ΦΥΣΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

Μέτρα Ασφάλειας

Στο κείμενο που ακολουθεί περιγράφονται τα μέτρα ασφάλειας που εφαρμόζονται από το Πανεπιστήμιο Δυτικής Μακεδονίας και εντάσσονται στις παρακάτω κατηγορίες:

Α. Οργανωτικά Μέτρα Ασφάλειας
Β. Τεχνικά Μέτρα Ασφάλειας
Γ. Μέτρα Φυσικής Ασφάλειας

Α. Οργανωτικά Μέτρα Ασφάλειας

1. Ρόλοι/Εξουσιοδοτήσεις

Οι εργαζόμενοι πρέπει να έχουν δικαίωμα πρόσβασης μόνο στα απολύτως απαραίτητα δεδομένα προσωπικού χαρακτήρα, βάσει των αρμοδιοτήτων και καθηκόντων που τους έχουν ανατεθεί (ρόλοι), να ενημερώνονται αρμοδίως για τις ευθύνες και τις υποχρεώσεις τους σε σχέση με την ασφάλεια πληροφοριών και δεδομένων, ώστε να ελαχιστοποιείται ο κίνδυνος από ανθρώπινα σφάλματα κατά τη διάρκεια της κανονικής τους εργασίας.

2. Αναθεώρηση ρόλων

Οι εξουσιοδοτήσεις και τα δικαιώματα πρόσβασης σε προσωπικά δεδομένα και πληροφορίες επανεξετάζονται από τον διοικητικά υπεύθυνο σε κάθε εργασιακή αλλαγή εργαζομένου: τοποθέτηση, μετακίνηση, αλλαγή καθηκόντων, αποχώρηση κλπ.

Επιπρόσθετα, οι εργαζόμενοι πρέπει να ενημερώνονται για τις υποχρεώσεις τους σε σχέση με την τήρηση των όρων εμπιστευτικότητας και εχεμύθειας, όταν αλλάζουν θέση εργασίας ή και κατά την λύση της συνεργασίας τους με το Πανεπιστήμιο.

3. Δέσμευση εμπιστευτικότητας

Είναι απαραίτητη η λήψη ειδικών μέτρων ως προς την εμπιστευτικότητα για τη δέσμευση του προσωπικού που επεξεργάζεται προσωπικά δεδομένα, ιδίως όταν το εν λόγω προσωπικό δεν δεσμεύεται ήδη για το απόρρητο.

Συγκεκριμένα στις συμβάσεις και στα συμφωνητικά με συνεργάτες/προμηθευτές πρέπει να συμπεριλαμβάνονται όροι εμπιστευτικότητας και μη αποκάλυψης ευαίσθητων πληροφοριών, όροι προστασίας της ιδιωτικότητας των φυσικών προσώπων και όροι για ασφάλεια των πληροφοριών.

4. Αποχώρηση υπαλλήλου

Κατά την αποχώρηση μέλους του προσωπικού ακολουθείται διαδικασία προστασίας των πληροφοριών και των προσωπικών δεδομένων με ευθύνη του διοικητικά υπευθύνου και την λήψη συγκεκριμένων μέτρων:

1. Απενεργοποίηση/κατάργηση των λογαριασμών πρόσβασης και των εξουσιοδοτήσεων σε πληροφοριακά συστήματα, εφαρμογές και υπολογιστές.
2. Κατάργηση των λογαριασμών ηλεκτρονικού ταχυδρομείου και μη ανάθεσή τους σε άλλον (μη επαναχρησιμοποίηση τους).
3. Επιστροφή οποιουδήποτε εξοπλισμού έχει παρασχεθεί συμπεριλαμβανομένων υπολογιστών, περιφερειακών, κλειδιών, ηλεκτρονικών καρτών εισόδου/εξόδου, κ.λπ.

