Ελληνικό Μεσογειακό Πανεπιστήμιο

Διεύθυνση Πληροφορικής & Βιβλιοθήκης

Κανονιστικά Πλαίσια και Πολιτικές

(Μάιος 2026)
Αρ. πράξης Συμβουλίου Διοίκησης 121/28.05.2026 (Θέμα 9)

Κανονιστικό Πλαίσιο Λειτουργίας Ιδρυματικού Λογαριασμού Χρήστη

Κανονιστικό Πλαίσιο Προστασίας Υποδομής ΤΠΕ

Κανονιστικό Πλαίσιο Διαχείρισης Αντιγράφων Ασφαλείας Δεδομένων

Πολιτικής Χρήσης Μικρών Αρχείων Κειμένου με Πληροφορίες Πλοήγησης Ιστοσελίδων (cookies)

Περιεχόμενα

Κανονιστικά Πλαίσια και Πολιτικές 1
Κανονιστικό Πλαίσιο Λειτουργίας Ιδρυματικού Λογαριασμού Χρήστη 4
Ιδρυματικός Λογαριασμός Χρήστη 4
Ιδρυματικός Λογαριασμός Φοιτητών 5
Προπτυχιακοί – Μεταπτυχιακοί – Διδακτορικοί 5
Δικαιώματα 5
Όρια Χρήσης 6
Απόφοιτοι 6
Ιδρυματικός Λογαριασμός Προσωπικού 7
Διαδικασία έκδοσης Ιδρυματικού Λογαριασμού Χρήστη (Φυσικό πρόσωπο) 7
Πρόσβαση σε Συστήματα και Υπηρεσίες μέσω του Ιδρυματικού Λογαριασμού 7
Μόνιμο Προσωπικό - Ομότιμοι Καθηγητές 8
Δικαιώματα 8
Όρια Χρήσης 8
Συνταξιοδότηση – Αποχώρηση – Μόνιμου Προσωπικού 9
Δικαιώματα 9
Όρια Χρήσης 9
Έκτακτο Προσωπικό 10
Δικαιώματα 10
Όρια Χρήσης 10
Λήξη Σύμβασης - Έκτακτο Προσωπικό 10
Δικαιώματα 11
Όρια Χρήσης 11
Κανονιστικό Πλαίσιο Προστασίας Υποδομής ΤΠΕ 12
Πολιτική Κωδικού πρόσβασης 12
Κλείδωμα οθόνης 12
Δικαιώματα τοπικού διαχειριστή 13
Όρια Ηλεκτρονικής Αλληλογραφίας 13
Όρια Χωρητικότητας Αποθήκευσης Αρχείων 14
Υπηρεσίες καταλόγου (LDAP – Active Directory) 15
Υπηρεσίες δικτύου 15

Απομάκρυνση υπολογιστών με λειτουργικά συστήματα που δεν υποστηρίζονται. 16
Τείχος Προστασίας (firewall) 16
Χρήση προγράμματος προστασίας από ιούς (Antivirus) 17
Παραβίαση ασφαλείας 17
Απενεργοποίηση λογαριασμού 17
Φιλοξενία Δικτυακού Τόπου 17
Συντήρησης Πρόσθετων και Θεμάτων Δικτυακών Τόπων 18
Επιμόρφωση προσωπικού (επισήμανση αναγκαιότητας) 19
Άδειες Εξαίρεσης 19
Καλές πρακτικές 20
α) Λίστες Αλληλογραφίας (Mailing Lists) 20
Ορισμός Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών 21
Σύμφωνα με το Ν 4961/2022 άρθρο 18 , παράγραφος 1, το ΕΛΜΕΠΑ έχει ορίσει υπεύθυνο και αναπληρωτή υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών, Αριθ.Πρωτ:7643/Φ30.1 απόφαση της Διεύθυνσης Διοικητικού. 21
Κανονιστικό Πλαίσιο Διαχείρισης Αντιγράφων Ασφαλείας Δεδομένων 22
Διαδικασία καθορισμού δεδομένων που συμπεριλαμβάνονται Αντίγραφα Ασφαλείας (Backup) 22
Διαδικασία Λήψης Αντιγράφων Ασφαλείας 22
Διατήρηση Αρχείου Αντιγράφων Ασφαλείας Εκτός Σύνδεσης (Offline) 23
Διαδικασία Επαναφοράς Αντιγράφων Ασφαλείας (Restore) 23
Κανονισμός Πολιτικής Χρήσης Μικρών Αρχείων Κειμένου με Πληροφορίες Πλοήγησης Ιστοσελίδων (COOKIES) 24
Τι είναι τα μικρά αρχεία κειμένου με πληροφορίες πλοήγησης ιστοσελίδων (cookies) ; 24
Ποιος νόμος ισχύει; 24
Ποια cookies εγκαθίστανται; 25
Πώς να ελέγχετε τα cookies 26
Πως μπορώ να αποδεχθώ η να απορρίψω τα cookies σε αυτόν τον ιστότοπο; 26
Πως θα πληροφορηθώ αν αλλάξει η πολιτική cookies 26
Πως μπορώ να επικοινωνήσω με το Ελληνικό Μεσογειακό Πανεπιστήμιο 26

Κανονιστικό Πλαίσιο Λειτουργίας Ιδρυματικού Λογαριασμού Χρήστη

Ιδρυματικός Λογαριασμός Χρήστη

Ο Λογαριασμός Χρήστη (User Account) σε ένα υπολογιστικό σύστημα, δίκτυο, ιστότοπο ή εφαρμογή είναι μια ψηφιακή ταυτότητα που αντιπροσωπεύει ένα συγκεκριμένο άτομο (ή οντότητα). Ουσιαστικά, είναι ο τρόπος με τον οποίο ένα ψηφιακό περιβάλλον αναγνωρίζει ποιος χρήστης είναι, τι επιτρέπεται να κάνει και πώς προτιμά να αλληλοεπιδρά.

Στο ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ λειτουργεί ένας ενοποιημένος κεντρικός ηλεκτρονικός κατάλογος (LDAP directory – Active directory) ο οποίος περιέχει όλους τους χρήστες του ιδρύματος, τους πόρους και τα δικαιώματα πρόσβασης. Η πρόσβαση σε όλες τις υπηρεσίες, και τα συστήματα πραγματοποιείται μέσω της Κεντρικής Υπηρεσίας Πιστοποίησης (Central Authentication Service), η οποία με βάση τον κατάλογο, πιστοποιεί τον χρήστη και παρέχει ή αποτρέπει την πρόσβαση στο συγκεκριμένο σύστημα – υπηρεσία.

Ο μοναδικός λογαριασμός χρήστη στον κεντρικό κατάλογο του ιδρύματος ονομάζεται Ιδρυματικός Λογαριασμός Χρήστη (HMU ID). Έχει τη γενική μορφή username@domainname, (User Principal Name) και μοιάζει με email address, χωρίς να είναι απαραίτητα συνδεμένος με email address. Σε κάθε λογαριασμό αντιστοιχεί και ένα κωδικός πρόσβασης (password) το οποίο ορίζει ο χρήστης.

Οι ιδρυματικοί λογαριασμοί χρήστη έχουν τις δύο παρακάτω μορφές:
A) **username@hmu.gr**
Πρόκειται για λογαριασμούς του προσωπικού του ιδρύματος με οποιαδήποτε σχέση εργασίας, ή για λογαριασμούς λοιπών οντοτήτων του ιδρύματος.

B) **username@edu.hmu.gr**

Πρόκειται για λογαριασμούς των φοιτητών του ιδρύματος σε οποιαδήποτε σχολή ή τμήμα κι αν ανήκουν, είτε πρόκειται για προπτυχιακούς, μεταπτυχιακούς ή υποψήφιους διδάκτορες. Είναι λογαριασμοί που σχετίζονται κυρίως με το φοιτητολόγιο και την ακαδημαϊκή πορεία του φοιτητή

Διευκρινίζεται ότι κάθε φυσικό πρόσωπο πρέπει να αναγνωρίζεται με ένα και μοναδικό ιδρυματικό λογαριασμό στην υπηρεσία καταλόγου του Ιδρύματος. Σε περίπτωση που εντοπίζονται διπλοί λογαριασμοί για το ίδιο φυσικό πρόσωπο θα πρέπει να συγχωνεύονται σε ένα μετά από συνεννόηση με το χρήστη, ο οποίος θα επιλέγει ποιο λογαριασμό επιθυμεί να διατηρήσει.

Διευκρινίζεται ότι ο Ιδρυματικός Λογαριασμός Χρήστη και η αντίστοιχη διεύθυνση αλληλογραφίας (email address) παρέχεται αποκλειστικά για υπηρεσιακή χρήση, όσο αυτός διατηρεί σχέση με το ίδρυμα, και δεν θα πρέπει να χρησιμοποιείται για την ιδιωτική επικοινωνία του χρήστη με τρίτες υπηρεσίες και οργανισμούς (τράπεζες, δημόσιοι φορείς, κοινωνικά δίκτυα κ.τ.λ)

Ιδρυματικός Λογαριασμός Φοιτητών

Προπτυχιακοί – Μεταπτυχιακοί – Διδακτορικοί

Κατά την εγγραφή των Προπτυχιακών ή και Μεταπτυχιακών φοιτητών/τριών στο Ίδρυμα δημιουργείται με αυτοματοποιημένο τρόπο ο αντίστοιχος Ιδρυματικός Λογαριασμός Χρήστη.

