεσιών στους φοιτητές αλλά και στους απόφοιτους
Ανάπτυξη της εξωστρέφειας και της διεθνοποίησης του Πανεπιστημίου
Υποστήριξη όλων των αναπτυξιακών πρωτοβουλιών σε περιφερειακό και εθνικό επίπεδο
Σύνδεση του Πανεπιστημίου με την τοπική κοινωνία και ουσιαστική συμβολή στην κοινωνική συνοχή
Στήριξη των φοιτητών στην αναζήτηση ποιοτικών επαγγελματικών διεξόδων
Δημιουργία κουλτούρας γόνιμου διαλόγου και σεβασμού στη διαφορετικότητα σε όλη την ακαδημαϊκή κοινότητα
Ενσωμάτωση των Τεχνολογιών Πληροφορίας και Επικοινωνίας
Συμπαράσταση σε όλες τις Ευαίσθητες Κοινωνικά Ομάδες

Για τους παραπάνω λόγους το ΠΑΠΕΛ έχει δημιουργήσει, συντηρεί και συνεχώς εξελίσσει ένα Δίκτυο Δεδομένων υψηλών ταχυτήτων που καλύπτει όλα τα σημεία παρουσίας του. Μέσω του Δικτύου αυτού, κάθε τμήμα του, συνδέεται με ελληνικά και διεθνή δίκτυα, και το Διαδίκτυο (Internet). Η υποδομή, οι υπηρεσίες και η αναπτυσσόμενη τεχνογνωσία γύρω από τα δίκτυα, χρησιμοποιούνται για την εξυπηρέτηση και προαγωγή της εκπαίδευσης, της έρευνας και της διοίκησης όλων των ερευνητικών ιδρυμάτων.

Στόχος του κάθε ιδρύματος θα πρέπει να είναι η αδιάλειπτη παροχή υπηρεσιών υψηλής ποιότητας προς την πανεπιστημιακή κοινότητα, και η εισαγωγή και εξοικείωση των μελών της με τεχνολογίες αιχμής στο χώρο της Πληροφορικής και των Τηλεπικοινωνιών. Με σκοπό την επίτευξη των στόχων αυτών και σύμφωνα με το άρθρο 51 του ν. 4623/2019, σε κάθε φορέα που παρέχει υπηρεσίες πληροφορικής και επικοινωνιών, συνιστάται ενιαία διοικητική **Μονάδα Ηλεκτρονικής Διακυβέρνησης (ΜΗΔ)** σε επίπεδο Τμήματος ή Διεύθυνσης. Στη μονάδα αυτή υπάγονται όλες οι υφιστάμενες οργανικές μονάδες του φορέα με αρμοδιότητες σχετικές με τις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ), την απλούστευση των διαδικασιών και γενικότερα την υλοποίηση δράσεων ηλεκτρονικής διακυβέρνησης, σύμφωνα με τις αρχές, το πλαίσιο και τις κατευθύνσεις της Βίβλου Ψηφιακού Μετασχηματισμού. Στην περίπτωση του ΠΑΠΕΛ, αυτή η μονάδα ονομάζεται Διεύθυνση Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (ΔΥΗΔ). Έτσι, η ΔΥΗΔ θα πρέπει να αναλάβει τον καθορισμό και την υλοποίηση των απαραίτητων τεχνικών και κανονιστικών διαδικασιών και τον συντονισμό όλων των επιμέρους ομάδων χρηστών της. Σε αυτό το πλαίσιο, ο παρών κανονισμός έχει σκοπό να οριοθετήσει το θεσμικό και κανονιστικό πλαίσιο λειτουργίας των δικτυωμένων υποδομών του ιδρύματος.

Ακολουθούν χρήσιμοι ορισμοί:

Δίκτυο Δεδομένων ονομάζεται το σύνολο των δικτυακών υπηρεσιών και υποδομών που υποστηρίζουν τις απαιτήσεις επικοινωνίας των υπολογιστικών συστημάτων του κάθε ιδρύματος.

Διεύθυνση Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (ΔΥΗΔ) ονομάζεται ο φορέας που προτείνει, υλοποιεί και παρακολουθεί σε τεχνικό επίπεδο την πολιτική σε θέματα ΤΠΕ που χαράσσει το κάθε ίδρυμα, καθώς και τις δράσεις ψηφιακού μετασχηματισμού.

Χρήστης (δικτύου) ονομάζεται η ακαδημαϊκή μονάδα του ιδρύματος (Σχολή, Τμήμα, Επιτροπή κτλ) ή το νομικό πρόσωπο (διασυνδεδεμένος φορέας) ή το φυσικό πρόσωπο (μέλος του ιδρύματος ή διασυνδεδεμένου φορέα), στο οποίο παρέχονται υπηρεσίες. Ως φυσικό πρόσωπο «χρήστης» νοείται οποιοσδήποτε στον οποίο παρέχονται υπηρεσίες από την ΔΥΗΔ (π.χ. υπηρεσία e-mail). Επίσης «χρήστης» μπορεί να είναι ένα μηχάνημα το οποίο μπορούν να χρησιμοποιούν ένα ή περισσότερα φυσικά πρόσωπα, και το οποίο είναι φυσικά διασυνδεδεμένο με τον εξοπλισμό της ΔΥΗΔ. Επειδή όμως για κάθε διασυνδεδεμένο μηχάνημα υπάρχει κάποιος υπόλογος, οι κανονισμοί αφορούν και όλα τα φυσικά πρόσωπα που έχουν πρόσβαση στο Δίκτυο.

Ομάδα Διερεύνησης Περιστατικών Παραβίασης Ασφαλείας (ΟΔΕ) ονομάζεται η ομάδα, η οποία απαρτίζεται από όργανα επί θητεία, τα οποία έχουν την ευθύνη διερεύνησης περιστατικών παραβίασης ασφαλείας που αφορούν το Δίκτυο Δεδομένων του ιδρύματος.

Ο παρών Κανονισμός Λειτουργίας εφαρμόζεται σε όλες τις κατηγορίες χρηστών του δικτύου. Η συμμόρφωση των μελών κάθε διασυνδεδεμένου φορέα με τον παρόντα Κανονισμό αποτελεί ευθύνη του κάθε μέλους προσωπικά καθώς και του ίδιου του φορέα.

1.2. Δραστηριότητες Διεύθυνσης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Ενδεικτικά, οι δραστηριότητες της ΔΥΗΔ μπορούν να καταταχθούν στις παρακάτω κατηγορίες:

Εγκατάσταση νέων τμημάτων καλωδιακού συστήματος, ενεργών στοιχείων και λογισμικού συστημάτων δικτύου και εφαρμογών. Όσον αφορά στο κομμάτι του καλωδιακού συστήματος, οι επεμβάσεις αφορούν την ενσωμάτωση νέων τμημάτων του δικτύου στο ήδη υπάρχον. Η εγκατάσταση των νέων ενεργών στοιχείων που συχνά προμηθεύεται το ίδρυμα, σχεδιάζεται, επιβλέπεται ή/και εκτελείται από τη ΔΥΗΔ, ανάλογα με τις επιμέρους απαιτήσεις και την υπάρχουσα τεχνογνωσία του αναδόχου. Παρομοίως, όσον αφορά στο λογισμικό συστημάτων δικτύου και εφαρμογών, η παραγωγή προστιθέμενης αξίας από την ίδια τη ΔΥΗΔ είναι βασική πολιτική επιλογή, η οποία ενισχύει την αυτοτέλεια και μειώνει τις δαπάνες του ιδρύματος.

Συντήρηση ενεργών στοιχείων, καλωδιακού συστήματος και λογισμικού. Η ΔΥΗΔ μεριμνά για την καλή κατάσταση και την ικανοποιητική απόδοση του δικτύου με περιοδικές επισκέψεις των στελεχών της στα κομβικά σημεία του δικτύου, κατά τη διάρκεια των οποίων πραγματοποιούνται συντηρήσεις ή/και αναβαθμίσεις. Επίσης, σε περιπτώσεις όπου η συντήρηση των ενεργών στοιχείων έχει ανατεθεί σε εξωτερικούς εργολάβους, τότε η ΔΥΗΔ πρέπει να επιβλέπει και να πιστοποιεί την καλή εκτέλεση της, καθώς και να φροντίζει για την έγκαιρη προμήθεια ανταλλακτικών και τη διεξαγωγή επιδιορθώσεων, στις περιπτώσεις που δεν υπάρχει συμβόλαιο συντήρησης. Τέλος, το λογισμικό είναι ένας τομέας που απαιτεί μεγάλες και επίπονες προσπάθειες συντήρησης, καθώς υπάρχει συχνά ανάγκη για αναβάθμιση του συνόλου ή κάποιων τμημάτων των εξειδικευμένων προγραμμάτων, τα οποία επιπλέον μπορεί να έχουν διαμορφωθεί ειδικά για τις ανάγκες του ιδρύματος. Είναι απαραίτητο πάντα να υπάρχει εύστοχος και έγκαιρος προγραμματισμός αγοράς νέων

εκδόσεων προϊόντων λογισμικού και το συνήθως δωρεάν διαθέσιμο λογισμικό θα πρέπει να μεταφερθεί από το προσεκτικά επιλεγμένο και κατάλληλο σημείο του Internet, πάντα υπό την επίβλεψη των τεχνικών της ΔΥΗΔ.

Διαχείριση ενεργών στοιχείων, καλωδιακών κόμβων και εφαρμογών. Σε ένα δίκτυο απαιτείται μια ολοκληρωμένη χαρτογράφηση, καταγραφή και διαχείριση του καλωδιακού συστήματος, ώστε να εξασφαλίζεται η απρόσκοπτη καθημερινή λειτουργία και οι σωστές μικρο-προσαρμογές του δικτύου, η έγκαιρη διάγνωση βλαβών και ο εύστοχος σχεδιασμός επεκτάσεων. Ιδιαίτερα κρίσιμος παράγοντας για την αποδοτική λειτουργία του δικτύου είναι η σωστή διαμόρφωση και παρακολούθηση των συνθηκών λειτουργίας (φόρτος, στατιστικά στοιχεία, βλάβες) των ενεργών στοιχείων και των βασικών υπολογιστών παροχής δικτυακών εφαρμογών, μέσα από μια πλατφόρμα διαχείρισης βασισμένη στο ανοικτά διεθνή πρότυπα (π.χ. SNMP). Στα προηγούμενα εντάσσεται και η δυνατότητα των χρηστών που αντιμετωπίζουν δικτυακά προβλήματα να ζητήσουν επίσκεψη τεχνικού της ΔΥΗΔ (ή εξωτερικού συνεργάτη σε συνεννόηση με τη ΔΥΗΔ).

Εκπαίδευση και τεχνική υποστήριξη των μελών και των υπολογιστών του ιδρύματος. Ειδικότερα, η εκπαίδευση μπορεί να αφορά τη χρήση του Δικτύου Δεδομένων και των προσφερόμενων υπηρεσιών του ιδρύματος, καθώς και δράσεις για την ενημέρωση-ευαισθητοποίηση των χρηστών για θέματα κυβερνοασφάλειας (Cybersecurity) [13].

Παροχή δικτυακών υπηρεσιών προστιθέμενης αξίας στο φορέα και στην ευρύτερη ακαδημαϊκή κοινότητα. Ενδεικτικά αναφέρονται οι παρακάτω υπηρεσίες:

Ηλεκτρονικό Ταχυδρομείο (e-mail) και ηλεκτρονικό ταχυδρομείο μέσω διαδικτύου (webmail)
Υπηρεσίες Παγκόσμιου Ιστού (www)
Μεταφορά Αρχείων (FTP)
Διευθυνσιοδότηση Υπολογιστών (DNS)
Υπηρεσίες Καταλόγου (LDAP)
Μηχανές Αναζήτησης Πληροφοριών Ιστού (Search Engines)
Λογισμικό ασφαλείας – Firewall, IDS, IPS, Antivirus κλπ.