5. Διαχείριση πληροφοριακών αγαθών

Α) Καταγραφή

Σε ενιαίο μητρώο των πληροφοριακών και δικτυακών υποδομών, των συστημάτων του λογισμικού καθώς και των κατηγοριών αρχείων και δεδομένων που χρησιμοποιούνται και τηρούνται, καταγράφεται το σύνολο των κεντρικών πληροφοριακών πόρων του Πανεπιστημίου που σχετίζονται με την ασφάλεια πληροφοριών και την ασφάλεια προσωπικών δεδομένων.
Συγκεκριμένα, κάθε υπηρεσιακή οργανική μονάδα που διαθέτει και λειτουργεί υποδομή πληροφορικής και δικτύων με ευθύνη του διοικητικά υπεύθυνου της μονάδας και σε συνεργασία με τον υπεύθυνο ασφάλειας φροντίζει ώστε να καταγραφούν:

- Υπολογιστικός εξοπλισμός (εξυπηρετητές, σταθμοί εργασίας, συστήματα δίσκων) · Δικτυακός εξοπλισμός
- Συσκευές δικτυακής ασφάλειας
- Φορητές συσκευές
- Λειτουργικά συστήματα, ενδιάμεσο λογισμικό, βάσεις δεδομένων
- Εφαρμογές λογισμικού και πληροφοριακά συστήματα
- Δεδομένα / πληροφορίες (βάσεις δεδομένων, έντυπα ή ηλεκτρονικά έγγραφα, δεδομένα σε οπτικά ή μαγνητικά μέσα, κ.λπ..)
- Εγκαταστάσεις (γραφεία, Data Room, κ.λπ..)
- Βοηθητικά δίκτυα / υποστηρικτικά συστήματα (ηλεκτρικό ρεύμα, τηλεπικοινωνίες, κλιματισμός)
- Φυσικό αρχείο (εκτυπώσεις, πρωτότυπα έγγραφα)

Στη συνέχεια για κάθε πληροφοριακό πόρο καταγράφεται ο υπεύθυνος (ιδιοκτήτης) που σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων, καθορίζουν τα μέτρα που είναι απαραίτητα για την προστασία του πόρου (εξοπλισμός, λογισμικό ή πληροφορία).

Β) Διαχείριση φυσικού αρχείου

Σε κάθε υπηρεσιακή μονάδα πρέπει να εφαρμόζονται συγκεκριμένες διαδικασίες για την ορθή οργάνωση/αρχειοθέτηση/ταξινόμηση του φυσικού αρχείου (δηλ. του αρχείου με τους φυσικούς φακέλους).

Γ) Διαβάθμιση πληροφοριών

Για τις πληροφορίες και τα προσωπικά δεδομένα (ηλεκτρονικά αρχεία, έγγραφα) που διατηρούν και επεξεργάζονται οι υπηρεσιακές μονάδες πρέπει να οριστεί κατάλληλο σχήμα διαβάθμισης. Οι υπεύθυνοι των πόρων χαρακτηρίζουν τις πληροφορίες (δεδομένα) με ευθύνη του διοικητικά υπεύθυνου βάσει του είδους και της κρισιμότητάς τους και σύμφωνα με το ενδεικτικό σχήμα διαβάθμισης.

I. Δημόσιας Χρήσης
II. Εσωτερικά Αδιαβάθμητα
III.Εμπιστευτικά

Για κάθε κατηγορία διαβάθμισης ως προς την Ασφάλεια Πληροφοριών, θα πρέπει να οριστεί αναλυτικά ο τρόπος χειρισμού των πόρων (διαδικασία) από την υπηρεσιακή μονάδα (εκτός εάν προβλέπεται κεντρικά) και σε σχέση με το αντίστοιχο πληροφοριακό σύστημα (εάν χρησιμοποιείται),
ώστε να διαφυλάσσεται η εμπιστευτικότητα των πληροφοριών που περιέχουν και να ελαχιστοποιείται η πιθανότητα διαρροής.