Το πρόθεμα του λογαριασμού υποδηλώνει το πρόγραμμα σπουδών του (τμήμα στο οποίο ανήκει) ακολουθούμενο από τον μοναδικό αριθμό μητρώου του στο Φοιτητολόγιο. Π.χ. tp3456@edu.hmu.gr.

Από τη γραμματεία του τμήματος στέλνεται ενημερωτικό μήνυμα στη διεύθυνση ηλεκτρονικού ταχυδρομείου που έχει δηλώσει ο φοιτητής/τρια, το οποίο περιέχει πληροφορίες για τα συστήματα και τις υπηρεσίες που έχει πρόσβαση ο φοιτητής/τρια, καθώς και οδηγίες για την ενεργοποίηση του λογαριασμού του.

Δικαιώματα

Όλοι οι ενεργοί φοιτητές/τριες του Ιδρύματος έχουν πρόσβαση μέσω του λογαριασμού τους στα παρακάτω:

- Υπηρεσίες Ηλεκτρονικής Αλληλογραφίας (με Προσωπικό Γραμματοκιβώτιο)

- Συμμετοχή στις Λίστες Διανομής Αλληλογραφίας φοιτητών
- Υπηρεσίες Μητρώου Σπουδαστών (Φοιτητολόγιο)
- Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων (Eclass)
- Υπηρεσίες Βιβλιοθήκης
- Απομακρυσμένη πρόσβαση στο δίκτυο του Πανεπιστημίου μέσω Εικονικού Ιδιωτικού Δικτύου (VPN)
- Πρόσβαση στο ασύρματο δίκτυο (Wi-Fi) του Πανεπιστημίου καθώς και στα συνεργαζόμενα Ιδρύματα, μέσω του διεθνούς δικτύου Eduroam
- Πρόσβαση τις εφαρμογές Google Apps for Education
- Πρόσβαση στις υπηρεσίες Microsoft 365
- Πρόσβαση σε εξωτερικές υπηρεσίες οι οποίες παρέχονται μέσω της συνομοσπονδίας του ΕΔΕΤ
    - Ηλεκτρονική Υπηρεσία Ολοκληρωμένης Διαχείρισης Συγγραμμάτων (ΕΥΔΟΞΟΣ)
    - Ηλεκτρονική Υπηρεσία Απόκτησης Ακαδημαϊκής Ταυτότητας
    - Λοιπές υπηρεσίες
- *Σημείωση: Επικαιροποιημένη λίστα και πληροφορίες είναι αναρτημένες στο δικτυακό τόπο της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης στην ηλεκτρονική διεύθυνση:* http://www.icsd.hmu.gr/ypiresies_gia_foitites

Όρια Χρήσης

- Για την ηλεκτρονική αλληλογραφία δείτε παρακάτω στο παρόν έγγραφο την αντίστοιχη ενότητα 2.4.
- Για τον διαθέσιμο χώρο αποθήκευσης αρχείων δείτε παρακάτω στο παρόν έγγραφο την αντίστοιχη ενότητα 2.5 .

Απόφοιτοι

Μετά την κτήση του πτυχίου ο Ιδρυματικός Λογαριασμός Χρήστη των φοιτητών/τριών παραμένει ενεργός με μοναδικό δικαίωμα πρόσβασης στις Υπηρεσίες Μητρώου Σπουδαστών (Φοιτητολόγιο).

Κατά τη διαδικασία ανακήρυξης του αποφοίτου θα πρέπει ο υποψήφιος απόφοιτος να συμπληρώνει την εξωτερική διεύθυνση ηλεκτρονικής αλληλογραφίας (email address) που επιθυμεί να λαμβάνει ενημέρωση από το Πανεπιστήμιο. Στη διεύθυνση αυτή θα γίνεται προώθηση των ηλεκτρονικών μηνυμάτων του μετά από αίτημά του. Μετά την υποβολή της αίτησης πτυχίου δίνεται περιθώριο δύο (2) μηνών ώστε ο απόφοιτος να:

- Αποθηκεύσει τοπικά (σε προσωπικό υπολογιστή) τα μηνύματα ηλεκτρονικής αλληλογραφίας που βρίσκονται στο γραμματοκιβώτιο του.

- Να αποθηκεύσει σε προσωπικό αποθηκευτικό μέσο τυχόν αρχεία που έχει αποθηκεύσει στις υπηρεσίες νέφους Google Drive και One Drive η σε άλλα σημεία αποθήκευσης (πχ υπολογιστές εργαστηρίων, eclass)
- Μετά την παρέλευση του χρονικού διαστήματος των δύο μηνών διαγράφονται όλα τα αρχεία από τις υπηρεσίες νέφους καθώς και το γραμματοκιβώτιο με τα μηνύματα του απόφοιτου
- Τέλος ο Ιδρυματικός Λογαριασμός του απόφοιτου αποσυνδέεται από τις ομάδες δικαιωμάτων (security groups) των ενεργών φοιτητών του Ιδρύματος

Ιδρυματικός Λογαριασμός Προσωπικού

Διαδικασία έκδοσης Ιδρυματικού Λογαριασμού Χρήστη (Φυσικό πρόσωπο)

Για την έκδοση Ιδρυματικού Λογαριασμού Χρήστη συμπληρώνεται ηλεκτρονικό αίτημα από τον χρήστη μέσω του παρακάτω συνδέσμου https://secretariat.hmu.gr/auth/request.html. Η αρχική πιστοποίηση του χρήστη για την συμπλήρωση του αιτήματος γίνεται με τους κωδικούς του TaxisNet. Στην περίπτωση που ο χρήστης δεν διαθέτει λογαριασμό στο TaxisNet το αίτημα θα κατατίθεται από τον/την υπεύθυνο/η συνεργασίας.

Κατά τη διαδικασία συμπλήρωσης του αιτήματος ο χρήστης καλείται να συμπληρώσει προσωρινό κωδικό για τη δημιουργία του λογαριασμού. Μετά τη δημιουργία του λογαριασμού στέλνεται ενημερωτικό μήνυμα στο προσωπικό email που έχει ορίσει ο χρήστης, το οποίο τον ενημερώνει για τα στοιχεία του λογαριασμού του και για τα συστήματα και τις υπηρεσίες που έχει πρόσβαση μέσω αυτού του λογαριασμού. Κατά την πρώτη είσοδο του χρήστη, στον Λογαριασμό Ηλεκτρονικής Αλληλογραφίας, απαιτείται αλλαγή κωδικού πρόσβασης (password).

Ιδρυματικοί λογαριασμοί οι οποίοι δεν ανήκουν σε φυσικά πρόσωπα (π.χ διοικητικές μονάδες, ερευνητικά εργαστήρια, συνέδρια κ.α) έχουν πρόσβαση μόνο στην υπηρεσία ηλεκτρονικής αλληλογραφίας, μέσω διαμοιραζόμενων γραμματοκιβωτίων. Η πρακτική αυτή θεωρείται βέλτιστη καθώς τα διαμοιραζόμενα γραμματοκιβώτια δε δεσμεύουν άδειες χρήσης και οι χρήστες έχουν πρόσβαση στα διαμοιραζόμενα γραμματοκιβώτια με χρήση του ιδρυματικού τους λογαριασμού. Ένας χρήστης μπορεί να έχει πρόσβαση σε περισσότερα από ένα διαμοιραζόμενα γραμματοκιβώτια.