Ανάπτυξη νέων προηγμένων υπηρεσιών δικτύου και ενσωμάτωση τους στο περιβάλλον του δικτύου σε πλήρη κλίμακα.

Επίσης, η ΔΥΗΔ θα μπορούσε να αναλάβει, στα πλαίσια χρηματοδοτούμενων ερευνητικών προγραμμάτων, την παροχή υπηρεσιών και τεχνογνωσίας προς τρίτους (Ερευνητικούς και Ακαδημαϊκούς Φορείς, Δημόσιες Υπηρεσίες κτλ.) στα γνωστικά αντικείμενά «μελέτη, σχεδιασμός και διαχείριση δικτύων», «ανάπτυξη, διαχείριση και υποστήριξη ηλεκτρονικών υπηρεσιών και εφαρμογών», καθώς και σε άμεσα συναφή γνωστικά αντικείμενα, εφόσον καλύπτει πλήρως τις υποχρεώσεις παροχής υπηρεσιών που έχει προς την ακαδημαϊκή κοινότητα του ιδρύματος.

1.3. Περιορισμοί Ευθύνης

Η χρήση λογισμικού, εξοπλισμού, υπολογιστικών πηγών και τεκμηρίωσης είναι προνόμιο το οποίο παραχωρείται χωρίς χρέωση στους καθηγητές, τους φοιτητές και το προσωπικό του ΠΑΠΕΛ. Με ευθύνη και άδεια των νομίμων οργάνων του ιδρύματος, το παραπάνω προνόμιο επεκτείνεται και προς επιλεγμένους επισκέπτες ή άλλους συνεργάτες του. Η χρήση του δικτύου του ιδρύματος παραχωρείται για συγκεκριμένους σκοπούς, σύμφωνα με τις αρχές που διέπουν τη λειτουργία του και σε καμία περίπτωση δεν συνιστούν αυτονόητο δικαίωμα.

Το ίδρυμα επιφυλάσσεται για κάθε νόμιμο δικαίωμα του, και ρητά δηλώνει εκ των προτέρων στους χρήστες του Δικτύου Δεδομένων του, τους παρακάτω περιορισμούς ευθύνης:

1. Το ίδρυμα αποποιείται κάθε ευθύνη για οποιαδήποτε ζημία ή απώλεια δεδομένων προκύπτει άμεσα ή έμμεσα από τη χρήση είτε του Δικτύου Δεδομένων του, είτε γενικώς εξοπλισμού του.

Το ίδρυμα θα πρέπει να μεριμνά ώστε να κρατούνται αντίγραφα των δεδομένων που αποθηκεύονται στα συστήματα του, σε τακτά χρονικά διαστήματα. Όμως, από αυτό το γεγονός, δεν προκύπτει εγγύηση ότι τυχόν απολεσθέντα δεδομένα θα αποκατασταθούν. **Σημείωση:** πρόσβαση στα αντίγραφα των δεδομένων που έχουν κρατηθεί, παρέχεται αποκλειστικά και μόνο στους νόμιμους κατόχους των αρχικών δεδομένων.

Στόχος του ιδρύματος είναι η βέλτιστη αξιοποίηση των πόρων του Δικτύου και των συστημάτων του, χωρίς δύσχρηστες διαδικασίες και χρονοβόρους περιορισμούς. Το επίπεδο είναι ανάλογο ενός ανοικτού, ακαδημαϊκού περιβάλλοντος, στο οποίο λαμβάνεται μέριμνα για παροχή ικανοποιητικού επιπέδου ασφαλείας προς τους χρήστες. Παρόλα αυτά, όπως και σε κάθε ανοικτό δίκτυο, η πιθανότητα παραβιάσεων ασφαλείας δεν μπορεί να αποκλειστεί εντελώς. Συνεπώς το ίδρυμα, στον βαθμό και την έκταση που επιτρέπεται από τη νομοθεσία, αποποιείται κάθε ευθύνης για οποιαδήποτε παραβίαση ιδιωτικού απόρρητου, κλοπή πληροφοριών, αλλοίωση ή απώλεια δεδομένων, και γενικά κάθε βλάβη που προκύπτει άμεσα ή έμμεσα εξαιτίας της έλλειψης ή δυσλειτουργίας των μηχανισμών ασφαλείας του.

Λόγω της φύσης του δικτυακού πρωτοκόλλου IP, το ίδρυμα δεν μπορεί να εγγυηθεί για την εύρυθμη λειτουργία όλων των υπηρεσιών σε κάθε χρονική στιγμή. Η ποιότητα υπηρεσιών μπορεί να μεταβάλλεται ανάλογα με διάφορους εσωτερικούς παράγοντες (πλήθος ενεργών χρηστών, είδος εργασιών χρηστών, υπάρχων δικτυακός εξοπλισμός, κ.ά.) αλλά και από εξωτερικούς παράγοντες (διαθεσιμότητα και φόρτος δικτύου ΕΔΥΤΕ, κ.ά.).

Απόψεις που εκφράζονται, ή κείμενα που δημοσιεύονται (εσωτερικά στο ΠΑΠΕΛ ή και σε ολόκληρο το Internet) μέσω του Δικτύου Δεδομένων του ιδρύματος από οποιονδήποτε χρήστη, δεν είναι κατ' ανάγκη επίσημες απόψεις του ιδρύματος, ούτε το δεσμεύουν με οποιονδήποτε τρόπο από μόνα τους. Οι απόψεις και τα κείμενα των χρηστών θα πρέπει να θεωρούνται προσωπικά, και το ίδρυμα δεν ευθύνεται για το περιεχόμενο τους, δεν έχει την τεχνική δυνατότητα να τα ελέγχει, αλλά ούτε και τη βούληση να επιβάλλει λογοκρισία.

Επειδή το ίδρυμα, είναι συμμορφούμενο σύμφωνα με την Ευρωπαϊκή Οδηγία 679/2016 και με την Εθνική Νομοθεσία ν.4624/2019 για την προστασία δεδομένων προσωπικού χαρακτήρα, δεν ελέγχει κατά κανένα τρόπο το περιεχόμενο της διακινούμενης και αποθηκευμένης πληροφορίας, αποποιείται κάθε ευθύνη για ενδεχόμενη διακίνηση πάνω στο δίκτυό του, προϊόντων, υπηρεσιών, περιεχομένου ή μέσων των οποίων η κατοχή ή διακίνηση συνιστούν παραβίαση της νομοθεσίας περί διανοητικής ιδιοκτησίας ή άλλο αδίκημα.

1.4. Δικαιώματα και υποχρεώσεις χρηστών

Η πρόσβαση των χρηστών στο Δίκτυο Δεδομένων και στα υπολογιστικά συστήματα του ιδρύματος, διέπεται από τους παρακάτω κανόνες:

1. Κάθε πρίζα του Δικτύου Δεδομένων ενεργοποιείται μετά από αίτηση του υπευθύνου προσωπικού για το συγκεκριμένο χώρο όπου βρίσκεται η πρίζα. Η IP διεύθυνση κάθε δικτυωμένου υπολογιστή (με συγκεκριμένη MAC διεύθυνση) παρέχεται από τη ΔΥΗΔ.

Κανένας χρήστης δεν έχει δικαίωμα αλλαγής IP διεύθυνσης υπολογιστή, κάρτας δικτύου, ή πρίζας χωρίς την πρότερη έγκριση της ΔΥΗΔ.

Κάθε χρήστης είναι υπεύθυνος και υπόλογος για κάθε είδους δραστηριότητα η οποία ξεκινάει ή αναπτύσσεται μέσω της πρίζας δεδομένων, του προσωπικού υπολογιστή, ή του λογαριασμού που του έχει παραχωρηθεί.

Όσον αφορά υπολογιστές που εξυπηρετούν πολλούς χρήστες ή πρίζες που παρέχουν πρόσβαση σε πολλούς υπολογιστές (πχ νησίδες, εργαστήρια), εκτός από τον χρήστη, συνυπεύθυνοι είναι και οι αντίστοιχοι τεχνικοί υπεύθυνοι του εργαστηρίου ή υπολογιστή.

Κάθε χρήστης είναι αποκλειστικά υπεύθυνος για τη σωστή λειτουργία του προσωπικού υπολογιστή του, όσον αφορά τη σύνδεση με το Δίκτυο Δεδομένων και τυχόν προβλήματα που μπορεί να προκαλέσουν στο Δίκτυο ελαττωματικά καλώδια, κάρτες δικτύου ή λογισμικό. Η ΔΥΗΔ και οι κατά τόπους υπεύθυνοι του ιδρύματος, παρέχουν τεχνικές συμβουλές και συστάσεις με τις οποίες οι χρήστες υποχρεούνται να συμμορφώνονται.

Για κάθε υπολογιστή ή λοιπό εξοπλισμό του ιδρύματος, υπάρχει τουλάχιστον ένας διαχειριστής, ο οποίος είναι υπεύθυνος και υπόλογος για το λογισμικό που βρίσκεται εγκατεστημένο σε αυτόν.

Κάθε χρήστης είναι υπεύθυνος για την επιλογή και τη διαφύλαξη «ασφαλούς» συνθηματικού (password), το οποίο επιτρέπει την πρόσβαση στο λογαριασμό του. Τα συνθηματικά δεν πρέπει ποτέ να δίνονται σε τρίτους, να φυλάσσονται σε ηλεκτρονική μορφή ή να γράφονται σε χαρτί.

Ιδιαίτερη προσοχή πρέπει να δίνεται σε κακόβουλες προσπάθειες επικοινωνίας (μέσω ηλεκτρονικού ταχυδρομείου ή τηλεφώνου) από άτομα που ισχυρίζονται ότι είναι υπεύθυνοι συστημάτων και ζητούν να μάθουν συνθηματικά χρηστών. Οι πραγματικοί υπεύθυνοι συστημάτων ποτέ δεν θα ζητήσουν κάτι τέτοιο. Οι χρήστες πρέπει να απορρίπτουν τις τηλεφωνικές αυτές επικοινωνίες και να διαγράφουν τα αντίστοιχα μηνύματα ηλεκτρονικού ταχυδρομείου.

Σε κάθε σύστημα, παρέχονται ένα σύνολο από μηχανισμούς/εργαλεία που μπορούν να αξιοποιηθούν από τον κάθε χρήστη για την προστασία των δεδομένων του από λαθραία ανάγνωση ή αλλοίωση από τρίτους. Οι εξ ορισμού (ρυθμίσεις) παρέχουν ένα ικανοποιητικό επίπεδο ασφάλειας και ο χρήστης είναι υπεύθυνος για την αξιοποίηση του συνόλου ή μέρους των μηχανισμών και των εργαλείων για την επίτευξη του επιθυμητού επιπέδου προστασίας των δεδομένων του.

Οι χρήστες δεσμεύονται να μη προβούν σε ενέργειες που συνιστούν παραβίαση του προσωπικού απόρρητου και της ακεραιότητας των δεδομένων άλλων χρηστών (π.χ. υποκλοπή ή αλλοίωση αρχείων/μηνυμάτων) και του απορρήτου των επικοινωνιών μέσω του Δικτύου Δεδομένων του ιδρύματος (π.χ. υποκλοπή μεταδιδόμενων δεδομένων). Επίσης, οι χρήστες απαγορεύεται να προβαίνουν σε παράνομη επεξεργασία προσωπικών δεδομένων. Τέλος, οι χρήστες δεσμεύονται να αποκτούν πρόσβαση αποκλειστικά σε δεδομένα που αναφέρονται στους ίδιους ή είναι δημοσίως ανακοινώσιμα.

Κάθε χρήστης είναι υπεύθυνος να αναφέρει επώνυμα ή ανώνυμα, κάθε παραβίαση ή απόπειρα παραβίασης των κανόνων λειτουργίας και ασφάλειας, στους αντίστοιχους υπεύθυνους συστημάτων ή στη ΔΥΗΔ.