Δ) Διακίνηση πληροφοριακών αγαθών

Κάθε υπηρεσιακή μονάδα με ευθύνη του διοικητικά υπεύθυνου θα τηρεί:

1. λίστα του μηχανογραφικού εξοπλισμού (προσωπικός υπολογιστής, φορητός, εκτυπωτής, εξωτερικός δίσκος, usb disk, κλπ) που παραχωρείται στους εργαζομένους της. Επιπλέον οι εργαζόμενοι θα υπογράφουν σε σχετική φόρμα κατά την παραλαβή αλλά και κατά την παράδοση (επιστροφή) του αντίστοιχου εξοπλισμού.
2. λίστα με τις κεντρικές εφαρμογές άλλων δημοσίων φορέων που έχει πρόσβαση και τους λογαριασμούς των εργαζομένων που συνδέονται σε αυτές. Επίσης στην ίδια λίστα συμπεριλαμβάνει τις υπηρεσίες cloud ή τις άλλες υπηρεσίες τρίτων που χρησιμοποιεί για τις ανάγκες της υπηρεσίας.

Σε περίπτωση που εξοπλισμός (π.χ. υπολογιστής ή USB) με προσωπικά δεδομένα μεταφέρεται εκτός των εγκαταστάσεων του Πανεπιστημίου, η ενέργεια αυτή πρέπει να καταγράφεται (ημερομηνία και ώρα εξόδου, πρόσωπο που χρησιμοποιεί τον εξοπλισμό, επιστροφή του εξοπλισμού).
Ιδιαίτερη προσοχή πρέπει να δοθεί από το προσωπικό στις παρακάτω περιπτώσεις διακίνησης ευαίσθητων πληροφοριών και προσωπικών δεδομένων:

· Τα έντυπα και τα μέσα αποθήκευσης με κρίσιμα προσωπικά δεδομένα, διακινούνται από και προς το Πανεπιστήμιο, με ειδικών προδιαγραφών φακέλους και πακέτα και καταγράφονται σε ειδικό πρωτόκολλο καταγραφής εισερχομένων/εξερχομένων.
· Τα έντυπα και τα μέσα αποθήκευσης με προσωπικά δεδομένα που διακινούνται εντός του Πανεπιστημίου, από γραφείο σε γραφείο ή μεταξύ οργανωτικών μονάδων επίσης καταγράφονται.
· Για την αποστολή ευαίσθητων πληροφοριών μέσω fax, πρέπει να γίνεται επιβεβαίωση ότι ο παραλήπτης βρίσκεται δίπλα στο fax, πριν την αποστολή τους.
· Κατά την εκτύπωση ευαίσθητων πληροφοριών σε κοινόχρηστους εκτυπωτές, όταν δεν μπορεί να αποφευχθεί, ο εργαζόμενος πρέπει να βρίσκεται δίπλα στον εκτυπωτή αμέσως μετά την αποστολή του αρχείου
· Η ηλεκτρονική αποστολή αρχείων με ευαίσθητα δεδομένα, θα πρέπει να πραγματοποιείται με χρήση ασφαλών μεθόδων, δηλαδή με χρήση κρυπτογραφημένου συνημμένου και αποστολή του κλειδιού κρυπτογράφησης (password) μέσω διαφορετικού καναλιού (τηλεφωνικά ή μέσω SMS).