Πρόσβαση σε Συστήματα και Υπηρεσίες μέσω του Ιδρυματικού Λογαριασμού

Οι κάτοχοι Ιδρυματικού Λογαριασμού Χρήστη έχουν πρόσβαση στα παρακάτω συστήματα:

- Είσοδο σε σταθμούς εργασίας (Η/Υ) στους τομείς του Ιδρύματος
- Υπηρεσία Ηλεκτρονικής Αλληλογραφίας (email account της μορφής username@hmu.gr)
- Απομακρυσμένη πρόσβαση στο δίκτυο του Πανεπιστημίου μέσω της υπηρεσίας Εικονικού Ιδιωτικού Δικτύου (VPN)
- Σύστημα Διαχείρισης Αιτημάτων
- G Suite (Google Apps) και Google Drive
- Office ΔΗΛΟΣ 365
- Μετακινήσεις προσωπικού
- Πλατφόρμα δήλωσης προσωπικού ασφαλείας
- Λογισμικό τηλεδιασκέψεων (Microsoft Teams)
- Φιλοξενία ιστότοπων
- Υπηρεσίες Βιβλιοθήκης
- Πρόσβαση στην υπηρεσία eClass.
- Πρόσβαση σε διιδρυματικές υπηρεσίες

Σημείωση: Επικαιροποιημένη λίστα και πληροφορίες είναι αναρτημένες στο δικτυακό τόπο της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης στην ηλεκτρονική διεύθυνση: http://www.icsd.hmu.gr/ypiresies_gia_prosopiko

Μόνιμο Προσωπικό - Ομότιμοι Καθηγητές

Δικαιώματα

Το Μόνιμο Προσωπικό του Πανεπιστημίου, μέσω του Ιδρυματικού Λογαριασμού Χρήστη, έχει πρόσβαση στα παρακάτω:

- Όλα τα συστήματα που αναφέρονται στην ενότητα «Πρόσβαση σε Συστήματα και Υπηρεσίες μέσω του Ιδρυματικού Λογαριασμού»
- Προσωπική περιοχή αποθήκευσης αρχείων στον τοπικό διακομιστή (File Server) του Ιδρύματος.
- Πρόσβαση στους διαμοιρασμένους δικτυακούς δίσκους αποθήκευσης Κοινόχρηστων Εγγράφων.
- Συμμέτοχή στις Λίστες Διανομής Αλληλογραφίας
- Υπηρεσίες Μητρώου Σπουδαστών (Εκπαιδευτικό Προσωπικό)
- Εξειδικευμένες υπηρεσίες ανάλογα με την θέση και την ιδιότητα

Όρια Χρήσης

- Για την ηλεκτρονική αλληλογραφία δείτε παρακάτω στο παρόν έγγραφο την αντίστοιχη ενότητα 2.4.

- Για τον διαθέσιμο χώρο αποθήκευσης αρχείων δείτε παρακάτω στο παρόν έγγραφο την αντίστοιχη ενότητα 2.5 .
- Υποχρεωτική αλλαγή του Κωδικού πρόσβασης σε διάστημα ενός (1) έτους το πολύ.

Συνταξιοδότηση – Αποχώρηση – Μόνιμου Προσωπικού

Κατά τη συνταξιοδότηση, ή την αποχώρηση για οποιοδήποτε λόγο, (π.χ. μετάταξη, διορισμός σε άλλη υπηρεσία) ακολουθείται η παρακάτω διαδικασία

Ο χρήστης πριν την αποχώρησή του φροντίζει να παραδώσει όλο το υπηρεσιακό ηλεκτρονικό υλικό το οποίο διαχειριζόταν (αρχεία, μηνύματα ηλεκτρονικής αλληλογραφίας, κωδικούς πρόσβασης κλπ) στον προϊστάμενο της μονάδας στην οποία ανήκε, και σε συνεννόηση με τη Διεύθυνση Πληροφορικής, να πάρει αντίγραφα ασφαλείας σε προσωπικά αρχεία που τυχόν διαθέτει σε τοπικούς υπολογιστές, δικτυακούς δίσκους ή σε δίσκους νέφους (cloud drives) καθώς αυτά θα διαγραφούν μετά την αποχώρησή του.

Μετά από συνταξιοδότησή ή αποχώρηση μετάταξη, το Μόνιμο Προσωπικό του Ιδρύματος έχει τη δυνατότητα να διατηρήσει τον Ιδρυματικό του Λογαριασμό ενεργό εφόσον το επιθυμεί.

Ο λογαριασμός του χρήστη παραμένει ενεργός για διάστημα ενός (1) έτους μετά την συνταξιοδότηση ή τη λήξη της σύμβασης εργασίας του με το Ίδρυμα.. Μετά την λήξη του παραπάνω διαστήματος αποστέλλεται μήνυμα στον χρήστη σχετικά με την διατήρηση ή μη του λογαριασμού του. Αν δεν υπάρξει ανταπόκριση σε διάστημα ενός(1) μηνός από την αποστολή του παραπάνω μηνύματος ο λογαριασμός μπαίνει σε κατάσταση απενεργοποίησης. Αν δεν υπάρξει άλλη επικοινωνία εντός εξαμήνου ο λογαριασμός διαγράφεται.

Δικαιώματα

Για όσο χρονικό διάστημα παραμένει ο λογαριασμός ενεργός, ο χρήστης έχει πρόσβαση στα παρακάτω:

- Υπηρεσία Ηλεκτρονική Αλληλογραφία (email account της μορφής username@hmu.gr)
- Πρόσβαση στη Γενική Λίστα Διανομής Αλληλογραφίας (mail–list)

Όρια Χρήσης

Για όσο διάστημα ο Ιδρυματικός Λογαριασμός Χρήστη είναι ενεργός ισχύουν τα παρακάτω:

- Σχετικά με την ηλεκτρονική αλληλογραφία, ισχύει ένα από τα παρακάτω:
  - Είτε διατηρείται το γραμματοκιβώτιο του χρήστη στο Διακομιστή Αλληλογραφίας (Mail Server) του Ιδρύματος (με βάση τα όρια της ενότητας 2.4)

- Είτε γίνεται ανακατεύθυνση των μηνυμάτων (forwarding) σε προσωπική εξωτερική διεύθυνση ηλεκτρονικής αλληλογραφίας (email account) που θα δηλώσει στο αίτημά του ο χρήστης, χωρίς διατήρηση αντιγράφου στο στο Διακομιστή Αλληλογραφίας (Mail Server) του Ιδρύματος

- Ο λογαριασμός χρήστη αποσυνδέεται, ανάλογα με την ιδιότητα του χρήστη, από ομάδες (group) που του εκχωρούν δικαιώματα σε εφαρμογές και κομβικές υπηρεσίες του Ιδρύματος.
- Υποχρεωτική αλλαγή του Κωδικού πρόσβασης σε διάστημα ενός (1) έτους το πολύ.

Έκτακτο Προσωπικό

Δικαιώματα

Το Έκτακτο Προσωπικό του Πανεπιστημίου μέσω του λογαριασμού του έχει πρόσβαση στα παρακάτω:

- Όλα τα συστήματα που αναφέρονται στην ενότητα «Πρόσβαση σε Συστήματα και Υπηρεσίες μέσω του Ιδρυματικού Λογαριασμού»
- Προσωπική περιοχή αποθήκευσης αρχείων στους διακομιστές (File Servers) του Ιδρύματος σε προσωπικό που υποστηρίζει διοικητικές διαδικασίες του ΕΛΜΕΠΑ.
- Πρόσβαση σε χώρους αποθήκευσης Κοινόχρηστων Εγγράφων σε προσωπικό που υποστηρίζει διοικητικές διαδικασίες του ΕΛΜΕΠΑ.
- Λίστα Διανομής Υπηρεσιακού Ταχυδρομείου
- Λίστα Διανομής Αλληλογραφίας (mail–list)

Όρια Χρήσης

- Κατά τη συμπλήρωση του αιτήματος για τη δημιουργία του λογαριασμού θα πρέπει να αναφέρεται ο επιστημονικά υπεύθυνος ή ο προϊστάμενος τμήματος στο οποίο θα απασχολείται.
- Παρέχεται γραμματοκιβώτιο στους Διακομιστές Αλληλογραφίας (Mail Servers) του Ιδρύματος, με βάση τα όρια της ενότητας 2.4).
- Ο Ιδρυματικός Λογαριασμός Χρήστη δημιουργείται με για συγκεκριμένο χρονικό διάστημα. Η ημερομηνία λήξης του λογαριασμού ορίζεται στα 2 έτη από την υπογραφή της σύμβασης με δικαίωμα ανανέωσης.

Λήξη Σύμβασης - Έκτακτο Προσωπικό

Μετά τη λήξη της σύμβασής του το Έκτακτο Προσωπικό του Πανεπιστημίου έχει τη δυνατότητα να διατηρήσει τον Ιδρυματικό του Λογαριασμό του εφόσον το επιθυμεί για ένα (1) έτος.

Η προβλεπόμενη διαδικασία για τη διατήρηση του λογαριασμού είναι η εξής:

Ο χρήστης συμπληρώνει αίτημα μέσω ηλεκτρονικής αλληλογραφίας στη διεύθυνση helpdesk@hmu.gr στο οποίο αναφέρει ότι επιθυμεί να παραμείνει ο λογαριασμός του ενεργός για το χρονικό διάστημα του ενός(1) έτους. Μετά την λήξη του παραπάνω διαστήματος αποστέλλεται μήνυμα στον χρήστη σχετικά με την διαγραφή του λογαριασμού του. Αν δεν υπάρξει ανταπόκριση σε διάστημα ενός (1) μήνα από την αποστολή του παραπάνω μηνύματος ο λογαριασμός διαγράφεται οριστικά.