Είναι υποχρέωση του κάθε χρήστη να χειρίζεται και να χρησιμοποιεί οποιοιδήποτε εξοπλισμό συστημάτων ή δικτύου που ανήκει στον φορέα με προσοχή, ώστε να μην προκαλούνται ζημιές ή φθορές.

Τυχόν φθορές που σχετίζονται με τον εξοπλισμό, θα πρέπει να αναφέρονται το ταχύτερο στη ΔΥΗΔ (ή στα αντίστοιχα αρμόδια όργανα). Η ΔΥΗΔ διατηρεί το δικαίωμα να διερευνήσει τους λόγους της φθοράς και, εφ' όσον προκύψουν σχετικές ευθύνες, να καταλογίσει το κόστος της δαπάνης στον υπαίτιο.

Τέλος, κάθε χρήστης οφείλει να σέβεται και να μην παρενοχλεί τους υπόλοιπους χρήστες, να μην σπαταλά άσκοπα πόρους και να μην προβαίνει σε πράξεις που παραβιάζουν τον νόμο, τους κανονισμούς και τη δεοντολογία του ιδρύματος, χρησιμοποιώντας τα συστήματα και το Δίκτυο Δεδομένων του.

Επίσης, οι χρήστες των υπηρεσιών του ιδρύματος οφείλουν να τηρούν τους γραπτούς και άγραφους – εθιμικούς κανόνες (πχ Netiquette RFC 1855 [14][15]) που διέπουν τη χρήση του Διαδικτύου και γενικότερα των δικτύων τηλεφωνίας και υπολογιστών. Έτσι, διαμέσου του Δικτύου Δεδομένων του ιδρύματος δεν επιτρέπεται μεταξύ άλλων:

Η προσπάθεια παραβίασης (επιτυχής ή όχι) της ασφάλειας (security) υπολογιστικών συστημάτων (του ιδρύματος ή οποιουδήποτε αλλού), είτε αυτή η προσπάθεια συνδέεται είτε δεν συνδέεται με απώλεια δεδομένων.
Η προσπάθεια παραβίασης (επιτυχής ή όχι) του προσωπικού απόρρητου χρηστών.
Η επίθεση (επιτυχής ή όχι) προς υπολογιστικά συστήματα, με σκοπό την άρνηση παροχής υπηρεσίας (Denial of Service - DoS attack) [12].
Η υπερφόρτωση και η μη λελογισμένη χρήση των υπολογιστικών και δικτυακών πόρων του ιδρύματος.
Η αποστολή μαζικού ηλεκτρονικού ταχυδρομείου χωρίς κάτι τέτοιο να ζητηθεί από τους παραλήπτες (spamming).
Η χρήση των δικτυακών πόρων και των υπολογιστικών συστημάτων με τρόπο που δημιουργεί κίνδυνο για την εθνική ασφάλεια και τις σχέσεις της χώρας με τρίτες χώρες.
Η χρήση των δικτυακών πόρων και των υπολογιστικών συστημάτων για παράνομες ή αντιδεοντολογικές δραστηριότητες.
Η χρήση των δικτυακών πόρων για παραβίαση (με παραγωγή, δημοσίευση ή διακίνηση υλικού) των πνευματικών δικαιωμάτων (copyrights) των δικαιούχων.

1.5. Δικαιοδοσία και υποχρεώσεις ΔΥΗΔ

Ενδεικτικά και σε γενικές γραμμές, οι πράξεις και η συμπεριφορά της ομάδας εργαζομένων της ΔΥΗΔ διέπεται από τις εξής αρχές:

1. Η ΔΥΗΔ θα πρέπει να παρέχει κάθε δυνατή διευκόλυνση στους χρήστες του δικτύου, ώστε να είναι σε θέση να ανταποκριθούν στα καθήκοντα που τους ανατίθενται από το ίδρυμα.

Η ΔΥΗΔ καταβάλει κάθε δυνατή προσπάθεια ώστε να διασφαλίζεται το απόρρητο των αρχείων, μηνυμάτων ηλεκτρονικού ταχυδρομείου και δεδομένων κάθε χρήστη.
Οποτεδήποτε καταγγέλλεται κάποιο περιστατικό παραβίασης ασφαλείας το οποίο αφορά το Δίκτυο Δεδομένων του ιδρύματος, τότε αυτό θα πρέπει να διερευνάται από την ΟΔΕ.
Η ΔΥΗΔ απαγορεύεται να εξετάζει αρχεία, μηνύματα ηλεκτρονικού ταχυδρομείου και άλλα δεδομένα χρηστών. Σε εξαιρετικές περιπτώσεις με αποκλειστικό σκοπό τη διάγνωση και αντιμετώπιση προβλημάτων λογισμικού ή όταν υπάρχουν βάσιμες υποψίες για παραβίαση της ασφάλειας του δικτύου ή όταν υπάρχει σχετική κατά νόμο εντολή από δικαστικές ή διωκτικές αρχές, γίνονται οι απαραίτητες τεχνικές ενέργειες. Η διαδικασία αυτή ενεργοποιείται μόνο μετά από ενημέρωση και εντολή της ΟΔΕ, η οποία μπορεί να ζητήσει τον προσωρινό τερματισμό της σύνδεσης των εμπλεκομένων χρηστών. Η ΟΔΕ, αφού ολοκληρώσει τη διερεύνηση του περιστατικού, θα ενημερώνει τη Σύγκλητο με το σχετικό πόρισμα. Η Σύγκλητος που θα έχει όλα τα δεδομένα στη διάθεση της, θα αποφασίζει εάν υπάρχει ανάγκη για περαιτέρω ενέργειες (ενημέρωση των αρμόδιων αρχών κλπ.). Σε κάθε περίπτωση οι εμπλεκόμενοι χρήστες μπορούν να προσφύγουν στη Σύγκλητο για εξέταση της υπόθεσης τους, η οποία έχει την τελική αρμοδιότητα επιβολής ποινής. Τα παραπάνω ισχύουν με την επιφύλαξη σχετικών προβλέψεων από την ισχύουσα νομοθεσία. Η εξέταση αυτή αφορά δεδομένα αποθηκευμένα σε δίσκους ή μαγνητικές ταινίες της ΔΥΗΔ.
Παρομοίως, η ΔΥΗΔ απαγορεύεται να παρακολουθεί κατά οποιονδήποτε τρόπο υπολογιστικά συστήματα ή δραστηριότητα χρηστών. Σε εξαιρετικές περιπτώσεις με αποκλειστικό σκοπό τη διάγνωση και αντιμετώπιση προβλημάτων λογισμικού ή όταν

υπάρχουν βάσιμες υποψίες για παραβίαση της ασφάλειας του δικτύου ή όταν υπάρχει σχετική κατά νόμο εντολή από δικαστικές ή διωκτικές αρχές, γίνονται οι απαραίτητες τεχνικές ενέργειες. Η διαδικασία αυτή ενεργοποιείται μόνο μετά από ενημέρωση και εντολή της ΟΔΕ, η οποία μπορεί να ζητήσει τον προσωρινό τερματισμό της σύνδεσης των εμπλεκομένων χρηστών. Η ΟΔΕ, αφού ολοκληρώσει τη διερεύνηση του περιστατικού, θα ενημερώνει τη Σύγκλητο με το σχετικό πόρισμα. Η Σύγκλητος που θα έχει όλα τα δεδομένα στη διάθεση της, θα αποφασίζει εάν υπάρχει ανάγκη για περαιτέρω ενέργειες (ενημέρωση των αρμόδιων αρχών κλπ.). Σε κάθε περίπτωση οι εμπλεκόμενοι χρήστες μπορούν να προσφύγουν στη Σύγκλητο για εξέταση της υπόθεσης τους, η οποία έχει την τελική αρμοδιότητα επιβολής ποινής. Τα παραπάνω ισχύουν με την επιφύλαξη σχετικών προβλέψεων από την ισχύουσα νομοθεσία.

Σε όλες τις περιπτώσεις, απαγορεύεται ρητά η διαρροή ή δημοσιοποίηση στοιχείων των παραπάνω δύο περιπτώσεων εκτός της ΔΥΗΔ και της ΟΔΕ. Μόνοι αρμόδιοι να έχουν πρόσβαση σε τέτοια στοιχεία είναι τα προϊστάμενα όργανα του ιδρύματος, με την επιφύλαξη της ισχύουσας νομοθεσίας.

Η ΔΥΗΔ επιτρέπεται να παρακολουθεί στατιστικής φύσεως δεδομένα, και κυρίως τον όγκο της διακινούμενης πληροφορίας. Τα δεδομένα αυτά αφορούν σύνολο διακινούμενης πληροφορίας σε κάποιο μηχάνημα ή υποδίκτυο. Το περιεχόμενο όμως της διακινούμενης πληροφορίας εντάσσεται στην κατηγορία των προσωπικών δεδομένων και δεν παρακολουθείται κατά κανένα τρόπο. Τα δεδομένα αυτά προκύπτουν από νόμιμα, τυποποιημένα πακέτα λογισμικού, και εξάγονται από αρχεία καταγραφής (log files). Σε αρχεία καταγραφής επίσης καταχωρούνται στοιχεία που προβλέπονται από τη νομοθεσία (π.χ. αποστολείς, παραλήπτες και χρονόσημα μηνυμάτων ηλεκτρονικής αλληλογραφίας), καθώς και στοιχεία που είναι απαραίτητα για τον εσωτερικό έλεγχο διαδικασιών (π.χ. στοιχεία μεταβολών βαθμολογιών στο πληροφοριακό σύστημα γραμματειών) για το προβλεπόμενο διάστημα. Τα δεδομένα θα πρέπει να αποθηκεύονται με τέτοιο τρόπο, ώστε να είναι απαραίτητη η παρουσία τουλάχιστον δύο εξουσιοδοτημένων ατόμων, για να γίνει οποιαδήποτε τροποποίηση ή διαγραφή τους.

Η ΔΥΗΔ έχει την υποχρέωση να αναφέρει προβλήματα ασφαλείας στην ΟΔΕ, η οποία και εισηγείται περαιτέρω ενέργειες.

Σε περιπτώσεις εξωτερικών προβλημάτων η ΔΥΗΔ οφείλει να ενημερώνει την ΟΔΕ και αυτές οι δύο να συνεργάζονται με τις αρμόδιες επιτροπές (όπως πχ GRNET-CERT). Σε κάθε περίπτωση ισχύουν οι υφιστάμενοι νόμοι, οι κανονισμοί που προκύπτουν από συμβάσεις, αλλά και οι κανόνες δεοντολογίας.

Η ΔΥΗΔ δικαιούται να ελαττώνει την προτεραιότητα, ή να τερματίζει τη χρήση πόρων του δικτύου σε περίπτωση που χρήστης καταχράται τις δυνατότητες που του παρέχονται και δημιουργεί προβλήματα στην ποιότητα υπηρεσιών που είναι διαθέσιμες στο σύνολο των χρηστών του δικτύου. Ο όρος «χρήστης» στη συγκεκριμένη αυτή περίπτωση περιλαμβάνει και κάθε υπολογιστικό σύστημα που συνδέεται με το Δίκτυο Δεδομένων του ιδρύματος.

Σε περίπτωση κακής ή κακόβουλης χρήσης του δικτύου, η ΔΥΗΔ θα πρέπει να ενημερώνει την ΟΔΕ και να λαμβάνει αποφάσεις (μετάπτωσης), ώστε να δύναται να διακόπτει τη σύνδεση ή να περιορίζει τους χώρους δράσης της που εγκυμονούν κινδύνους.

Η ΔΥΗΔ υποχρεούται να ενημερώνει τους χρήστες για ζητήματα ασφαλείας που ανακύπτουν (νέοι ιοί κ.λπ.).