6. Καταστροφή δεδομένων και αποθηκευτικών μέσων

Α) Διαδικασίες καταστροφής δεδομένων

Πριν από την καταστροφή εντύπων ή ηλεκτρονικών αρχείων που περιέχουν προσωπικά δεδομένα θα πρέπει να λαμβάνονται τα κατάλληλα μέτρα ώστε να διασφαλίζεται η πλήρης και μόνιμη διαγραφή των δεδομένων αυτών. Ειδικότερα, θα πρέπει να ακολουθούνται κατ' ελάχιστον όσα προβλέπονται στην Οδηγία 1/2005 της Αρχής για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας.
Στην περίπτωση προσωπικών δεδομένων που παράγονται ή/και χρησιμοποιούνται καθημερινά σε έντυπη μορφή στο πλαίσιο των εργασιών και τα οποία, μετά από την διεκπεραίωση της συγκεκριμένης εργασίας, είναι πλέον άχρηστα (π.χ. αντίγραφα, πρόχειρες εκθέσεις, σημειώσεις των υπαλλήλων, κ.α.) καταστρέφονται συστηματικά με χρήση καταστροφέων εγγράφων (shredders).
Σε περίπτωση απόσυρσης ή επαναχρησιμοποίησης πληροφοριακού εξοπλισμού (προσωπικοί υπολογιστές, δίσκοι, φορητά μέσα αποθήκευσης), επειδή η διαγραφή αρχείων ή και το format δίσκων δεν είναι επαρκή, θα πρέπει να πραγματοποιείται μόνιμη διαγραφή δεδομένων/αρχείων μέσω προχωρημένων τεχνικών (wipe, secure wipe, low level format) που θα εφαρμόζονται από εξειδικευμένο προσωπικό.

7. Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων

Α) Αναφορά Συμβάντων και Ευπαθειών Ασφάλειας

Τα μέλη της Ακαδημαϊκής Κοινότητας του Πανεπιστημίου γενικά και ειδικότερα το προσωπικό είναι υποχρεωμένο να αναφέρει οποιαδήποτε συμβάν και ευπάθεια αναγνωρίσει ή του αναφερθεί σε σχέση με την ασφάλεια πληροφοριών, όπως τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Η γνωστοποίηση θα γίνεται το συντομότερο δυνατόν, στον ΥΠΔ για την αξιολόγηση του συμβάντος και την πιθανή ενεργοποίηση των κατάλληλων διαδικασιών διαχείρισης περιστατικού ασφάλειας και την έγκαιρη εκτέλεση των προβλεπόμενων ενεργειών.

Β) Διαχείριση περιστατικών ασφάλειας

Για την διαχείριση περιστατικών ασφαλείας ακολουθείται η σειρά ενεργειών σύμφωνα με την σχετική διαδικασία που ειναι αναρτημένη στον ιστότοπο του ΥΠΔ του Πανεπιστημίου Δυτικής Μακεδονίας.

Β. Τεχνικά Μέτρα Ασφάλειας

1. Έλεγχος πρόσβασης

Α) Διαχείριση λογαριασμών χρηστών

Τα πληροφοριακά συστήματα και οι εφαρμογές πρέπει να διαθέτουν διαδικασίες για τη διαχείριση των λογαριασμών των χρηστών, οι οποίες πρέπει να περιλαμβάνουν κατ' ελάχιστο την προσθήκη, τη μεταβολή ιδιοτήτων και τη διαγραφή

λογαριασμού.

Η σύνδεση με την κεντρική υπηρεσία ταυτοποίησης και εξουσιοδότησης χρηστών, όπου αυτό είναι εφικτό σε οργανωτικό και τεχνικό επίπεδο, είναι επιβεβλημένη για λόγους εξοικονόμησης πόρων (σε προγραμματισμό και διαχείριση), βέλτιστης αξιοπιστίας και γενικευμένης χρήσης ενός κεντρικού λογαριασμού χρήστη.

Β) Μηχανισμοί ελέγχου πρόσβασης

Τα πληροφοριακά συστήματα και οι εφαρμογές θα πρέπει να διαθέτουν μηχανισμούς που να απαγορεύουν την πρόσβαση σε πόρους/υποσυστήματα/αρχεία από μη εξουσιοδοτημένους χρήστες: ουσιαστικά, πρέπει να διαθέτουν κατάλληλα μέτρα που να εξασφαλίζουν την εγγυημένα ορθή ταυτοποίηση και αυθεντικοποίηση των χρηστών, ενώ ταυτοχρόνως πρέπει να γίνεται σε τεχνικό επίπεδο συγκεκριμένη εκχώρηση δικαιωμάτων/εξουσιοδοτήσεων σε κάθε χρήστη.