Δικαιώματα

Για όσο διάστημα ο Ιδρυματικός Λογαριασμός Χρήστη είναι ενεργός ισχύουν τα παρακάτω:

- Ηλεκτρονική Αλληλογραφία (email account της μορφής username@hmu.gr)
- Πρόσβαση σε Γενική Λίστα Διανομής Αλληλογραφίας (mail–list)

Όρια Χρήσης

Για όσο διάστημα ο Ιδρυματικός Λογαριασμός Χρήστη είναι ενεργός ισχύουν τα παρακάτω:

- Σχετικά με την ηλεκτρονική αλληλογραφία, ισχύει ένα από τα παρακάτω:
    - Είτε διατηρείται το γραμματοκιβώτιο του χρήστη στο Διακομιστή Αλληλογραφίας (Mail Server) του Ιδρύματος (με βάση τα όρια της ενότητας 2.4)
    - Είτε γίνεται ανακατεύθυνση των μηνυμάτων (forwarding) σε προσωπική εξωτερική διεύθυνση ηλεκτρονικής αλληλογραφίας (email account) που θα δηλώσει στο αίτημά του ο χρήστης, χωρίς διατήρηση αντιγράφου στο Διακομιστή Αλληλογραφίας (Mail Server) του Ιδρύματος
- Ο λογαριασμός πρόσβασης του χρήστη αποσυνδέεται από ομάδες (group) που του εκχωρούν δικαιώματα σε εφαρμογές και κομβικές υπηρεσίες του Ιδρύματος.
- Ο λογαριασμός πρόσβασης του χρήστη εντάσσεται σε ομάδα (group) στην οποία είναι μέλη όλο το έκτακτο προσωπικό που έχει λήξει η σύμβασή του.
- Υποχρεωτική αλλαγή του Κωδικού πρόσβασης σε διάστημα ενός (1) έτους το πολύ.

Κανονιστικό Πλαίσιο Προστασίας Υποδομής ΤΠΕ

Σύμφωνα με την πιστοποίηση ISO 27001 (Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών) και ISO 27701 (Σύστημα Διαχείρισης Προσωπικών Δεδομένων) που έχει λάβει το Ίδρυμα, ορίζονται πολιτικές για την αύξηση της προστασίας των προσωπικών δεδομένων που διατηρεί, επεξεργάζεται και συλλέγει το Ελληνικό Μεσογειακό Πανεπιστήμιο.
Λαμβάνοντας υπόψη ότι το θέμα της προστασίας των προσωπικών δεδομένων είναι κρίσιμο, και τα σχετικά θέματα που δημιουργούνται κατά την χρήση νέων τεχνολογιών συνεχώς αυξάνονται, ορίζεται η ενσωμάτωση των ακόλουθων πολιτικών στη λειτουργία της υπολογιστικής και δικτυακής υποδομής του Πανεπιστημίου:

Πολιτική Κωδικού πρόσβασης

Όλοι οι κωδικοί χρήστη που χρησιμοποιούνται για οποιαδήποτε πρόσβαση στον οργανισμό θα πρέπει να αποτελούνται από τουλάχιστον 9 χαρακτήρες οι οποίοι χαρακτήρες υποχρεωτικά θα είναι συνδυασμός πεζών και κεφαλαίων χαρακτήρων, αριθμών και συμβόλων.

Οι χρήστες θα πρέπει:

- Να μη χρησιμοποιούν εύκολα προβλέψιμους κωδικούς (π.χ. ονοματεπώνυμα, ημερομηνία γεννήσεως κ.λπ.)
- Να διαμορφώνουν τους κωδικούς τους ώστε να περιέχουν συνδυασμό από γράμματα, σύμβολα και αριθμούς.
- Να απομνημονεύουν τους κωδικούς και μην τους καταγράφουν σε μέρη που μπορεί να υποκλαπούν (ατζέντες, σημειωματάρια κ.λπ.)
- Να αλλάζουν τους κωδικούς το αργότερο κάθε 12 μήνες.
- Να μην αποκαλύπτουν τον κωδικό τους σε κανένα, για κανένα λόγο.
- Να ενημερώνουν άμεσα τη Διεύθυνση Πληροφορικής και Βιβλιοθήκης σε περίπτωση υποψίας παραβίασης ή μη εξουσιοδοτημένης χρήσης του κωδικού τους.

Αύξηση της πολυπλοκότητας των κωδικών ασφαλείας των χρηστών όπως περιγράφεται στο Άρθρο 8 του παρόντος εγγράφου.

Παράλληλα έχει ενεργοποιηθεί λειτουργικότητα που υποχρεώνει τους χρήστες να αλλάζουν κωδικούς κάθε 12 μήνες.

Κλείδωμα οθόνης

Όλοι οι σταθμοί εργασίας έχουν ρυθμιστεί ώστε μετά από χρονικό διάστημα αδράνειας 15 λεπτών της ώρας, να κλειδώνουν, χωρίς αδρανοποίηση του σταθμού εργασίας, και να απαιτείται ξανά πιστοποίηση του χρήστη. Για μηχανήματα που δεν μπορεί να εφαρμοστεί η κεντρική πολιτική (policy) θα είναι ευθύνη του διαχειριστή του σταθμού εργασίας να εφαρμόζει σχετική πολιτική.

Δικαιώματα τοπικού διαχειριστή

Δεν παραχωρούνται δικαιώματα τοπικού διαχειριστή σε χρήστες.
Στους σταθμούς εργασίας που χρησιμοποιούνται για διοικητικό έργο έχουν αφαιρεθεί τα δικαιώματα τοπικού διαχειριστή από όλους τους χρήστες. Συνίσταται η εφαρμογή του κανονισμού και στους Η/Υ που χρησιμοποιεί το εκπαιδευτικό και λοιπό προσωπικό του Ιδρύματος .
Σε όσους σταθμούς εργασίας που για οποιοδήποτε λόγο έχουν εκχωρηθεί δικαιώματα τοπικού διαχειριστή, είναι υποχρέωση του διαχειριστή του σταθμού εργασίας να εφαρμόζει τη σχετική πολιτική.

Όρια Ηλεκτρονικής Αλληλογραφίας

Για την διασφάλιση της ομαλής λειτουργίας των συστημάτων ηλεκτρονικής αλληλογραφίας και για να αποφευχθεί ο κίνδυνος καταχώρησης των διακομιστών του Ιδρύματος σε spam lists, ορίζονται τα παρακάτω όρια, τα οποία η Διεύθυνση Πληροφορικής και Βιβλιοθήκης μπορεί να τροποποιεί και να επικαιροποιεί, με γνώμονα τις δυνατότητες του εξοπλισμού, τις απαιτήσεις ασφάλειας, τους διαθέσιμους πόρους, τις δυνατότητες αδειοδότησης (licensing) και λαμβάνοντας πάντα υπόψη τις ανάγκες των διοικητικών και εκπαιδευτικών υπηρεσιών.
Τα όρια που ισχύουν σήμερα (Μάιος 2026) περιγράφονται παρακάτω. Επκαιροποιημένη κατάσταση θα βρίσκεται αναρτημένη στο δικτυακό τόπο της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης.

Για ιδρυματικούς λογαριασμούς της μορφής someuser@hmu.gr

- Χωρητικότητα Γραμματοκιβωτίου 10 GBs
- Μέγιστο μέγεθος μεμονωμένου μηνύματος 20 MBs
- Μέγιστο πλήθος παραληπτών σε ένα μήνυμα 100
- Μέγιστο πλήθος αποστολής μηνυμάτων σε ένα 24ωρο 500 (κάθε παραλήπτης θεωρείται ένα μήνυμα),
- Η πρόσβαση στο γραμματοκιβώτιο επιτρέπεται μέσω των πρωτοκόλλων Exchange (ActiveSync, EWS, OWA), IMAP4, POP3.
- Η πρόσβαση μέσω του πρωτοκόλλου SMTP επιτρέπεται μόνο από διευθύνσεις IP εντός Ελλάδος (GeoIP location)
- **Όταν το γραμματοκιβώτιο (server mailbox) γεμίσει** τότε εξάγεται το περιεχόμενό του σε αρχείο τύπου pst και παραδίδεται στο χρήστη, προκειμένου να το εγκαταστήσει τοπικά στον υπολογιστή του. Στην συνέχεια, σε συνεννόηση πάντα με το χρήστη, διαγράφεται το περιεχόμενο του γραμματοκιβωτίου στο server

(π.χ. παλιότερα μηνύματα), ώστε η χωρητικότητα να παραμείνει εντός του προκαθορισμένου ορίου.

Για ιδρυματικούς λογαριασμούς της μορφής someuser@edu.hmu.gr

- Χωρητικότητα Γραμματοκιβωτίου 160 MBs
- Μέγιστο μέγεθος μεμονωμένου μηνύματος 8 MBs
- Μέγιστο πλήθος παραληπτών σε ένα μήνυμα 100
- Μέγιστο πλήθος αποστολής μηνυμάτων σε ένα 24ωρο 500 (κάθε παραλήπτης θεωρείται ένα μήνυμα),
- Η πρόσβαση στο γραμματοκιβώτιο επιτρέπεται μόνο μέσω webmail.
- Η πρόσβαση μέσω άλλων πρωτοκόλλων αλληλογραφίας (IMAP, POP3, SMTP, κλπ) είναι απενεργοποιημένη.

Όρια Χωρητικότητας Αποθήκευσης Αρχείων

Ανάλογα με την ιδιότητα και τις υπηρεσιακές ανάγκες του κάθε χρήστη παρέχεται προσωπικός χώρος αποθήκευσης αρχείων σε δικτυακούς δίσκους του ιδρύματος είτε τοπικά (on premises) είτε στο νέφος (cloud drives)
Τα όρια που ισχύουν σήμερα (Μάιος 2026) περιγράφονται παρακάτω. Επκαιροποιημένη κατάσταση θα βρίσκεται αναρτημένη στο δικτυακό τόπο της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης.