Η ΔΥΗΔ υποχρεούται να ανακοινώνει προγραμματισμένες εργασίες, οι οποίες επιφέρουν διακοπή λειτουργίας σε τμήματα ή υπηρεσίες του Δικτύου Δεδομένων, τουλάχιστον δύο ημέρες πριν την έναρξη τους. Εξαιρούνται οι περιπτώσεις κατεπειγουσών εργασιών λόγω τεχνικών προβλημάτων, οι οποίες θα πρέπει καταγράφονται κάπου, ώστε να δύναται να βρει κανείς εκεί τις απαραίτητες λεπτομέρειες σε περίπτωση που προκύψει κάποιο ιδιαίτερο πρόβλημα.

Η ΔΥΗΔ υποχρεούται να συνεργάζεται με τις αρμόδιες αρχές της Πολιτείας, σύμφωνα με τα προβλεπόμενα στην εθνική και κοινοτική νομοθεσία, όποτε αυτό απαιτείται.

1.6. Οριοθέτηση χρήσης συστημάτων και δικτυακών πόρων

1. Οι χρήστες οφείλουν να μην καταχρώνται και μονοπωλούν πόρους του Δικτύου και των συστημάτων, όπως αποθηκευτικό χώρο σκληρών δίσκων, διαθέσιμη χωρητικότητα συνδέσεων, άδειες χρήσης λογισμικού, κύκλους μηχανής επεξεργαστών κ.τ.λ. Ιδιαίτερη προσοχή θα πρέπει να επιδεικνύεται ώστε να αποφεύγεται άσκοπη χρήση πόρων, όταν αυτό είναι δυνατόν.

Οι χρήστες οφείλουν να αποδεσμεύουν άδειες χρήσης λογισμικού τις οποίες δεν χρησιμοποιούν.

Οι χρήστες οφείλουν να αποδεσμεύουν διευθύνσεις δικτύου τις οποίες δεν χρησιμοποιούν και να μεριμνούν για τη σωστή και έγκαιρη ενημέρωση της ΔΥΗΔ για αυτές.

Οι χρήστες οφείλουν να μεριμνούν ώστε εργασίες που εκτελούν σε σταθμούς εργασίας μέσω απομακρυσμένης σύνδεσης, μέσω χρονοπρογραμματισμένων εργασιών ή μέσω εργασιών παρασκηνίου να μην παρενοχλούν τον χρήστη που εργάζεται στην κονσόλα του εν λόγω σταθμού.

Το Δίκτυο Δεδομένων και τα συστήματα του ιδρύματος χρησιμοποιούνται για ακαδημαϊκές και ερευνητικές δραστηριότητες και μόνον. Απαγορεύεται ρητά η οποιαδήποτε μορφής παροχή υπηρεσίας ή εμπορικής δραστηριότητας ή συναφών ενεργειών (με ή χωρίς αμοιβή), χωρίς την έγγραφη άδεια της αρμόδιας επιτροπής του ιδρύματος.

Σε κάθε περίπτωση που πρόκειται να χρησιμοποιηθεί λογισμικό ή υλικό με ακαδημαϊκή άδεια χρήσης για άλλους σκοπούς, θα πρέπει να ενημερώνονται τα αρμόδια όργανα του ιδρύματος.

Όσον αφορά υλικό ή λογισμικό που αναπτύσσεται στον φορέα, θα πρέπει να λαμβάνεται μέριμνα ώστε να μην διακυβεύεται η ασφάλεια και η ορθή λειτουργία του δικτύου του.

Απαγορεύεται η χρήση και ανάπτυξη ιών λογισμικού, και γενικά προγραμμάτων που προσπαθούν να παρακάμψουν ή να παραβιάσουν τους μηχανισμούς ασφαλείας του δικτύου, να εξαντλήσουν τους υπολογιστικούς πόρους ή να υποκλέψουν συνθηματικά. Οι υπεύθυνοι συστημάτων του ιδρύματος, οι οποίοι έχουν σε νόμιμα πλαίσια ανάγκες για εμπλοκή με τέτοιου είδους λογισμικό, θα πρέπει να ενημερώνουν τη ΔΥΗΔ.

Η έλλειψη μέτρων ασφάλειας και προστασίας σε οποιοδήποτε σύστημα, λογαριασμό χρήστη ή αρχείο εντός και εκτός του ιδρύματος, σε καμιά περίπτωση δεν δικαιολογεί πρόσβαση (ανάγνωση, αντιγραφή ή αλλοίωση) σε αυτό από τρίτους χρήστες. Το ίδιο ισχύει και για αρχεία του συστήματος που περιέχουν ευαίσθητες πληροφορίες (π.χ. συνθηματικά). Εάν χρήστης εντοπίσει περίπτωση όπου σε αρχείο συστήματος που περιέχει ευαίσθητες πληροφορίες δεν έχουν εφαρμοστεί οι κατάλληλοι μηχανισμοί προστασίας, οφείλει να ενημερώσει την ΟΔΕ, η οποία με τη σειρά της θα ενημερώσει τη ΔΥΗΔ. Επιτρέπεται ανάγνωση αρχείων συστήματος όπου υπάρχουν προνόμια από το λειτουργικό σύστημα, αλλά όχι και αντιγραφή χωρίς άδεια.

Η ΔΥΗΔ είναι αποκλειστικά αρμόδια για την καταχώρηση των συστημάτων που συνδέονται στο Δίκτυο Δεδομένων του ιδρύματος, εκτός από τις περιπτώσεις που η αρμόδια επιτροπή έχει αναθέσει αυτή την υποχρέωση σε τρίτους.

Οι χρήστες οφείλουν να απευθύνονται στη ΔΥΗΔ για σύνδεση ή μεταφορά υπολογιστικών συστημάτων μέσα στο Δίκτυο. Επίσης, οφείλουν να ζητούν επίσημα καταχωρημένη διεύθυνση για το σύστημα τους, σε περίπτωση που θέλουν να συνδεθούν στο εσωτερικό δίκτυο του ιδρύματος.

Επίσης, απαγορεύονται ρητά:

1. Οποιαδήποτε χρήση του δικτύου η οποία αντιβαίνει στην Ελληνική νομοθεσία.

Η χρήση και χορήγηση επίσημων διευθύνσεων του ιδρύματος εκτός των χώρων του (π.χ. με VPN) χωρίς την έγγραφη άδεια της αρμόδιας επιτροπής του ιδρύματος.

Η χρήση επίσημου ονόματος (Fully Qualified Domain Name - FQDN) εκτός των ορίων του domain του ιδρύματος σε συστήματα που χρησιμοποιούν επίσημες διευθύνσεις του, χωρίς την έγγραφη άδεια της αρμόδιας επιτροπής αυτού.

1.7. Κατατεθέντα σήματα και άδειες λογισμικού

1. Η προστασία Κατατεθέντων Σημάτων, αδειών λογισμικού και δικαιωμάτων διανοητικής ιδιοκτησίας διέπεται από την Ελληνική, Ευρωπαϊκή και Διεθνή νομοθεσία και θα πρέπει να είναι σύμφωνη με την πάγια πρακτική και πολιτική του ιδρύματος.

Συμφωνίες ή υποχρεώσεις που τυχόν απορρέουν από τη χρήση λογισμικού αναγνωρίζονται ως έγκυρες από το ίδρυμα, μόνο εφόσον είναι σύμφωνες με την Ελληνική νομοθεσία και την πολιτική του παρόντος κειμένου.

Δεν επιτρέπεται η χρήση οποιουδήποτε λογισμικού χωρίς την αντίστοιχη νόμιμη άδεια χρήσης.

Απαγορεύεται η αντιγραφή και εξαγωγή εκτός του ιδρύματος οποιασδήποτε μορφής δεδομένων (εικόνες, αρχεία, κείμενα, κτλ.) εκτός εάν:

υπάρχει γραπτή άδεια του συγγραφέα ή

βρίσκονται σε χώρο όπου αποθηκεύονται αρχεία προς αντιγραφή ή

κρίνεται απαραίτητο για τη διακρίβωση εγκλημάτων από τα εξουσιοδοτηθέντα προς τούτο όργανα της Πολιτείας.

1.8. Πρόληψη και αντιμετώπιση παραβάσεων

Σε πολλές περιστάσεις μπορεί να προκύψουν παραβιάσεις της παραπάνω πολιτικής, οι οποίες συνήθως οφείλονται σε άγνοια ή ελλιπή ενημέρωση των χρηστών. Η ΔΥΗΔ πάντοτε αντιμετωπίζει τους χρήστες καλοπροαίρετα και τους ενθαρρύνει να ζητούν, όταν έχουν οποιαδήποτε αμφιβολία, τη βοήθεια των τεχνικών της.

Οι τεχνικοί της ΔΥΗΔ έχουν την εξουσιοδότηση να λάβουν άμεσα τα μέτρα που απαιτούνται για την αντιμετώπιση ενός προβλήματος, και να κατευθύνουν τους χρήστες ώστε να μην υποπέσουν ξανά στα ίδια σφάλματα. Συμβάντα όπως μη ηθελημένη κατάχρηση υπολογιστικών πόρων ή προφανή συνθηματικά (που μπορούν εύκολα να αποκωδικοποιηθούν) κ.λπ. μπορούν και θα αντιμετωπίζονται άτυπα και κατά περίπτωση.

Σε περίπτωση υπερβολικής χρήσης των δικτυακών πόρων του ιδρύματος, και με μόνο γνώμονα την αποκατάσταση της καλής λειτουργίας του δικτύου για την ευρεία πλειονότητα των χρηστών του, ή για τον περιορισμό σοβαρών περιπτώσεων παραβιάσεων ασφαλείας (παραβίαση ασφάλειας μηχανημάτων, ιοί, κ.ά.), η ΔΥΗΔ έχει το δικαίωμα να προβαίνει σε προσωρινά μέτρα (απενεργοποίηση λογισμικού, περιορισμό ταχύτητας πρόσβασης, αποσύνδεση κ.τ.λ.) έπειτα από ενημέρωση και έγκριση της ΟΔΕ ή της Συγκλήτου, ανάλογα με τις απαιτήσεις της κάθε περίπτωσης. Πριν από οποιαδήποτε τέτοια πράξη προηγείται προσπάθεια επίλυσης του προβλήματος με τους χρήστες και/ή τον υπεύθυνο του υπολογιστή που προκαλεί το πρόβλημα, εφόσον αυτή η επικοινωνία είναι εφικτή. Τα προσωρινά αυτά μέτρα προστασίας πρέπει να έχουν την ελάχιστη δυνατή διάρκεια που θα εξασφαλίσει την ομαλή λειτουργία του δικτύου, και σε κάθε περίπτωση καταγράφονται και αναφέρονται αναλυτικά στην αρμόδια επιτροπή του ιδρύματος.

Σε σοβαρότερες περιπτώσεις, όπως επαναλαμβανόμενες παραβιάσεις, παράνομες πράξεις, αυθαίρετη εμπορευματοποίηση πόρων του ιδρύματος, κλοπή δεδομένων, κ.τ.λ. η ΔΥΗΔ ενημερώνει την ΟΔΕ και η ΟΔΕ τη Σύγκλητο, προκειμένου να προσδιοριστούν τα προσωρινά μέτρα (απενεργοποίηση λογισμικού ή λογαριασμού, αποσύνδεση κ.τ.λ.) που θα τεθούν σε

ισχύ, πάντα με γνώμονα τα όσα αναπτύχθηκαν στις προηγούμενες παραγράφους. Επίσης η ΔΥΗΔ μπορεί να εισηγηθεί στην ΟΔΕ και τη λήψη πιο μακρόχρονων μέτρων, όπως η περιορισμένη, μακροχρόνια, ή και μόνιμη παύση δικαιωμάτων χρήσης του δικτύου και/ή της παροχής λογαριασμού σε κοινόχρηστους υπολογιστές.