Πρέπει να πραγματοποιείται από τους υπεύθυνους των πληροφοριακών συστημάτων περιοδικός έλεγχος (τουλάχιστον ετησίως) των δικαιωμάτων πρόσβασης και να λαμβάνονται τα απαραίτητα διορθωτικά μέτρα στις περιπτώσεις ύπαρξης λογαριασμών χρήστη με δικαιώματα που δεν αντιστοιχούν στο υφιστάμενο ρόλο του εργαζομένου.

Γ) Διαχείριση συνθηματικών

Η πολιτική διαχείρισης των συνθηματικών των χρηστών, περιλαμβάνει κανόνες αποδοχής για το ελάχιστο μήκος και τους επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του. Συγκεκριμένα τα συνθηματικά των χρηστών θα πρέπει:

1. Να έχουν μήκος τουλάχιστον 8 χαρακτήρων.
2. Να περιέχουν χαρακτήρες που να ανήκουν σε τουλάχιστον 3 από τις 4 ακόλουθες ομάδες: · Μικρά γράμματα.
    i. · Κεφαλαία γράμματα.
    ii. · Αριθμοί.
    iii. · Ειδικοί χαρακτήρες.
2. Να αλλάζουν οπωσδήποτε εντός διαστήματος μικρότερου του ενός έτους
3. Να μη συμπίπτουν με τα τελευταία 3 συνθηματικά χρήστη.

Οι χρήστες πρέπει να αλλάζουν οι ίδιοι το (προκαθορισμένο) συνθηματικό που τους ανατίθεται εξαρχής, καθώς επίσης να αλλάζουν όπως έχει αναφερθεί το συνθηματικό τους ανά τακτά χρονικά διαστήματα.

Η παραπάνω πολιτική σε σχέση με τα συνθηματικά των χρηστών (password policy) θα πρέπει να επιβληθεί μέσω του κεντρικού συστήματος διαχείρισης χρηστών και σε σύνδεση με τους επιμέρους μηχανισμούς ταυτοποίησης των χρηστών στις εφαρμογές και τα συστήματα. Όπου αυτό δεν είναι εφικτό στο σύνολό του ή σε μέρος του, είναι οι χρήστες αποκλειστικά υπεύθυνοι να συμμορφώνονται με τις βέλτιστες πρακτικές που επιβάλλει η πολιτική συνθηματικών.

Η ίδια πολιτική συνθηματικών πρέπει να ακολουθείται στους κωδικούς πρόσβασης διαχειριστών και χρηστών στους προσωπικούς υπολογιστές (σταθερούς, φορητούς), tablets και στις άλλες συσκευές.

Επίσης σε σχέση με τις πρακτικές που ακολουθούνται στη διαχείριση και χρήση των συνθηματικών από τους χρήστες **απαγορεύεται:**

1. οι προσωπικοί κωδικοί πρόσβασης χρηστών να γνωστοποιούνται σε άλλους χρήστες. Η συγκεκριμένη πρακτική ενέχει υψηλό κίνδυνο διαρροής των κωδικών και εμφάνισης περιστατικών μη εξουσιοδοτημένης πρόσβασης σε συστήματα, εφαρμογές και πληροφορίες, καθώς επίσης περιορίζει την αξιοπιστία του ελέγχου για το ποιος χρήστης έχει πρόσβαση σε ποιο πληροφοριακό πόρο.
2. οι κωδικοί πρόσβασης να συμπίπτουν με κωδικούς που χρησιμοποιούν οι εργαζόμενοι εκτός Πανεπιστημίου
3. να καταγράφονται οι κωδικοί πρόσβασης σε έντυπα μέσα
4. να αποθηκεύονται οι κωδικοί πρόσβασης σε ηλεκτρονική μορφή χωρίς να κρυπτογραφούνται.

Για τα συστήματα ή τις εφαρμογές όπου δεν μπορεί να εφαρμοστεί ένα password policy, οι χρήστες είναι υπεύθυνοι να συμμορφώνονται με τις βέλτιστες πρακτικές.