Οι προσωπικές περιοχές στον τοπικό διακομιστή αρχείων (File Server) έχουν τα παρακάτω χαρακτηριστικά:

- Διαθέσιμες μόνο για το μόνιμο προσωπικό του ιδρύματος (διοικητικό και εκπαιδευτικό), καθώς για το έκτακτο προσωπικό που εκτελεί διοικητικό έργο.
- Χωρητικότητα 50 GBs
- Πρόσβαση μόνο από το τοπικό δίκτυο του ιδρύματος ή μέσω VPN
- Πρόσβαση μέσω πρωτοκόλλου SMB2 (samba)
- Αντιστοίχιση ως δίσκος X: (που δείχνει στο \\zeus\home$\username)

Οι προσωπικές περιοχές σε δίσκους νέφους (Cloud Drives) έχουν τα παρακάτω χαρακτηριστικά

- Είναι διαθέσιμες στους ενεργούς φοιτητές του ιδρύματος όσο και στο προσωπικό

- Παρέχονται είτε ως Google Drive μέσω της συνδρομής του ιδρύματος στο Google Apps for Education είτε ως OneDrive μέσω της συνδρομής του ιδρύματος στο Microsoft Office 365 (κοινοπραξία DELOS365)
- Η χωρητικότητα στο OneDrive είναι 100 GB
- Η χωρητικότητα στο Google Drive είναι 100 GB
- Πρόσβαση στα αρχεία είναι δυνατή από οποιοδήποτε υπολογιστή που έχει πρόσβαση στο internet.

Διευκρινίζεται ότι τα όρια χωρητικότητας ειδικά στους δίσκους νέφους (Google Drive, OneDrive) μπορούν να μεταβάλλονται με βάση τη συνολική διαθέσιμη χωρητικότητα της συνδρομής του ιδρύματος στον αντίστοιχο πάροχο.

Υπηρεσίες καταλόγου (LDAP – Active Directory)

Η ενσωμάτωση όλων των σταθμών εργασίας γραφείων και εργαστηρίων (desktop pcs) (εκπαιδευτικών και ερευνητικών), που λειτουργούν εντός του δικτύου του Ιδρύματος, στην υπηρεσία κεντρικού καταλόγου (LDAP – Active Directory) , γίνεται υποχρεωτική, ώστε όλοι οι χρήστες να χρησιμοποιούν τον ιδρυματικό λογαριασμό για την πρόσβαση σε αυτούς. Παράλληλα, για να μειωθεί ο κίνδυνος ευαλωσημότητας, να ενταχθούν εντός του τείχους προστασίας (firewall) του Ιδρύματος όλοι οι σταθμοί εργασίας, ανεξάρτητα από την χρήση τους.

Όλα τα ασύρματα δίκτυα που λειτουργούν εντός του Ιδρύματος πρέπει να ρυθμιστούν κατάλληλα ώστε να χρησιμοποιούν την κεντρική υπηρεσία πιστοποίησης για να επιτρέπουν την πρόσβαση.

Να δημιουργηθεί υπηρεσία δημιουργία προσωρινών λογαριασμών (π.χ. μέχρι 20 ενεργούς) την οποία θα χρησιμοποιούν όσοι επιθυμούν να παρέχουν πρόσβαση στο διαδίκτυο σε επισκέπτες. Η συγκεκριμένη υπηρεσία θα είναι διαθέσιμη μόνο για τα μέλη του μόνιμου εκπαιδευτικού προσωπικού και τους προϊσταμένους διευθύνσεων και αυτόνομων τμημάτων, η διάρκεια ισχύος των λογαριασμών θα είναι δέκα (10) ημέρες, με δυνατότητα παράτασης όποτε απαιτείται.

Σε όσους σταθμούς εργασίας δεν υπάρχει κεντρική διαχείριση είναι υποχρέωση του διαχειριστή του σταθμού εργασίας να εφαρμόζει σχετική πολιτική.

Υπηρεσίες δικτύου

Υποχρεωτική χρήση ταυτοποίησης από τους χρήστες που επιθυμούν να έχουν πρόσβαση στο εσωτερικό δίκτυο του Ιδρύματος που διαχειρίζεται η Διεύθυνση Πληροφορικής & Βιβλιοθήκης. Για την ταυτοποίηση θα πρέπει να χρησιμοποιείται ο Ιδρυματικός λογαριασμός (το HMU ID της μορφής username@hmu.gr), χρησιμοποιώντας την κεντρική υπηρεσία πιστοποίησης του Ιδρύματος, είτε άλλη υπηρεσία του Ιδρύματος (π.χ.

CAS, Ldap) που πιστοποιεί τους χρήστες από την Κεντρική Υπηρεσία Καταλόγου του Ιδρύματος.
Παράλληλα, όλα τα ασύρματα δίκτυα που λειτουργούν εντός του Ιδρύματος πρέπει να ρυθμιστούν ώστε να χρησιμοποιούν την συγκεκριμένη διαδικασία πρόσβασης.

Απομάκρυνση υπολογιστών με λειτουργικά συστήματα που δεν υποστηρίζονται.

Απόσυρση όλων των σταθμών εργασίας που λειτουργούν με λειτουργικά συστήματα που έχει περάσει ο χρόνος υποστήριξης τους (π.χ. Windows XP, Windows 7, Ubuntu 14.04 LTS, κτλ.). Οι σταθμοί εργασίας θα παραδίδονται στην Διεύθυνση Πληροφορικής και Βιβλιοθήκης, για να αξιολογηθούν και να κριθεί αν μπορούν να αναβαθμιστούν με χρήση εκδόσεων λειτουργικού που λαμβάνουν ενημερώσεις, ώστε να είναι αποδοτικοί και ασφαλείς.
Οι διαχειριστές της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης, πρέπει να εκτελούν διαδικασία αυτοματοποιημένης σάρωσης του δικτύου, τουλάχιστον μια φορά τον χρόνο, για να εντοπίζουν σταθμούς εργασίας που χρησιμοποιούν λειτουργικά συστήματα που δεν υποστηρίζονται, και να ξεκινούν την διαδικασία της απόσυρσής τους.
Όσοι σταθμοί εργασίας δεν είναι στην διαχείριση της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης, ο διαχειριστής τους έχει την υποχρέωση να εφαρμόζει σχετική πολιτική.

Τείχος Προστασίας (firewall)

Ανάπτυξη πολιτικών στο τείχος προστασίας που θα αποτρέπουν τις εσωτερικές και εξωτερικές επιθέσεις.
Το εσωτερικό εικονικό δίκτυο του ΕΛΜΕΠΑ, θα ενώνει τις κεντρικές εγκαταστάσεις στο Ηράκλειο με όλα τις υπόλοιπες εγκαταστάσεις σε: Σητεία, Άγιο Νικόλαο, Ρέθυμνο (εγκαταστάσεις εκπαίδευσης και έρευνας (Τρία Μοναστήρια)), Χανιά και όσες άλλες εγκαταστάσεις επεκταθεί το Πανεπιστήμιο στο μέλλον. Όλες οι υπολογιστικές υποδομές (σταθμοί εργασίας, φορητές συσκευές, εξυπηρετητές, κτλ.) πρέπει να ενταχθούν εντός από το τείχος προστασίας, εκτός αν για λόγους υποστήριξης της υποδομής και της φύσης της εργασίας που εκτελούν πρέπει να είναι εκτός (π.χ. εξωτερικοί DNS). Υπεύθυνοι για να ορίσουν και να χρησιμοποιούν αυτόν τον εξοπλισμό είναι αποκλειστικά το προσωπικό της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης και ειδικότερα οι εκτελούντες χρέη κεντρικού διαχειριστή.
Το τείχος προστασίας θα υλοποιεί τις πολιτικές χρήσης του δικτύου και θα ρυθμίζει την πρόσβαση σε διάφορους πόρους ανάλογα με τα δικαιώματα χρήσης που διαθέτει ο κάθε χρήστης. Η λειτουργία αυτή είναι απαραίτητη, γιατί ο κίνδυνος κακόβουλων επιθέσεων από το εσωτερικό δίκτυο παρουσιάζεται αυξημένος, σύμφωνα με την εμπειρία χρήσης.
Το τείχος προστασίας θα υλοποιεί πολιτική καταγραφής της κίνησης κάθε χρήστη, ώστε σε περίπτωση που ζητηθεί από αρμόδιο φορέα, στα πλαίσια του υφιστάμενου νομικού πλαισίου, το Ίδρυμα να μπορεί να παρέχει τις ζητούμενες πληροφορίες για την χρήση των

υποδομών του. Η περίοδος διατήρησης των στοιχείων καταγραφής πρέπει να ακολουθεί όσα ορίζονται από το υφιστάμενο νομικό πλαίσιο και όχι λιγότερο από 6 μήνες.