Τέλος, η ΔΥΗΔ δεν έχει αρμοδιότητα να επιβάλλει ή να αίρει κυρώσεις. Διακοπή συνδέσεων χρηστών γίνεται όταν υπάρχουν σοβαρά προβλήματα (κακόβουλη χρήση, μονοπώληση πόρων, τεχνικά προβλήματα που δημιουργούν λειτουργικά προβλήματα στο Δίκτυο, κ.λπ.). Η διακοπή σύνδεσης έχει προσωρινό χαρακτήρα, μέχρις ότου το θέμα εξεταστεί από την αρμόδια επιτροπή του ιδρύματος. Σε περιπτώσεις που το πρόβλημα είναι τεχνικής φύσεως και διορθώνεται, η ΔΥΗΔ αποκαθιστά τη σύνδεση εφόσον δεν συντρέχει λόγος για περαιτέρω διακοπή της λειτουργίας.

1.9. Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Για τη ΔΥΗΔ κρίνεται απαραίτητο, προκειμένου να διεκπεραιώσει την αποστολή της, να επεξεργάζεται προσωπικά δεδομένα χρηστών σύμφωνα με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (ΕΕ 2016/679) και τον Ελληνικό εφαρμοστικό νόμο ν. 4624/2019. Αυτό γίνεται με σεβασμό των δικαιωμάτων προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικότητας των φυσικών προσώπων.

Η ΔΥΗΔ συλλέγει προσωπικά δεδομένα για να εκτελέσει την αποστολή της και μόνο όπως προβλέπεται παρακάτω στους σκοπούς επεξεργασίας. Υπεύθυνος για την επεξεργασία των δεδομένων αυτών είναι ο νόμιμος εκπρόσωπός της.

Υπεύθυνος Προστασίας Δεδομένων: η επικοινωνία με τον Υπεύθυνο Προστασίας Δεδομένων του ΠΑΠΕΛ μπορεί να γίνει στα εξής στοιχεία:

E-mail: dpo@uop.gr
Τηλέφωνο: 2721065118

Οι χρήστες έχουν τα παρακάτω δικαιώματα από τη νομοθεσία:

1. **Δικαίωμα στην πρόσβαση**: ο χρήστης έχει το δικαίωμα να γνωρίζει ποια δεδομένα που τον αφορούν συλλέγονται, και μπορεί να ζητήσει και να λάβει αντίγραφο αυτών, το οποίο και τηρεί η ΔΥΗΔ.

Δικαίωμα στη διόρθωση, την επικαιροποίηση και τη συμπλήρωση: ο χρήστης μπορεί να ζητήσει τη διόρθωση ή την επικαιροποίηση ή τη συμπλήρωση των δεδομένων του, τα οποία τηρεί η ΔΥΗΔ.

Δικαίωμα στη διαγραφή: ο χρήστης των υπηρεσιών μπορεί να ζητήσει τη διαγραφή των στοιχείων του, στον βαθμό που αυτά δεν είναι απαραίτητα για την εκτέλεση των συμβατικών υποχρεώσεων όλων των μερών, αλλά και τις προβλέψεις του νόμου (π.χ. για ιστορικούς λόγους).

Δικαίωμα στον περιορισμό της επεξεργασίας: ο χρήστης των υπηρεσιών μπορεί να ζητήσει τον περιορισμό της επεξεργασίας των δεδομένων του, στον βαθμό που αυτό δεν αντίκειται στις συμβατικές υποχρεώσεις όλων των μερών, αλλά και τις προβλέψεις του νόμου.

Δικαίωμα στη φορητότητα των δεδομένων: ο χρήστης έχει δικαίωμα να ζητήσει τα δεδομένα του να διατηρούνται σε μορφή ανεξάρτητη του πληροφοριακού συστήματος του ιδρύματος, ώστε αυτά να είναι φορητά σε περίπτωση που ζητηθεί.

Άσκηση των δικαιωμάτων του υποκειμένου: για την ενημέρωση και την άσκηση των δικαιωμάτων τους, οι χρήστες μπορούν να επικοινωνούν με τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του ΠΑΠΕΛ.

Δυνατότητα καταγγελίας στην **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** (ΑΠΔΠΧ): Οι χρήστες έχουν το δικαίωμα προσφυγής στην ΑΠΔΠΧ, εφόσον πιστεύουν ότι η επεξεργασία των προσωπικών δεδομένων τους δεν συνάδει με τους δημοσιευμένους σκοπούς και τον παρόντα κανονισμό. Στοιχεία εποπτεύουσας αρχής:

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα

Τηλεφωνικό Κέντρο: +30-210 6475600

Fax: +30-210 6475628

Ηλεκτρονικό Ταχυδρομείο: contact@dpa.gr

Νομική βάση της επεξεργασίας (σκοπός της επεξεργασίας) των δεδομένων: Τα προσωπικά δεδομένα των χρηστών χρησιμοποιούνται:

1. Για την εκπλήρωση της αποστολής της ΔΥΗΔ και της συμβατικής της σχέσης με τους χρήστες, με βάση το υπάρχον νομικό πλαίσιο.

Για την ικανοποίηση υποχρεώσεων από το Νόμο περί παρόχων Δικτύου Επικοινωνιών.
Για την ικανοποίηση αιτημάτων του χρήστη, π.χ. πρόσβαση σε εξωτερική βιβλιοθήκη.
Για σκοπούς αρχειοθέτησης και στατιστικά.
Για τη δημοσίευση συγκεκριμένων στοιχείων επικοινωνίας (ονοματεπώνυμο, τμήμα, ιδιότητα, e-mail) σε ευρετήρια χρηστών του ιδρύματος.

Αποδέκτες της επικοινωνίας: Η ΔΥΗΔ μπορεί να κοινοποιήσει προσωπικά δεδομένα ενός χρήστη:

1. Σε τρίτους, τους οποίους υποδεικνύει ο ίδιος ο χρήστης για την εξυπηρέτηση αιτήματός του, όπως π.χ. κατά την πρόσβαση σε ηλεκτρονική υπηρεσία τρίτων με ταυτοποίηση από υπηρεσία του ιδρύματος. Το ίδρυμα δεν φέρει καμία ευθύνη για τη χρήση των προσωπικών δεδομένων στα χέρια τρίτων.

Στις δικαστικές και εισαγγελικές Αρχές, αλλά και σε κάθε άλλη Δημόσια αρχή η οποία έχει αρμοδιότητα (π.χ. κατά την άσκηση δίωξης), όπως επιβάλλει ο νόμος.
Σε εκτελούντες την επεξεργασία για λογαριασμό του ιδρύματος.

Όπου ζητείται η συγκατάθεση χρήστη, αυτή πάντα μπορεί να ανακληθεί οποτεδήποτε.

Τέλος, το ίδρυμα δύναται να επικαιροποιεί την παρούσα δήλωση προστασίας προσωπικών δεδομένων, οποτεδήποτε, δημοσιεύοντάς την στην ιστοσελίδα του, ως μέρος του παρόντος κανονισμού. Οι χρήστες θα πρέπει να ενημερώνονται πριν την εφαρμογή της αναθεωρημένης μορφής του κανονισμού.

1.10. Διάφορα θέματα ενσύρματης πρόσβασης στο δίκτυο

1.10.1. Ορθολογική χρήση διεύθυνσης δικτύου IP

Η χρήση κάθε διεύθυνσης δικτύου IP πρέπει να είναι σύμφωνη με τον Κανονισμό Λειτουργίας Δικτύου του ιδρύματος.

1.10.2. Αποδέσμευση διεύθυνσης δικτύου IP

Σε περίπτωση που:

1. μια διεύθυνση IP δεν έχει χρησιμοποιηθεί (ενδεικτικά) για διάστημα μεγαλύτερο του ενός ημερολογιακού έτους ή

δεν έχει χρησιμοποιηθεί (ενδεικτικά) για χρονικό διάστημα δύο (2) μηνών από την στιγμή της απόδοσης της ή

ο διοικητικά υπεύθυνος έχει αποχωρήσει από το ίδρυμα (ενδεικτικά, αποχώρηση Διευθυντή εργαστηρίου), χωρίς η ΔΥΗΔ να έχει ενημερωθεί για τυχόν κατά νόμο αντικατάστασή του

τότε το ίδρυμα διατηρεί το δικαίωμα κατάργησης της συγκεκριμένης διεύθυνσης και απόδοσής της εκ νέου σε άλλον υπολογιστή.

1.10.3. Ορθότητα καταχωρημένων στοιχείων διευθύνσεων δικτύου

Οποιοσδήποτε έχει υπ' ευθύνη του έναν υπολογιστή που έχει αποκτήσει διεύθυνση δικτύου IP του ιδρύματος, οφείλει να ενημερώνει για τυχόν αλλαγές σε πρίζα, στα στοιχεία του υπολογιστή καθώς και γενικότερα για αλλαγές στον χώρο. Οι πληροφορίες αυτές είναι απαραίτητες προκειμένου να γίνεται σωστή υποστήριξη από τη ΔΥΗΔ σε περιπτώσεις προβλημάτων.

Επίσης, απαγορεύεται η χρήση μη καταχωρημένων (από τη ΔΥΗΔ) διευθύνσεων IP σε υπολογιστές, καθώς αυτό θα έχει σαν αποτέλεσμα τη δυσλειτουργία τους, αλλά και τη δυσλειτουργία άλλων υπολογιστών του δικτύου. Οι βασικές αιτίες είναι δύο:

1. Η άρνηση εξυπηρέτησης των συγκεκριμένων υπολογιστών από τους περισσότερους εξυπηρετητές (servers).

Η σύγκρουση (IP conflict) διευθύνσεων των υπολογιστών που διαθέτουν επίσημα καταχωρημένη διεύθυνση με εκείνους που τις χρησιμοποιούν αυθαίρετα.

Σε περίπτωση που διαπιστωθεί χρήση μη καταχωρημένης διεύθυνσης, η ΔΥΗΔ αυτομάτως παίρνει μέτρα για τη διακοπή της σύνδεσης του εν λόγω υπολογιστή, με σκοπό να διασφαλίσει την ομαλή λειτουργία του δικτύου του ιδρύματος.

1.10.4. Θέματα ασφάλειας

Αν προκύψει κάποιο θέμα ασφάλειας στο οποίο εμπλέκεται υπολογιστής με επίσημα καταχωρημένη διεύθυνση IP, τότε θα ενημερώνεται ο διοικητικά υπεύθυνος αυτής και ο χρήστης του υπολογιστή.

1.11. Παράρτημα Α. Νέες συνδέσεις και φυσική επέκταση δικτύου

Σε περίπτωση που μέλος της πανεπιστημιακής κοινότητας επιθυμεί την τοποθέτηση πρίζας δικτύου στο χώρο του, θα πρέπει να υποβάλλει άμεσα ανάλογο αίτημα στη ΔΥΗΔ, μαζί με μια συνοπτική περιγραφή του λόγου για τον οποίο γίνεται το αίτημα (πχ ανάγκη εγκατάστασης δικτυακού εκτυπωτή, σύνδεσης νέου υπολογιστή κλπ.). Στη συνέχεια η ΔΥΗΔ, αν το κρίνει σκόπιμο, αναζητά την έγκριση του διοικητικά υπεύθυνου της μονάδας στην οποία ανήκει ο χρήστης που έκανε την αίτηση (πχ για τμήμα του ΠΑΠΕΛ χρειάζεται απόφαση τμήματος, σε διαφορετική περίπτωση απόφαση Συγκλήτου). Σε κάθε περίπτωση, εισηγήσεις προς τα αρμόδια όργανα για επεκτάσεις δικτύων απαιτούν πάντα τη σύμφωνη γνώμη της ΔΥΗΔ.