Δ) Μη επιτυχημένες προσπάθειες πρόσβασης

Καταγράφονται οι επιτυχημένες και οι αποτυχημένες προσπάθειες σύνδεσης των χρηστών σε όλα τα πληροφοριακά συστήματα. Η καταγραφή αυτή μπορεί να αξιοποιηθεί σε προληπτικούς ελέγχους ασφάλειας για προσπάθειες μη εξουσιοδοτημένης πρόσβασης και στη διερεύνηση περιστατικών ασφάλειας.

Ε) Αδρανοποιημένος υπολογιστής

Προς αποφυγή με εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα, με χρήση ανοιχτού υπολογιστή, ο οποίος μένει χωρίς επίβλεψη (έστω και για λίγα λεπτά) πρέπει ενεργοποιούνται: αυτόματη προφύλαξη της οθόνης (screen saver) του υπολογιστή (μετά από χρονικό διάστημα αδράνειας που προσδιορίζεται στα 10’) – για την απενεργοποίηση της οποίας θα απαιτείται χρήση συνθηματικού ή και αυτόματη διαδικασία αποσύνδεσης του χρήστη (μετά από χρονικό διάστημα αδράνειας

που προσδιορίζεται στα 60').

2. Αντίγραφα Ασφάλειας

Α) Λήψη και τήρηση αντιγράφων ασφάλειας

Πολιτική για τη λήψη και διαχείριση των αντιγράφων ασφάλειας πρέπει να εφαρμοσθεί σε όλους τους κεντρικούς κρίσιμους πόρους δηλαδή τα πληροφοριακά συστήματα, εφαρμογές, βάσεις δεδομένων, συστήματα, αρχεία, δεδομένα αρχείων χρηστών, αρχεία καταγραφής (log files).

Το αρμόδιο προσωπικό για την διαχείριση και προστασία του εκάστοτε κρίσιμου πληροφοριακού πόρου συντάσσει συγκεκριμένη πολιτική αντιγράφων ασφάλειας συμπεριλαμβάνοντας · τους κατάλληλους μηχανισμούς (τεχνολογίες, λογισμικό και αποθηκευτικά μέσα), · τη συχνότητα της δημιουργίας/λήψης των αντιγράφων ασφάλειας (ανά τακτά διαστήματα, σε ημερήσια ή εβδομαδιαία βάση, ανάλογα με το μέγεθος και το είδος των δεδομένων, καθώς και με το πότε αυτά μεταβάλλονται),

- τη κατάλληλη επισήμανση αυτών,
- την ασφαλή αποθήκευσή τους,
- την ορθή ανάκτηση των δεδομένων από τα αντίγραφα ασφάλειας,
- τον περιοδικό έλεγχο ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται

Πολιτική λήψης αντιγράφων ασφάλειας εφαρμόζεται και στους σταθμούς εργασίας του προσωπικού που επεξεργάζεται προσωπικά δεδομένα, και στην περίπτωση που τα αντίγραφα αποθηκεύονται σε φορητά μέσα, ακόμη και εντός του χώρου εργασίας, τότε αυτά υποχρεωτικά κρυπτογραφούνται για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση.

Β) Τόπος τήρησης

Επιλεγμένα αντίγραφα ασφάλειας πρέπει να διατηρούνται σε διαφορετικό χώρο/φυσική τοποθεσία από το χώρο των πρωτογενών δεδομένων, δηλαδή να φυλάσσονται σε άλλο ασφαλή χώρο εντός του Πανεπιστημίου και να λαμβάνονται μέτρα για την ασφαλή μεταφορά τους. Η φύλαξη αντιγράφων ασφάλειας εκτός των κύριων κτιριακών εγκαταστάσεων του Πανεπιστημίου θα διευκολυνθεί με την δημιουργία και λειτουργία Κέντρου Δεδομένων σε εναλλακτικό χώρο (DR Datacenter), που επιπλέον θα εξασφαλίσει την επιχειρησιακή συνέχεια σε περιπτώσεις καταστροφικών γεγονότων στο (π.χ. πυρκαγιά, πλημμύρα κ.λπ.)..