Για να αποτρέπονται προσπάθειες παράκαμψης των κανόνων λειτουργίας με χρήση της σύνδεσης σε εξωτερικές υπηρεσίες VPN (είτε μέσω του λειτουργικού συστήματος, είτε μέσω χρήσης επεκτάσεων σε προγράμματα περιήγησης (browsers), είτε με χρήση άλλων τεχνολογιών) πρέπει το τείχος προστασίας (firewall) να απαγορεύει την εγκατάσταση συνδέσεων VPN, εσωτερικά ή εξωτερικά, χωρίς άδεια.

Χρήση προγράμματος προστασίας από ιούς (Antivirus)

Όλοι οι σταθμοί εργασίας θα πρέπει να διαθέτουν πρόγραμμα προστασίας από ιούς (Antivirus), το οποίο θα εφαρμόζει πολιτική καθημερινής γρήγορης σάρωσης καθώς και πλήρους εβδομαδιαίας. Σε περίπτωση που το πρόγραμμα που χρησιμοποιείται δεν είναι το προσφερόμενο από το Ίδρυμα, που ακολουθεί κεντρικά ορισμένη πολιτική (policy), είναι ευθύνη του διαχειριστή που εγκαθιστά το συγκεκριμένο πρόγραμμα να ρυθμίζει την σχετική πολιτική.

Όσοι σταθμοί εργασίας δεν είναι στην διαχείριση της Διεύθυνσης Πληροφορικής και Βιβλιοθήκης, ο διαχειριστής τους έχει την υποχρέωση να εφαρμόζει σχετική πολιτική.

Παραβίαση ασφαλείας

Η **τεκμηριωμένη απόπειρα** ενός χρήστη ενάντια στην ασφάλεια στα εσωτερικά συστήματα (πληροφοριακά συστήματα, δίκτυα κτλ. του Ιδρύματος ή απομακρυσμένων συστημάτων επιφέρει προσωρινό κλείδωμα του λογαριασμού του χρήστη και περαιτέρω έλεγχο της δραστηριότητάς του. Στην συνέχεια, για την ενεργοποίηση του λογαριασμού του θα πρέπει να καταθέσει έντυπη απολογία την οποία θα αξιολογήσει η Επιτροπή «Στρατηγικού Σχεδιασμού Υποδομών Πληροφορικής και Δικτύων» και θα εισηγηθεί για την αφαίρεση του λογαριασμού ή την επαναλειτουργία του.

Απενεργοποίηση λογαριασμού

Η Διεύθυνση Πληροφορικής και Βιβλιοθήκης έχει το δικαίωμα να προβεί σε αναστολή λειτουργίας λογαριασμών που είναι ανενεργοί για χρονικό διάστημα μεγαλύτερο του ενός (1) έτους. Πριν την αναστολή θα πρέπει να γίνει προσπάθεια επικοινωνίας με τον κάτοχο του λογαριασμού, για την διερεύνηση των προθέσεών του, όσον αφορά την χρήση του λογαριασμού.

Φιλοξενία Δικτυακού Τόπου

Κάθε χρήστης που επιθυμεί να χρησιμοποιήσει πόρους του Ιδρύματος για τη φιλοξενία δικτυακού τόπου εργαστηρίου ή προσωπικού δικτυακού τόπου οφείλει να υποβάλει αίτηση

μέσω της πλατφόρμας ΜΙΤΟΣ. Στην αίτηση θα πρέπει να αναφέρονται ο σκοπός και η χρήση του δικτυακού τόπου, η χρονική διάρκεια της φιλοξενίας, ο/η υπεύθυνος/-η διαχείρισης του δικτυακού τόπου, η σχέσης του/της υπεύθυνου/ης με το Ίδρυμα, καθώς και τα στοιχεία επικοινωνίας (κινητό, ηλεκτρονική διεύθυνση e-mail, κτλ.) όλων των εμπλεκομένων.

Η αίτηση αξιολογείται από την αρμόδια επιτροπή ή το διαχειριστή. Σε περίπτωση έγκρισης, φιλοξενία παρέχεται για χρονικό διάστημα που που συνδέεται με την χρονική διάρκεια της της σχέσης εργασίας ή της σύμβασης του προσωπικού που είναι υπεύθυνο για τη διαχείριση του δικτυακού τόπου, και δεν θα μπορεί να ξεπερνάει τα δύο (2) έτη. Με το πέρας της χρονικής διάρκειας φιλοξενίας απαιτείται υποβολή αίτησης ανανέωσης.

Ο χρονικός περιορισμός της φιλοξενίας τίθεται για λόγους ασφάλειας πληροφοριακών συστημάτων, καθώς έχει διαπιστωθεί ότι δημιουργούνται κίνδυνοι από περιπτώσεις δικτυακών τόπων που αναπτύχθηκαν από εξειδικευμένο προσωπικό (π.χ. στα πλαίσια προγραμμάτων) αλλά με το πέρας των συμβάσεων τους ή για άλλους λόγους οι δικτυακοί τόποι βρέθηκαν χωρίς εποπτεία και συντήρηση και αποτέλεσαν εύκολο στόχο για παραβίαση και πραγματοποίηση κακόβουλων ηλεκτρονικών επιθέσεων εντός και εκτός του Πανεπιστημίου.

Συντήρησης Πρόσθετων και Θεμάτων Δικτυακών Τόπων

Σε ιστοσελίδες που είναι εγκαταστημένες στην ιδρυματική υποδομή του ΕΛΜΕΠΑ και έχουν δημιουργηθεί ή διαχειρίζονται από μέλη της κοινότητας, εφόσον έχουν εγκατασταθεί συνιστώσες λογισμικού που αφορούν ενεργά πρόσθετα (plung in) είτε θέματα (themes), θα πρέπει να είναι συμβατές με τις τρέχουσες εκδόσεις του WordPress, της PHP και των βασικών πρόσθετων της ιστοσελίδας, καθώς και να διαθέτουν αναβαθμίσεις ασφαλείας είτε ενημερώσεις , οι οποίες να έχουν εκδοθεί εντός των τελευταίων δώδεκα (12) μηνών.

Η εγκατάσταση των διαθέσιμων ενημερώσεων ή αναβαθμίσεων ασφαλείας θα πρέπει να πραγματοποιείται το αργότερο εντός δύο εβδομάδων από την ημερομηνία έκδοσής τους. Σε αντίθετη περίπτωση, για λόγους ασφάλειας και έως την ολοκλήρωση των απαιτούμενων ενημερώσεων, τα σχετικά πρόσθετα ή θέματα θα αφαιρούνται από την ιστοσελίδα.

2.13.2 Πρόσβαση στο Διαχειριστικό Περιβάλλον των Δικτυακών Τόπων.

Για την ενίσχυση της ασφάλειας των ιστοσελίδων, η πρόσβαση στο διαχειριστικό τους περιβάλλον θα επιτρέπεται μόνο από προκαθορισμένες διευθύνσεις IP ή μέσω της ασφαλούς ιδρυματικής σύνδεσης VPN. Ο περιορισμός αυτός αποσκοπεί στη μείωση της έκθεσης των διαχειριστικών σελίδων στο διαδίκτυο, στον περιορισμό κακόβουλων προσπαθειών σύνδεσης και στη γενικότερη προστασία των λογαριασμών διαχείρισης.

Επιμόρφωση προσωπικού (επισήμανση αναγκαιότητας)

Η επιμόρφωση μελών της κοινότητας είναι το μοναδικό μη τεχνικό μέσο περιορισμού των κινδύνων παραβίασης αλλά ίσως και το σημαντικότερο.
Μέσω της επιμόρφωσης περιορίζεται η πιθανότητα επιτυχούς επίθεσης, με στόχο προσωπικά δεδομένα, αφού οι χρήστες ενημερώνονται για τους κινδύνους και εκπαιδεύονται να τους αποφεύγουν.
Η εκπαίδευση θα παρέχεται μέσω σεμιναρίων ενημέρωσης για νέες τεχνολογίες από τη διεύθυνση Πληροφορικής και Βιβλιοθήκης ή από άλλους φορείς. Κατά την εκπαίδευση πρέπει να γίνεται χρήση προσομοίωσης ρεαλιστικού σεναρίου κυβερνοεπίθεσης.

Άδειες Εξαίρεσης

Σύμφωνα με το Αρθρο 89 του Γ.Κ.Π.Δ δύναται στα Μέλη ΔΕΠ/ΕΔΙΠ/ΕΤΕΠ του πανεπιστημίου να παρεκκλίνουν με την επεξεργασία δεδομένων για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς με το κανονιστικό πλαίσιο λειτουργίας.
Για τις περιπτώσεις που μέλος ΔΕΠ, προϊστάμενος διεύθυνσης ή αυτόνομου τμήματος επιθυμεί να υπάρξει εξαίρεση για κάποιον από τους κανόνες λειτουργίας που αναφέρονται παραπάνω για εκπαιδευτικούς ή ερευνητικούς λόγους ή άλλο αίτιο θα πρέπει να υποβάλει αίτημα στο https://mitos.hmu.gr όπου θα αναφέρει τους λόγους που χρειάζεται να υλοποιηθεί η συγκεκριμένη εξαίρεση, τον χρήστη που αφορά, τον εξοπλισμό που αφορά, το είδος της εργασίας που θα εκτελείται, το χρονικό διάστημα και κυρίως το εξειδικευμένο προσωπικό που θα αναλάβει την διαχείριση του εξοπλισμού (εφόσον απαιτείται). Στην περίπτωση αυτή ο αιτών αναλαμβάνει την ευθύνη λειτουργίας των συστημάτων και της τήρησης του Γενικού Κανονισμού Προστασίας Δεδομένων.