Στην περίπτωση που δεν είναι επιθυμητή η αναμονή μέχρι τη διενέργεια του επόμενου διαγωνισμού επέκτασης, θα μπορούσε ένα φυσικό πρόσωπο, τμήμα ή μονάδα του ιδρύματος με τη σύμφωνη γνώμη της ΔΥΗΔ να τοποθετήσει πρίζα/ες με δικά του/της έξοδα. Στη περίπτωση αυτή η εργασία θα πρέπει να ανατεθεί σε εταιρία που έχει αποδεδειγμένα την ικανότητα εγκατάστασης και πιστοποίησης δομημένης καλωδίωσης σύμφωνα με το πρότυπο EIA/TIA 568-A [2].

Οποιαδήποτε εργασία γίνεται κάτω από την επίβλεψη των τεχνικών της ΔΥΗΔ, και αφού έχει προηγηθεί η απαραίτητη συνεννόηση. Με το πέρας της εγκατάστασης, η εταιρία είναι υποχρεωμένη να παραδώσει στη ΔΥΗΔ την απαραίτητη πιστοποίηση, η οποία θα αποτελείται από τις μετρήσεις της καλωδίωσης μέσω κατάλληλων προδιαγραφών Cable Tester, κατόψεις του χώρου τοποθέτησης σε ηλεκτρονική μορφή και πίνακες μικτονομήσεων (κυρίων και ενδιάμεσων). Κάθε πρίζα θα πρέπει να τοποθετείται σύμφωνα με το σύστημα αριθμοδότησης του ιδρύματος.

Σε περίπτωση που τα παραπάνω δεν τηρηθούν, η ΔΥΗΔ διατηρεί το δικαίωμα να μην επιτρέψει τη σύνδεση της πρίζας στο δίκτυο του ιδρύματος.

1.12. Παράρτημα Β. Φυσική ασφάλεια

Η φυσική ασφάλεια περιγράφει τα μέτρα ασφαλείας που αποσκοπούν στον περιορισμό της φυσικής πρόσβασης σε εγκαταστάσεις, εξοπλισμό και πόρους του ιδρύματος μόνο σε όσους είναι κατάλληλα εξουσιοδοτημένοι προς τούτο, καθώς και στην προστασία του προσωπικού και της περιουσίας του από ζημιές, βλάβες, κλοπές κλπ. Ως εκ τούτου, ιδιαίτερα σημαντικά είναι τα παρακάτω:

1. Το ίδρυμα οφείλει να μεριμνά για τη φυσική ασφάλεια των εγκαταστάσεων στις οποίες βρίσκονται εγκατεστημένα τα στοιχεία του δικτύου του. Τα μέτρα που λαμβάνονται είναι ανάλογα της κρισιμότητας των στοιχείων αυτών, ενώ λαμβάνεται υπ' όψιν και το κόστος εγκατάστασης και λειτουργίας των μέτρων. Τα μέτρα που λαμβάνει το ίδρυμα για τη φυσική ασφάλεια περιλαμβάνουν, ενδεικτικά, έλεγχο πρόσβασης, προστασία από σεισμό, πλημμύρες, υπερθέρμανση, φωτιά, κεραυνούς.

Κατά την επιλογή ή κατασκευή των εγκαταστάσεων στους οποίους εγκαθιστά στοιχεία του δικτύου του, καθώς και κατά την τοποθέτηση εξοπλισμού και υλοποίηση μέτρων φυσικής

προστασίας, το ίδρυμα θα πρέπει να λαμβάνει υπόψη του τις ιδιαίτερες φυσικές και άλλες συνθήκες οι οποίες επικρατούν στην περιοχή.

Το ίδρυμα οφείλει να μεριμνά ώστε τα κρίσιμα στοιχεία του δικτύου να είναι εγκατεστημένα σε διαφορετικές εγκαταστάσεις ή σε χώρους φυσικά ανεξάρτητους. Όπου αυτό δεν είναι δυνατό, αυτά θα πρέπει να προστατεύονται από ανεξάρτητα μέσα φυσικής προστασίας.

Το ίδρυμα θα πρέπει να μεριμνά ώστε, σε χώρους στους οποίους είναι εγκατεστημένα στοιχεία του δικτύου, χρησιμοποιώντας συστήματα ή διαδικασίες ασφάλειας, ηλεκτρονικά ή μη, να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση, να ελέγχεται η πρόσβαση του προσωπικού και των συνεργατών του μέσω καρτών πρόσβασης ή άλλων σχετικών διαδικασιών, οι οποίες επιτρέπουν την αναγνώριση του προσωπικού και των συνεργατών του αλλά και τον έλεγχο πρόσβασης των επισκεπτών.

Το ίδρυμα οφείλει να μεριμνά για τη φυσική ακεραιότητα, ανθεκτικότητα και τακτική συντήρηση των εγκαταστάσεων στις όποιες είναι εγκατεστημένα τα στοιχεία του δικτύου του.

Το ίδρυμα οφείλει να διαθέτει μηχανισμούς και διαδικασίες για την άμεση ενημέρωσή του ως προς γεγονότα που απειλούν τη φυσική ασφάλεια των στοιχείων του δικτύου του και των χώρων όπου αυτά είναι εγκατεστημένα, και να αξιοποιεί κατάλληλα και αποτελεσματικά τις ενημερώσεις από τους ανωτέρω μηχανισμούς και διαδικασίες.

Όπου αυτό είναι τεχνικά εφικτό, το ίδρυμα θα πρέπει να επιλέγει την υπόγεια εγκατάσταση καλωδίων έναντι της εναέριας. Επίσης, οφείλει να συνεργάζεται με υπηρεσίες δημόσιες και μη, οι οποίες ενδεχομένως εκτελούν εργασίες στο οδικό δίκτυο και εν γένει στους χώρους όπου διέρχονται καλώδια που υποστηρίζουν το δίκτυο του ιδρύματος, με στόχο την ελαχιστοποίηση της πιθανότητας ζημίας στα στοιχεία του δικτύου του.

Το ίδρυμα θα πρέπει να μεριμνά για τον τακτικό έλεγχο των μέτρων φυσικής ασφάλειας, προκειμένου να διασφαλίζεται η εύρυθμη λειτουργία τους.

1.13. Παράρτημα Γ. Τεκμηρίωση δικτύου

Η τεκμηρίωση δικτύου είναι μια μορφή τεχνικής τεκμηρίωσης (technical documentation) και αναφέρεται ουσιαστικά στον τρόπο με τον οποίο διατηρούνται τα διάφορα αρχεία και πληροφορίες για τα δίκτυα υπολογιστών. Η τεκμηρίωση χρησιμοποιείται προκείμενου να δώσει στους διαχειριστές πληροφορίες σχετικά με την αρχιτεκτονική και την υλοποίηση ενός δικτύου, το οποίο είναι ιδιαίτερα χρήσιμο στο πλαίσιο διερεύνησης και επίλυσης διαφόρων προβλημάτων που μπορεί να προκύψουν, αλλά και στις διαδικασίες σχεδιασμού της συντήρησης και της αναβάθμισης.

Η τεκμηρίωση του δικτύου του ιδρύματος, ενδεικτικά, θα πρέπει να περιλαμβάνει:

1. Την αποτύπωση του ενεργού εξοπλισμού, του δικτύου δεδομένων και του τηλεφωνικού δικτύου.

Τα σχέδια οριζόντιας και κατακόρυφης καλωδίωσης και καλωδίωσης κορμού, πάνω στις κατόψεις των ορόφων όλων των κτιρίων του ιδρύματος.

Την αρίθμηση και αποτύπωση παροχών πάνω στις κατόψεις των ορόφων των κτιρίων.

Την αποτύπωση των κατανεμητών που βρίσκονται εντός του ιδρύματος.

Την καταγραφή των μικτονομήσεων μεταξύ patch-panels και ενεργού εξοπλισμού.

Τα αποτελέσματα ελέγχου των καλωδιώσεων χαλκού και οπτικών ινών σύμφωνα με τα αντίστοιχα πρότυπα.

2. Κανονισμός Λειτουργίας Ασύρματων Τοπικών Δικτύων (WLANs)

2.1. Εισαγωγή

Ως ασύρματο δίκτυο χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο.

Τα ασύρματα δίκτυα προσφέρουν τη δυνατότητα σύνδεσης στο Internet υπολογιστών και συσκευών, συνήθως φορητών, χωρίς τη χρήση καλωδίου δικτύου. Απαραίτητες προϋποθέσεις είναι να διαθέτει ο υπολογιστής κάρτα ασύρματης δικτύωσης και να βρίσκεται εντός της εμβέλειας ενός από τα σημεία ασύρματης πρόσβασης (Wireless Access Points). Η δυνατότητα πρόσβασης σε δεδομένα χωρίς τους περιορισμούς των καλωδίων και διάφορων πολύπλοκων διαδικασιών εγκατάστασης κάνουν τα ασύρματα δίκτυα ιδιαίτερα δημοφιλή.

Καθώς όμως το μέσο μετάδοσης δεν είναι χωροταξικά ελεγχόμενο, προκύπτουν θέματα στη χρήση ασύρματων υπηρεσιών που δεν υφίστανται στις ενσύρματες εκδοχές τους. Στην παρούσα ενότητα περιγράφεται το κανονιστικό πλαίσιο και οι προδιαγραφές που πρέπει να τηρούνται σε ό,τι αφορά στη δημιουργία και χρήση ασύρματων τοπικών δικτύων (Wireless Local Area Networks – WLANs) εντός του ιδρύματος. Το κάθε WLAN μπορεί να αποτελείται από ένα ή περισσότερα Access Points.

Σημείωση: Σε περίπτωση που υπάρχει ανάγκη ενός χρήστη ή μιας πολύ μικρής κλειστής ομάδας χρηστών του ιδρύματος για ασύρματη πρόσβαση στο Internet (π.χ. διασύνδεση ασύρματων συσκευών εντός ενός γραφείου ή εργαστηρίου), τότε παρέχεται η δυνατότητα χρήσης ενός WLAN προσωπικής χρήσης, το οποίο να αποτελείται από ένα Access Point, μόνο εφόσον ο χώρος ενδιαφέροντος δεν καλύπτεται από το ασύρματο δίκτυο του ιδρύματος.

2.2. Αρχές

Ο Κανονισμός Λειτουργίας Δικτύου Δεδομένων που περιγράφεται στην προηγούμενη ενότητα, θα πρέπει να εφαρμόζεται και για τα ασύρματα τοπικά δίκτυα, τα οποία θεωρούνται τμήμα του Δικτύου Δεδομένων του ιδρύματος. Επιπλέον, το παρόν κανονιστικό πλαίσιο βασίζεται στις παρακάτω τρεις αρχές ευρείας αποδοχής. Οι ασύρματες υπηρεσίες του ιδρύματος θα πρέπει να έχουν κατάλληλες προδιαγραφές ώστε να επιτυγχάνεται:

1. Η προστασία των ίδιων των χρηστών της υπηρεσίας από υποκλοπή των στοιχείων πιστοποίησής τους (username, password) ή των δεδομένων της επικοινωνίας τους.

Η προστασία του Δικτύου Δεδομένων του ιδρύματος και του Internet από μη εξουσιοδοτημένη χρήση, σύμφωνα με α) τον Κανονισμό Λειτουργίας Δικτύου Δεδομένων που περιγράφεται στην προηγούμενη ενότητα και β) τις υποχρεώσεις του ιδρύματος έναντι τρίτων, π.χ. Κανονισμός Χρήσης ΕΔΥΤΕ [3].

Η πιστοποιημένη παροχή ασύρματης δικτυακής πρόσβασης σε όσο το δυνατόν περισσότερα μέλη της ακαδημαϊκής κοινότητας.

Η ευθύνη λειτουργίας του δικτύου ασύρματης πρόσβασης ανήκει στη ΔΥΗΔ.