3. Διαμόρφωση υπολογιστών

Α) Ενιαίο σχήμα διαχείρισης και εφαρμογή της πολιτικής ασφάλειας

Εφαρμόζεται ενιαία πολιτική ασφάλειας στους προσωπικούς υπολογιστές του προσωπικού στο σύνολο των υποδικτύων των διοικητικών υπηρεσιών μέσω υποδομής Active Directory. Κάθε υπολογιστής είναι ενταγμένος στο σύστημα ενιαίας διαχείρισης χρηστών (AD), προκειμένου να εφαρμόζονται καθολικά, σε επίπεδο χρήστη, ομάδας, τμήματος ή διεύθυνσης, οι ρυθμίσεις ασφάλειας πληροφοριών, η επιτρεπτή χρήση προγραμμάτων, η χρήση υπολογιστικών και δικτυακών πόρων (π.χ. εκτυπωτές, δικτυακή δίσκοι, backup).

Η υποδομή AD αξιοποιεί το σύστημα πλήρους διαχείρισης του κύκλου ζωής των προσωπικών λογαριασμών μέσω της σύνδεσής του με το κεντρικό LDAP.

Β) Προστασία από κακόβουλο λογισμικό

Πρέπει να υπάρχει προστασία από κακόβουλο λογισμικό όλων των υπολογιστών, τόσο των προσωπικών υπολογιστών του προσωπικού όσο και των εξυπηρετητών. Αυτό επιτυγχάνεται (πέραν της σωστής χρήσης αυτών από το προσωπικό) με αντιικά προγράμματα (antivirus), καθώς και με χρήση προγραμμάτων τειχών ασφάλειας (firewall). Σε κάθε προσωπικό υπολογιστή με ευθύνη του αρμόδιου προσωπικού υποχρεωτικά εγκαθίσταται και λειτουργεί antivirus και firewall, τα οποία πρέπει να διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις. Επιπλέον, στο λειτουργικό σύστημα των υπολογιστών (εφόσον είναι συνδεδεμένοι στο Διαδίκτυο) πρέπει να εγκαθίστανται σε τακτά χρονικά διαστήματα οι ενημερώσεις ασφάλειας.

Στους υπολογιστές που τηρούν ή επεξεργάζονται ευαίσθητες πληροφορίες ή προσωπικά δεδομένα πρέπει να λειτουργεί λογισμικό πλήρους προστασίας τελικού σημείου (Endpoint Protection) του οποίου η λειτουργία καθορίζεται αυτόματα από κεντρική πολιτική προστασίας, για να περιοριστεί η πιθανότητα λάθους στην χρήση του και να εξαλειφθεί ο κίνδυνος μόλυνσής τους με κακόβουλο λογισμικό. Το προσωπικό (οι χρήστες) θα ενημερωθεί και θα εκπαιδευτεί στο λογισμικό Endpoint Protection και στους ελέγχους που πρέπει να εκτελεί όταν λαμβάνει αρχεία που προέρχονται από εξωτερικά δίκτυα ή φορητά μέσα αποθήκευσης.