Η αίτηση θα υποβάλλεται μέσω της πλατφόρμας ΜΙΤΟΣ και θα περιλαμβάνει α) τις εξαιρέσεις που αιτούνται, β) τα στοιχεία του υπεύθυνου υποστήριξης, γ) τον υπεύθυνο λειτουργίας των συστημάτων και τήρησης των κανόνων του Γενικού Κανονισμού Προστασίας Δεδομένων, δ) το χρονικό διάστημα που ζητείται η/οι εξαίρεση/εις, ε) την περιγραφή της αναγκαιότητας που υπάρχει ώστε να υλοποιηθεί η εξαίρεση, στ) την υπηρεσία που αφορά η εξαίρεση.

Αφού ζητηθεί η γνώμη του Υπεύθυνου Προστασίας Δεδομένων και αφού αξιολογηθεί η αίτηση από την Επιτροπή Στρατηγικού Σχεδιασμού των Υποδομών Πληροφορικής, Δικτύων και Τηλεπικοινωνιών του ΕΛΜΕΠΑ (αρ. πράξης 8/24.07.2019 θέμα 5 Συνεδρίαση του Πρυτανικού Συμβουλίου) και είναι θετική η απάντηση θα προχωρά η υλοποίηση της εξαίρεσης. Η εξαίρεση θα υλοποιείται με χρονική διάρκεια, το μέγιστο τέσσερα (4) χρόνια και στην συνέχεια θα πρέπει να γίνει ανανέωση της άδειας εξαίρεσης. Ο χρονικος περιορισμός εφαρμόζεται με στόχο τον αποκλεισμό του γεγονότος ύπαρξης

υποδομών οι οποίες σε βάθος χρόνου αφέθηκαν χωρίς εποπτεία και συντήρηση. Επισημαίνεται το γεγονός ότι στο παρελθόν αντιμετωπίσθηκαν κακόβουλες επιθέσεις εντός και εκτός Ιδρύματος εξ αιτίας ύπαρξης τέτοιων υποδομών.

Η Επιτροπή ορίζει ότι η αίτηση για εξαιρέσεις γίνεται αποδεκτή όταν αφορά μία από τις ακόλουθες περιπτώσεις:

1) Καινοτόμο έρευνα που δεν μπορεί να υλοποιηθεί στα πλαίσια λειτουργίας των κεντρικών υποδομών
2) Συνεργασία του Πανεπιστημίου με εξωτερικούς Φορείς (Ιδρύματα, Οργανισμούς, Φορείς, κτλ.)
3) Χρήση καινοτόμων εκπαιδευτικών εργαλείων ή τεχνολογίας
4) Χρήση τεχνολογίας τρίτων για διοικητικές εργασίες
5) Δοκιμαστική χρήση νέων τεχνολογιών
6) Άλλες ειδικές περιπτώσεις που πρέπει να τεκμηριωθεί επαρκώς η απαίτηση.

Απαραίτητη προϋπόθεση για την παροχή της εξαίρεσης είναι να υπάρχει ανάληψη ευθύνης, από μόνιμο εκπαιδευτικό ή ερευνητικό ή διοικητικό προσωπικό, της λειτουργίας των συστημάτων και τήρηση των κανόνων του Γενικού Κανονισμού Προστασίας Δεδομένων.

Καλές πρακτικές

α) Λίστες Αλληλογραφίας (Mailing Lists)

Να εφαρμοστεί πολιτική που θα αποτρέπει την δημοσιοποίηση διευθύνσεων ηλεκτρονικής αλληλογραφίας αναίτια. Θα πρέπει όταν χρησιμοποιούνται οι λίστες ηλεκτρονικής αλληλογραφίας α) οι διευθύνσεις των παραληπτών να αποκρύβονται με χρήση της επιλογής “BCC”, β) όταν προωθούνται μηνύματα, θα πρέπει να γίνεται αφαίρεση των ηλεκτρονικών διευθύνσεων που εμφανίζονται στο σώμα του νέου κειμένου αν δεν προσθέτουν χρήσιμη πληροφορία, δυσκολεύοντας την ανάγνωση και προκαλώντας δημοσιοποίηση διευθύνσεων.

Ορισμός Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών

Σύμφωνα με το Ν 4961/2022 άρθρο 18 , παράγραφος 1, το ΕΛΜΕΠΑ έχει ορίσει υπεύθυνο και αναπληρωτή υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών, Αριθ.Πρωτ:7643/Φ30.1 απόφαση της Διεύθυνσης Διοικητικού.

Κανονιστικό Πλαίσιο Διαχείρισης Αντιγράφων Ασφαλείας Δεδομένων

Διαδικασία καθορισμού δεδομένων που συμπεριλαμβάνονται Αντίγραφα Ασφαλείας (Backup)

Διατηρείται αρχείο καταγραφής δεδομένων το οποίο περιλαμβάνει τις θέσεις των αρχείων (paths) και τα Εικονικά Μηχανήματα (VMs) στα οποία γίνεται λήψη Αντιγράφων Ασφαλείας.

Κάθε 6 μήνες θα στέλνεται λίστα των δεδομένων που συμπεριλαμβάνονται στα Αντίγραφα Ασφαλείας, ανά οργανωτική μονάδα, στον αρμόδιο προϊστάμενο, προκειμένου να διαπιστωθεί ότι όλα τα κρίσιμα δεδομένα των οργανωτικών μονάδων συμπεριλαμβάνονται στα Αντίγραφα Ασφαλείας. Συγκεκριμένα, ζητείται να γίνει έλεγχος - επικαιροποίηση της λίστα για τυχών προσθήκες ή τροποποιήσεις.

Διαδικασία Λήψης Αντιγράφων Ασφαλείας

Διατηρείται αρχείο καταγραφής δεδομένων Αντιγράφων Ασφαλείας (Backup) στο οποίο περιγράφεται το μέσο που χρησιμοποιείται για την λήψη του Backup, ο χρόνος διατήρησης και ο υπεύθυνος, για κάθε επίπεδο Αντιγράφων Ασφαλείας – Αντίγραφα Εφαρμογής, Αντίγραφα Αρχείων, Αντίγραφα Εικονικών Μηχανημάτων (Application Backup - File Backup - VM Backup).

Γενικότερα σε επίπεδο εφαρμογής και σε επίπεδο αρχείων λαμβάνεται μία φορά την εβδομάδα Πλήρες Αντίγραφο Ασφαλείας (Full Backup), και καθημερινά γίνεται λήψη των αλλαγών των δεδομένων (Incremental Backup) το οποίο γράφεται σε Μαγνητικές Ταινίες (Tapes). Όλα τα δεδομένα τα οποία έχουν εγγραφεί σε ταινίες είναι άμεσα διαθέσιμα στις αντίστοιχες συσκευές στην περίπτωση που ζητηθεί Επαναφορά (Restore)

Στα Εικονικά Μηχανήματα (Virtual Machines), τα οποία περιέχουν κρίσιμα δεδομένα, γίνεται λήψη Αντιγράφου Ασφαλείας ολόκληρου του VM σε καθημερινή βάση το οποίο διατηρείται για 15 ημέρες.

Στο Διακομιστή Ηλεκτρονικής Αλληλογραφίας (Mail Server) του προσωπικού, γίνεται λήψη Αντιγράφου Ασφαλείας σε καθημερινή βάση και υπάρχει δυνατότητα επαναφοράς online 365 ημέρες πίσω.

Διατήρηση Αρχείου Αντιγράφων Ασφαλείας Εκτός Σύνδεσης (Offline)

Σε μηνιαία βάση απομακρύνονται από τη Συσκευή Λήψης Αντιγράφων Ασφαλείας (Tape Streamer) οι μαγνητικές ταινίες οι οποίες περιέχουν Πλήρες Αντίγραφο Ασφαλείας (Full Backup) της τελευταίας εβδομάδας του μήνα. Οι μαγνητικές ταινίες αφού καταγραφούν σε αρχείο καταγραφής διατήρησης αρχείου Backup μεταφέρονται και αποθηκεύονται σε διαφορετικό ασφαλή χώρο (διαφορετικό κτήριο). Οι συγκεκριμένες ταινίες διατηρούνται στο αρχείο επ' αόριστο και είναι διαθέσιμα σε περίπτωση που ζητηθεί επαναφορά δεδομένων.