Η ευθύνη λειτουργίας των WLANs προσωπικής χρήσης ανήκει στους τελικούς χρήστες που τα εγκαθιστούν για προσωπική τους εξυπηρέτηση. Είναι ευθύνη των ίδιων των χρηστών των WLANs προσωπικής χρήσης να προστατεύονται από υποκλοπές και να εξασφαλίσουν την προστασία του δικτύου δεδομένων και του Διαδικτύου από κακή χρήση του συγκεκριμένου WLAN και των συσκευών που συνδέονται σε αυτό.

Τέλος, απαγορεύεται η παροχή ασύρματης πρόσβασης σε πάνω από (ενδεικτικά) 8 μέλη του ιδρύματος μέσω WLAN προσωπικής χρήσης. Εάν υπάρχουν τέτοιες ανάγκες, απαιτείται να ακολουθούνται οι προβλεπόμενες διαδικασίες για κάλυψη του χώρου από τη ΔΥΗΔ.

2.3. Πλαίσιο παροχής υπηρεσίας

2.3.1. Ασφάλεια

Συνήθως σε μία τοποθεσία υπάρχουν διαθέσιμα πολλά ασύρματα δίκτυα, οπότε ο χρήστης καλείται να διαλέξει αυτό στο οποίο θα συνδεθεί. Η ΔΥΗΔ εγγυάται για την ασφαλή διακίνηση των δεδομένων του χρήστη, μόνον εφόσον αυτός συνδεθεί σε κάποια επίσημα αναγνωρισμένη - πιστοποιημένη υποδομή ασύρματης πρόσβασης από τη ΔΥΗΔ. Άρα, ο χρήστης θα πρέπει να μπορεί με εύκολο τρόπο να επιβεβαιώσει εάν πρόκειται να συνδεθεί σε επίσημη ασύρματη υποδομή του ιδρύματος, και όχι σε ασύρματο εξοπλισμό κάποιου πιθανώς κακόβουλου διαχειριστή, ο οποίος μεταξύ άλλων, θα μπορούσε να παραποιήσει ή να υποκλέψει τη δικτυακή κίνηση και τα δεδομένα του υπολογιστή του εν λόγω χρήστη, ή σε εξοπλισμό που δεν προσφέρει εγγυήσεις ασφαλούς διακίνησης δεδομένων.

Η πιστοποίηση της ταυτότητας του χρήστη από την υποδομή ασύρματης πρόσβασης επιβάλλεται από την ανάγκη για προστασία του δικτύου δεδομένων του ιδρύματος από μη εξουσιοδοτημένη χρήση. Συνεπώς απαγορεύεται η να συνδέουν οι χρήστες στο δίκτυο του ιδρύματος εξοπλισμό πρόσβασης (access points), ο οποίος να υλοποιεί και να διαθέτει προς χρήση ασύρματα δίκτυα στα οποία μπορεί να συνδεθεί οποιοσδήποτε, χωρίς κανέναν έλεγχο. Η υλοποίηση και διάθεση προς χρήση ασύρματων δικτύων όπου οι χρήστες πιστοποιούνται με κοινόχρηστο κωδικό πρόσβασης επιτρέπεται μόνο στα WLANs προσωπικής χρήσης.

Τέλος, η χρήση ισχυρής κρυπτογράφησης στην ασύρματη επικοινωνία, βάσει των διεθνών προτύπων, διασφαλίζει ότι τα δεδομένα του κάθε χρήστη που μεταδίδονται στο ασύρματο μέσο δεν μπορούν να τύχουν υποκλοπής. Ισχυρά προτεινομένη είναι η μέθοδος κρυπτογράφησης WPA2 [7] με AES. Σε περίπτωση που δεν υποστηρίζεται, τότε μπορεί να χρησιμοποιηθεί η παλιότερη WPA [7] με TKIP. Δεν προτείνεται η χρήση της απαρχαιωμένης μεθόδου WEP [9].

2.3.2. Δικαιούχοι

Η πρόσβαση στο ασύρματο δίκτυο θα πρέπει να παρέχεται αποκλειστικά:

στα μέλη της πανεπιστημιακής κοινότητας του ιδρύματος
σε επισκέπτες - μέλη ακαδημαϊκών ιδρυμάτων, τα οποία συμμετέχουν στη διεθνή υποδομή πρόσβασης EduRoam [1].

Η ακαδημαϊκή φύση και οι γενικές αρχές που διέπουν το Δίκτυο Δεδομένων του ιδρύματος, επιβάλλουν κάθε WLAN να είναι προσβάσιμο από οποιοδήποτε μέλος του, ή από οποιοδήποτε μέλος ιδρύματος που συμμετέχει στο EduRoam και βρεθεί μέσα στην εμβέλειά

του. Απαραίτητη προϋπόθεση για να συνδεθεί κάποιος δικαιούχος σε ένα ασύρματο δίκτυο είναι να μπορεί να ταυτοποιηθεί και να εξουσιοδοτηθεί η πρόσβασή του μέσω μιας κεντρικής υποδομής, την οποία θα διαχειρίζεται η ΔΥΗΔ. Τέτοιοι είναι τελικοί χρήστες που:

διαθέτουν λογαριασμό σε τμήμα που συμμετέχει στην κεντρική υποδομή ή
διαθέτουν λογαριασμό σε ίδρυμα που μπορεί να πιστοποιείται μέσω της διεθνούς υποδομής EduRoam ή
διαθέτουν λογαριασμό χρήστη στη ΔΥΗΔ

Για τους επισκέπτες που συμμετέχουν σε ημερίδες, συνέδρια και λοιπές εκδηλώσεις, παρέχεται προσωρινή πρόσβαση επισκέπτη (“guest access”) για τη διάρκεια της εκδήλωσης, κατόπιν συνεννόησης με τη ΔΥΗΔ, εφόσον ο χώρος της εκδήλωσης καλύπτεται από το ασύρματο δίκτυο, χωρίς όμως να αίρεται η απαίτηση για προσωποποιημένη και πιστοποιημένη πρόσβαση. Για το σκοπό αυτό, εκδίδονται από τη ΔΥΗΔ προσωρινά προσωπικά στοιχεία πρόσβασης (username και password) για κάθε επισκέπτη.

Όπως αναφέρεται και στον Κανονισμό Λειτουργίας Δικτύου Δεδομένων του ιδρύματος στην προηγούμενη ενότητα, σε κάθε περίπτωση, η χρήση του δικτύου πρέπει να γίνεται για ακαδημαϊκές και ερευνητικές δραστηριότητες και μόνον. Ιδιαίτερα τονίζεται ότι απαγορεύονται πάσης φύσεως έκνομες δραστηριότητες καθώς και οποιαδήποτε μορφής παροχή υπηρεσίας ή εμπορικής δραστηριότητας ή συναφής ενέργεια (με ή χωρίς αμοιβή), χωρίς την έγγραφη άδεια της αρμόδιας επιτροπής του ιδρύματος.

2.3.3. Γεωγραφική Κάλυψη

Θα πρέπει να καταβάλλεται κάθε δυνατή προσπάθεια από τη ΔΥΗΔ, ώστε η κάλυψη των ασύρματων τοπικών δικτύων να περιορίζεται γεωγραφικά εντός των χώρων του ιδρύματος.

Ειδικά τα WLANs προσωπικής χρήσης θα πρέπει να καλύπτουν ένα σχετικά μικρό χώρο (γραφείο ή εργαστήριο), ενώ δεν επιτρέπεται να εγκαθίστανται και να λειτουργούν παρέχοντας πρόσβαση στο δίκτυο σε χώρους όπου υπάρχει επαρκής κάλυψη από το ασύρματο δίκτυο του ιδρύματος. Σε περίπτωση που ένα WLAN προσωπικής χρήσης ανιχνευθεί με σχετικά ισχυρό σήμα, η ΔΥΗΔ θα πρέπει να ζητήσει από τον υπεύθυνο του WLAN προσωπικής χρήσης κατ' αρχήν να μειώσει την ισχύ εκπομπής του αντίστοιχου Access Point και κατά δεύτερον να εξετάσει την αναγκαιότητα λειτουργίας αυτού του WLAN. Σε περίπτωση μη συμμόρφωσης ως προς τη μείωση της ισχύος εκπομπής, η ΔΥΗΔ διατηρεί το δικαίωμα να διακόψει τη σύνδεση του αντίστοιχου Access Point με το Δίκτυο.

2.4. Τεχνικές προδιαγραφές

2.4.1. Εισαγωγή

Το Wi-Fi είναι μια ομάδα ραδιο-τεχνολογιών (radio technologies) που χρησιμοποιούνται συνήθως για την ασύρματη τοπική δικτύωση συσκευών και βασίζεται στην οικογένεια προτύπων IEEE 802.11 [4].

Για τα δίκτυα καταναλωτών Wi-Fi, υπάρχουν δύο ζώνες συχνοτήτων: 2,4 GHz και 5 GHz.

2.4.2. Περιοχές συχνοτήτων 2,4 και 5 GHz

Παρακάτω ακολουθεί μια λίστα με τα πλεονεκτήματα και τα μειονεκτήματα της κάθε ζώνης:

2,4 GHz:

Θετικά: μεγαλύτερη εμβέλεια, καλύτερη διαπερατότητα σε εμπόδια (για παράδειγμα τοίχοι), μεγαλύτερη υποστήριξη (περισσότερες ασύρματες συσκευές υποστηρίζουν τη συχνότητα 2,4 GHz σε σχέση με τη συχνότητα 5 GHz).

Αρνητικά: πιο αργή ταχύτητα, λιγότερα κανάλια που δεν επικαλύπτονται, μεγαλύτερη συμφόρηση από τα δίκτυα 5 GHz επειδή οι οικιακές συσκευές (για παράδειγμα, φούρνοι μικροκυμάτων και ασύρματα τηλέφωνα) αλλά και οι συσκευές Bluetooth χρησιμοποιούν τη ζώνη δικτύου 2,4 GHz.

5 GHz:

Θετικά: μεγαλύτερη ταχύτητα, κανάλια με λιγότερη συμφόρηση, περισσότερα κανάλια που δεν επικαλύπτονται.

Αρνητικά: μικρότερη εμβέλεια σε σχέση με τα δίκτυα 2,4 GHz, χειρότερη διαπερατότητα τοίχων και άλλων εμποδίων από τα δίκτυα 2,4 GHz, δεν υποστηρίζεται από πολλές συσκευές.

Στις ζώνες συχνοτήτων 2400 - 2483,5 MHz και 5470 - 5725 MHz, επιτρέπεται η λειτουργία συστημάτων ασύρματης πρόσβασης εξωτερικού χώρου, συμπεριλαμβανομένων των ασυρμάτων δικτύων, χωρίς να απαιτείται σχετική αδειοδότηση από την ΕΕΤΤ.

Η χρήση των ζωνών αυτών είναι «ελεύθερη», δηλαδή δεν απαιτεί κάποιου είδους αδειοδότηση από την ΕΕΤΤ, για την ανάπτυξη συγκεκριμένων εφαρμογών, όπως ορίζεται στον Κανονισμό Όρων Χρήσης Μεμονωμένων Ραδιοσυχνοτήτων ή Ζωνών Ραδιοσυχνοτήτων (ΦΕΚ 1713/Β/26-6-2014) και με τη χρήση εξοπλισμού που ικανοποιεί αυστηρά καθορισμένες προδιαγραφές (βλέπε ενότητα 2.4.3). Επιπλέον και ειδικότερα, η χρήση των ζωνών αυτών για εφαρμογές ασυρμάτων δικτύων (τεχνολογία WiFi, ή και άλλες παρόμοιες) υπόκειται σε περιορισμό μέγιστης επιτρεπομένης εκπεμπόμενης ισχύος.

Έτσι, η μέγιστη επιτρεπόμενη ισοτροπικά ακτινοβολούμενη ισχύς στη ζώνη των 2.4 GHz είναι 100 mW e.i.r.p. και στη ζώνη των 5 GHz είναι 1 W e.i.r.p. Στην ισχύ αυτή συνυπολογίζεται η ισχύς εξόδου του πομπού και το κέρδος της κεραίας.

2.4.3. Εξοπλισμός

Σύμφωνα με το Άρθρο 12 εδάφιο λε του Νόμου 4070/2012, όπως ισχύει τροποποιηθέν με το Άρθρο 60 του Νόμου 4313/2014, η ΕΕΤΤ: «*Είναι αρμόδια για θέματα που αφορούν τις προϋποθέσεις χρήσης και διάθεσης στην αγορά του τερματικού εξοπλισμού και ραδιοεξοπλισμού. Με κανονισμό τον οποίο εκδίδει, καθορίζεται κάθε σχετικό με τα ανωτέρω θέμα και κάθε αναγκαία λεπτομέρεια, καθώς και ιδιαίτερα ζητήματα που αφορούν σε τεχνικά χαρακτηριστικά πιθανούς περιορισμούς χρήσης και ραδιοδιεπαφές και διεξαγωγή ελέγχων για την διαπίστωση συμμόρφωσης ραδιεξοπλισμού και τηλεπικοινωνιακού τερματικού εξοπλισμού με τα οριζόμενα στο Π.Δ 44/2002*».

Επίσης, τα θέματα ραδιεξοπλισμού ρυθμίζονται με το Προεδρικό Διάταγμα 98/2017 (ΦΕΚ Α/139/20-9-17), «*Εναρμόνιση της Ελληνικής Νομοθεσίας προς την Οδηγία 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Απριλίου 2014 (ΕΕ L 153/22.05.2014) σχετικά με τη διαθεσιμότητα ραδιεξοπλισμού στην αγορά και την κατάργηση της Οδηγίας 1999/5/ΕΚ*». Με το άρθρο 48 του Π.Δ. 98/2017 καταργείται το παλαιότερο Π.Δ 44/2002.

Με βάση τον ορισμό που περιλαμβάνεται στο Π.Δ.98/2017, ως ραδιεξοπλισμός εννοείται κάθε «*ηλεκτρικό ή ηλεκτρονικό προϊόν που εκούσια εκπέμπει και/ή λαμβάνει ραδιοκύματα για σκοπούς ραδιοεπικοινωνίας και/ή ραδιοεντοπισμού, ή ηλεκτρικό ή ηλεκτρονικό προϊόν που*

πρέπει να συμπληρωθεί με εξάρτημα, όπως π.χ κεραία ώστε εκούσια να εκπέμπει και/ή να λαμβάνει ραδιοκύματα για σκοπούς ραδιοεπικοινωνίας και/ή ραδιοεντοπισμού».

Σύμφωνα με το Άρθρο 3 του Π.Δ. 98/2017, ο ραδιεξοπλισμός πρέπει να κατασκευάζεται με τρόπο που να εξασφαλίζεται η τήρηση των παρακάτω τριών ουσιωδών απαιτήσεων:

1. η προστασία της υγείας και της ασφάλειας των προσώπων και των κατοικίδιων ζώων, καθώς και η προστασία της περιουσίας

το επαρκές επίπεδο ηλεκτρομαγνητικής συμβατότητας

η αποδοτική χρήση του ραδιοφάσματος αφενός και η υποστήριξη της αποδοτικής χρήσης του ραδιοφάσματος αφετέρου, προκειμένου να αποφεύγονται οι επιβλαβείς παρεμβολές

Επίσης, το νομοθετικό πλαίσιο προβλέπει ότι οι συσκευές ραδιοεξοπλισμού πρέπει να φέρουν συγκεκριμένες σημάνσεις και να συνοδεύονται από σχετικά έγγραφα, τα οποία προσδιορίζονται στα σχετικά άρθρα του ΠΔ 98/2017, που ενσωματώνει την οδηγία 2014/53/ΕΕ. Αυτές οι απαραίτητες σημάνσεις και έγγραφα παρουσιάζονται παρακάτω:

Συσκευή:
Σήμανση CE
Μοντέλο & τύπος - Αριθμός παρτίδας & σειράς
Κατασκευαστής: Επωνυμία/εμπορικό σήμα & ταχυδρομική διεύθυνση
Εισαγωγέας: Επωνυμία/εμπορικό σήμα & ταχυδρομική διεύθυνση
Συσκευασία:
Σήμανση CE
Περιορισμοί/Απαιτήσεις
Μοντέλο & τύπος συσκευής
Κατασκευαστής: Επωνυμία/εμπορικό σήμα & ταχυδρομική διεύθυνση
Εισαγωγέας: Επωνυμία/εμπορικό σήμα & ταχυδρομική διεύθυνση
Συνοδευτικά έγγραφα:
Οδηγίες & πληροφορίες για την ασφάλεια και τη χρήση
Περιγραφή εξαρτημάτων/λογισμικού
Ζώνες συχνοτήτων & μέγιστη ραδιοηλεκτρική ισχύς
Περιορισμοί/Απαιτήσεις
Δήλωση συμμόρφωσης
Μοντέλο & τύπος συσκευής
Κατασκευαστής: Επωνυμία/εμπορικό σήμα & ταχυδρομική διεύθυνση
Εισαγωγέας: Επωνυμία/εμπορικό σήμα & ταχυδρομική διεύθυνση

Τέλος, κάποιες πρόσθετες απαιτήσεις για τον ασύρματο εξοπλισμό (Wireless Access Point) που πρέπει να τίθενται από τη ΔΥΗΔ είναι:

Να είναι WiFi certified [5].
Να είναι συμβατό τουλάχιστον με το standard της IEEE 802.11g (προαιρετικά και με τα 802.11a [6] και 802.11n).
Να υποστηρίζει τα πρωτόκολλα WPA και WPA2 σύμφωνα με το standard IEEE 802.11i [8].

Σημειώνεται ότι, καθώς το πρωτόκολλο WEP του προτύπου IEEE 802.11 πλέον θεωρείται πεπαλαιωμένο και μη ασφαλές, και συνακόλουθα δεν επιτρέπεται η χρήση του στην υλοποίηση της κρυπτογράφησης των ασύρματων δικτύων.

2.4.4. Λειτουργικές απαιτήσεις

Σύμφωνα με τις αρχές που αναλύθηκαν στις προηγούμενες παραγράφους, κρίνεται απαραίτητο να τηρούνται και οι εξής λειτουργικές απαιτήσεις για το σύνολο του ασύρματου εξοπλισμού του ιδρύματος:

- Να διαθέτει SSID [10] με το επίσημα καταχωρημένο όνομα μονάδας του ιδρύματος, το οποίο και απαγορεύεται να χρησιμοποιείται από οποιοδήποτε άλλο WLAN στο ίδρυμα.
- Να επιβάλλεται κρυπτογράφηση στο κανάλι επικοινωνίας μεταξύ του Access Point και της ασύρματης συσκευής του χρήστη. Προτείνεται το WPA2 με AES σύμφωνα με το IEEE 802.11i ή εναλλακτικά το WPA με TKIP.
- Να τηρείται από τους διαχειριστές της υπηρεσίας αρχείο καταγραφής πρόσβασης (accounting logs) από όπου θα προκύπτει ο ακριβής χρόνος σύνδεσής και η ταυτότητα του χρήστη. Η διάρκεια και οι συνθήκες φύλαξης και εξουσιοδοτημένης πρόσβασης των στοιχείων του αρχείου πρέπει να είναι σύμφωνα με την ισχύουσα νομοθεσία.

Επίσης, για τον εξοπλισμό που εγκαθιστά το ΠΑΠΕΛ και υλοποιεί την υπηρεσία Eduroam, εκτός από τις παραπάνω λειτουργικές απαιτήσεις, κρίνεται απαραίτητο να τηρούνται και τα παρακάτω:

Να διαθέτει SSID με το αναγνωρίσιμο όνομα “eduroam”
Να εντάσσεται στην ιεραρχία RADIUS [11] του ιδρύματος.
Να υποστηρίζει πιστοποίηση χρηστών προτού δοθεί πρόσβαση στο LAN με χρήση πρωτοκόλλου IEEE 802.1x και επικοινωνία με επίσημο εξυπηρετητή RADIUS μονάδας του ιδρύματος για πιστοποίηση των χρηστών. Ο εν λόγω RADIUS server υποχρεωτικά θα πρέπει να εντάσσεται στην ιεραρχία του ιδρύματος και να λειτουργεί ως μεταγωγός (relaying proxy).
Να υποστηρίζεται συνεργασία του 802.1x authentication με την διεθνή υποδομή EduRoam για υπηρεσίες προς επισκέπτες του ιδρύματος.

2.5. Εγκατάσταση νέων WLANs & Access Points και υποστήριξη

Για την κάλυψη ενός νέου χώρου του ιδρύματος από το ασύρματο δίκτυο, θα πρέπει να υποβληθεί αίτημα προς τη ΔΥΗΔ, προκειμένου να μελετηθούν οι ανάγκες και να γίνουν οι απαραίτητες ενέργειες για την επέκταση της κάλυψης του δικτύου, με εγκατάσταση νέων Access Points.

Για την εγκατάσταση νέου WLAN προσωπικής χρήσης, αρκεί ο χρήστης να το δηλώσει μέσω μιας αίτησης απόδοσης δικτυακών στοιχείων για το αντίστοιχο Access Point.

Η ΔΥΗΔ θα πρέπει να υποστηρίζει όλους τους χρήστες του ασύρματου δικτύου του ιδρύματος. Ωστόσο, η υποστήριξη των χρηστών που επιθυμούν να συνδεθούν στα WLANs προσωπικής χρήσης, θα πρέπει να γίνεται από τους οικείους διαχειριστές που είναι υπεύθυνοι για τη λειτουργία αυτών.

3. Γλωσσάριο όρων

Access Point: σημείο πρόσβασης ασύρματης δικτύωσης
AES: Advanced Encryption Standard
EduRoam: διεθνής συνεργασία πιστοποίησης χρηστών Ακαδημαϊκών - Ερευνητικών ιδρυμάτων
e.i.r.p. – Equivalent isotropically radiated power: μέση ισοδύναμη ισοτροπικά ακτινοβολούμενη ισχύς
IEEE: Institute of Electrical and Electronics Engineers
TKIP: Temporal Key Integrity Protocol
WPA: Wi-Fi Protected Access
WEP: Wired Equivalent Privacy
WLAN: Wireless Local Area Network – ασύρματο τοπικό δίκτυο
ΔΥΗΔ: Διεύθυνση Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης
SNMP: Simple Network Management Protocol
WWW: World Wide Web
FTP: File Transfer Protocol
DNS: Domain Name System
IP (address): Internet Protocol (address)
ΕΔΥΤΕ: Εθνικό Δίκτυο Υποδομών Τεχνολογίας και Έρευνας
MAC (address): Media Access Control (address)
ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
SSID: Service Set Identifier
RADIUS: Remote Authentication Dial-In User Service

4. Αναφορές

1. https://www.eduroam.org
https://en.wikipedia.org/wiki/TIA/EIA-568
https://grnet.gr/aup/
https://en.wikipedia.org/wiki/IEEE_802.11
https://www.wi-fi.org/certification/programs
https://en.wikipedia.org/wiki/IEEE_802.11a-1999
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
https://en.wikipedia.org/wiki/IEEE_802.11i-2004
https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
https://en.wikipedia.org/wiki/Service_set_(802.11_network)
https://en.wikipedia.org/wiki/RADIUS
https://en.wikipedia.org/wiki/Denial-of-service_attack
https://en.wikipedia.org/wiki/Computer_security
https://en.wikipedia.org/wiki/Etiquette_in_technology
https://tools.ietf.org/html/rfc1855