Διαδικασία Επαναφοράς Αντιγράφων Ασφαλείας (Restore)

Τα αντίγραφα που απομακρύνονται από τη Συσκευή Λήψης Αντιγράφων Ασφαλείας (Tape Streamer) και φυλάσσονται εκτός του χώρου που φιλοξενείται η Συσκευή Λήψης Αντιγράφων Ασφαλείας είναι διαθέσιμα σε περίπτωση που ζητηθεί να γίνει επαναφορά δεδομένων. Επίσης σε τακτική βάση (ανά δύο μήνες) γίνεται δειγματοληπτικός έλεγχος (δοκιμαστική επαναφορά – restore) προκειμένου να εντοπιστούν πιθανά προβλήματα. Διατηρείται αρχείο καταγραφής επαναφοράς αντιγράφων ασφαλείας.

Κανονισμός Πολιτικής Χρήσης Μικρών Αρχείων Κειμένου με Πληροφορίες Πλοήγησης Ιστοσελίδων (COOKIES)

Σκοπός της πολιτικής είναι η ενημέρωση των χρηστών ως προς τη χρήση cookies της ιστοσελίδας και η λήψη της συγκατάθεσής τους για το σκοπό αυτό.

Τι είναι τα μικρά αρχεία κειμένου με πληροφορίες πλοήγησης ιστοσελίδων (cookies) ;

Τα «cookies» είναι **μικρά αρχεία με πληροφορίες** που μια ιστοσελίδα (συγκεκριμένα ο εξυπηρετητής ιστού - web server) αποθηκεύει στον υπολογιστή /ταμπλέτα /κινητό τηλέφωνο ενός χρήστη, ώστε κάθε φορά που ο χρήστης συνδέεται στην ιστοσελίδα, η τελευταία να ανακτά τις εν λόγω πληροφορίες και να προσφέρει στο χρήστη σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει ο χρήστης στη συγκεκριμένη ιστοσελίδα (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, διαφημίσεων, κλπ).

Ποιος νόμος ισχύει;

Τα cookies διέπονται από την e-privacy Οδηγία 2002/58/ΕΚ όπως τροποποιήθηκε με την Οδηγία 2009/136 /ΕΚ (η οποία έχει ενσωματωθεί στο Ελληνικό Δίκαιο με τον Ν 3471/2006) όπως ρητώς προβλέπεται και στον 2016/679 Κανονισμό Προστασίας Προσωπικών Δεδομένων αιτιολογική σκέψη 173**.**

Σύμφωνα με ισχύον δίκαιο Ν3471/2006 (βλέπε άρθρο 4 παρ.5 του νόμου αυτού όπως τροποποιήθηκε με το άρθρο 170 Ν 4070/2012) «**Η εγκατάσταση των «cookies» επιτρέπεται μόνο με τη συγκατάθεση του χρήστη και μετά από κατάλληλη ενημέρωσή του.»**
Γι' αυτό και κατά την πρώτη επίσκεψη του χρήστη στην ιστοσελίδα https://www.hmu.gr/el εμφανίζονται αναδυόμενα παράθυρα όπου μπορεί ο επισκέπτης-χρήστης να δηλώσει την συγκατάθεσή του στην εγκατάσταση των cookies που ειδικώς αναφέρονται και πρόκειται για μη λειτουργικά cookies που στοχεύουν στην βελτίωση των υπηρεσιών που παρουσιάζονται στην Ιστοσελίδα όπως είναι: δυνητική βαθμολόγηση από τον Χρήστη ή αξιολόγηση των υπηρεσιών, η σύνδεση με μέσα κοινωνικής δικτύωσης, η ρύθμιση παραμέτρων σε συσκευές αναπαραγωγής ήχου και εικόνας προσαρμοζόμενων των πληροφοριών στις προσωπικές προτιμήσεις του χρήστη, cookies στατιστικής ανάλυσης σχετικά με τον αριθμό των επισκεπτών στην ιστοσελίδα και των αριθμό των σελίδων που προβλήθηκαν χωρίς άμεση ταυτοποίηση του χρήστη.

Ποια cookies εγκαθίστανται;

Α. Με τη συγκατάθεσή σας

Λειτουργικά

Στατιστικά

Τα Cookies που εγκαθίσταται περιγράφονται αναλυτικά στο αναδυόμενο παράθυρο των Cookies της Ιστοσελίδας.

Β. Χωρίς τη συγκατάθεσή σας

Υπάρχουν «cookies» που έχουν εκτιμηθεί από την Ομάδα Εργασίας του άρθρου 29* ως **τεχνικά-λειτουργικά απαραίτητα** για την πραγματοποίηση της σύνδεσης στην ιστοσελίδα ή για την παροχή της υπηρεσίας διαδικτύου. **Για αυτά ο νόμος δεν απαιτεί προηγούμενη συγκατάθεση .**

Αυτά είναι (βλέπε Wp29 Opinion 4/2012)

- Cookies» που είναι απαραίτητα για την αναγνώριση ή/και διατήρηση περιεχομένου που εισάγει ο συνδρομητής ή χρήστης κατά τη διάρκεια μίας σύνδεσης (session) σε ιστοσελίδα καθ' όλη τη διάρκεια της συγκεκριμένης σύνδεσης. (Για παράδειγμα τέτοια «cookies» είναι απαραίτητα κατά τη συμπλήρωση μίας ηλεκτρονικής φόρμας από τον χρήστη).
  Στην ίδια κατηγορία εντάσσονται και τα «επίμονα» (persistent) «cookies» που εγκαθίστανται για τον ίδιο σκοπό και διαρκούν για διάστημα μερικών ωρών.
- «Cookies» που είναι απαραίτητα για την αυθεντικοποίηση του συνδρομητή ή χρήστη σε υπηρεσίες που απαιτούν αυθεντικοποίηση
- «Cookies» που εγκαθίστανται με σκοπό την ασφάλεια του συνδρομητή ή χρήστη, όπως για παράδειγμα «cookies» που εντοπίζουν επαναλαμβανόμενες αποτυχημένες προσπάθειες εισόδου στον λογαριασμό ενός χρήστη σε μία συγκεκριμένη ιστοσελίδα.
- «Cookies» με πολυμεσικό περιεχομένο, όπως flash player «cookies», κατά τη διάρκεια μίας σύνδεσης (session) σε ιστοσελίδα. Τέτοια είναι για παράδειγμα τα «cookies» που εγκαθίστανται με την προβολή ενός βίντεο στην ιστοσελίδα που έχει επισκεφτεί ο χρήστης.
- «Cookies» που «θυμούνται» τις επιλογές του συνδρομητή ή χρήστη σχετικά με την παρουσίαση της ιστοσελίδας (π.χ. «cookies» που αφορούν την επιλογή της γλώσσας ή της παρουσίασης αποτελεσμάτων αναζήτησης σε μία ιστοσελίδα).
- «Cookies» που εγκαθίστανται μέσω πρόσθετων προγραμμάτων (plug ins) σε ιστοσελίδες κοινωνικών δικτύων και αφορούν στο διαμοιρασμό περιεχομένου μεταξύ των πιστοποιημένων μελών που έχουν ήδη πραγματοποιήσει σύνδεση (logged in).

Πώς να ελέγχετε τα cookies

Μπορείτε να διαγράψετε όλα τα cookies που βρίσκονται ήδη στον υπολογιστή σας, όπως και να ρυθμίσετε τους περισσότερους φυλλομετρητές κατά τρόπο που να μην επιτρέπουν την εγκατάσταση cookies. Ωστόσο, στην περίπτωση αυτή, ίσως χρειαστεί να προσαρμόζετε εσείς από μόνοι σας ορισμένες προτιμήσεις κάθε φορά που επισκέπτεστε έναν ιστότοπο, και επίσης ενδέχεται να μην λειτουργούν και μερικές υπηρεσίες.

Για να ελέγχετε και/ή να διαγράφετε τα cookies ανάλογα με τις επιθυμίες σας λεπτομέρειες θα βρείτε εδώ:

http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm#section_2

https://www.aboutcookies.org/

Πως μπορώ να αποδεχθώ η να απορρίψω τα cookies σε αυτόν τον ιστότοπο;

Μπορείτε εύκολα να αποδεχτείτε ή να απορρίψετε τα cookies σε αυτόν τον ιστότοπο επιλέγοντας έναν από τους παρακάτω συνδέσμους:

- Αποδοχή όλων / Παραμετροποίηση/Απόρριψη όλων.

Πως θα πληροφορηθώ αν αλλάξει η πολιτική cookies

Οποιαδήποτε τροποποίηση στην παρούσα πολιτική για τα cookies θα εμφανίζεται εγκαίρως στον Ιστότοπο.

Πως μπορώ να επικοινωνήσω με το Ελληνικό Μεσογειακό Πανεπιστήμιο

Αν έχετε οποιαδήποτε παρατήρηση ερώτηση απορία παρακαλούμε όπως επικοινωνήσετε μέσω E-mail: info@hmu.gr , στο τηλ.: 2810379407, είτε μέσω της Ηλεκτρονικής Συνομιλίας στην Κεντρική Σελίδα του Πανεπιστημίου στο σύνδεσμο https://hmu.gr .