Γ) Ρυθμίσεις υπολογιστών

Στους υπολογιστές του προσωπικού που λειτουργούν ανεξάρτητα επιτρέπεται η σύνδεση με διαχειριστικούς λογαριασμούς μόνο στο αρμόδιο προσωπικό διαχείρισης. Οι εργαζόμενοι συνδέονται μόνο με δικαιώματα απλού χρήστη και χωρίς δυνατότητες ενεργειών που μπορεί να επηρεάσουν την συνολική λειτουργία και διαμόρφωση π.χ. απενεργοποίηση αντιικών προγραμμάτων, εγκατάσταση νέων προγραμμάτων ή αλλαγή ρυθμίσεων υπαρχόντων, κ.λπ.. Στους υπολογιστές αυτούς πρέπει να γίνεται από το αρμόδιο προσωπικό περιοδικός έλεγχος του εγκατεστημένου λογισμικού για τον τυχόν εντοπισμό προγραμμάτων που έχουν εγκατασταθεί με βάση εγκεκριμένες διαδικασίες.
Επίσης πρέπει να ληφθεί υπόψη ότι η χρήση λογαριασμών με κλιμακούμενα δικαιώματα (όχι πλήρους διαχείρισης) στους ανεξάρτητους υπολογιστές βελτιώνει το επίπεδο ασφάλειας, ειδικά στις περιπτώσεις που συγκεκριμένες εφαρμογές έχουν σαν προϋπόθεση για την λειτουργία τους επαυξημένα δικαιώματα χρήστη.

Δ) Σύνδεση αποσπώμενων μέσων

Οι ηλεκτρονικοί υπολογιστές που χρησιμοποιούνται από τους τελικούς χρήστες δεν πρέπει να διαθέτουν δυνατότητα εξαγωγής δεδομένων σε αποσπώμενα μέσα (π.χ. USB, CD/DVD), εκτός αν υπάρχει σχετική έγκριση από την υπηρεσία.

Ε) Υπολογιστές με πρόσβαση στο Διαδίκτυο

Δεν πρέπει να αποθηκεύονται προσωπικά δεδομένα ειδικών κατηγοριών σε υπολογιστές που έχουν σύνδεση με το διαδίκτυο (εκτός αν κάτι τέτοιο είναι απολύτως απαραίτητο στο πλαίσιο του ρόλου/αρμοδιοτήτων που έχουν ανατεθεί στο χρήστη του υπολογιστή).

4. Αρχεία καταγραφής (log files)

Α) Τήρηση και έλεγχος αρχείων καταγραφής

Στα κρίσιμα συστήματα τηρούνται από το αρμόδιο προσωπικό (διαχειριστές) και ελέγχονται σε τακτά χρονικά διαστήματα, τα αρχεία καταγραφής των ενεργειών (log files) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων που σχετίζονται με την ασφάλεια.
Πρόσβαση στα αρχεία αυτά, εκτός από τους διαχειριστές συστημάτων, δύναται να έχουν ο Υπεύθυνος Ασφάλειας, και όποια άλλα μέλη του προσωπικού είναι επιφορτισμένα με αρμοδιότητες διαχείρισης περιστατικών ασφάλειας κατόπιν κατάλληλης εξουσιοδότησης.

Β) Διαγραφή αρχείων καταγραφής

Τα αρχεία καταγραφής ενσωματώνονται στην πολιτική λήψης αντιγράφων ασφάλειας και δεν διαγράφονται χωρίς κατάλληλη έγκριση και πριν την πάροδο χρονικού διαστήματος δύο τουλάχιστον ετών, το οποίο καθορίζεται επακριβώς από τον υπεύθυνο του συστήματος σε συνεργασία με τον Υπεύθυνο Ασφάλειας.

5. Ασφάλεια επικοινωνιών

Α) Ασφάλεια Δικτύων

Το δίκτυο του Πανεπιστημίου διαχωρίζεται από τα εξωτερικά δίκτυα και λόγω τους μεγέθους του έχει κατατμηθεί σε υποδίκτυα ή/και ζώνες ασφάλειας με στόχο την αποτελεσματική προστασία των πληροφοριακών πόρων. Διαθέτει μηχανισμούς και συστήματα ασφάλειας (ενδεικτικά αναφέρονται: αναχώματα ασφάλειας (firewall), συστήματα ανίχνευσης και αποτροπής εισβολών (IPS), λίστες ελέγχου πρόσβασης (ACL), ιδεατά ιδιωτικά δίκτυα), των οποίων η λειτουργία και η τεχνική διαμόρφωση λαμβάνει υπόψη τις διεθνείς, ευρέως αποδεκτές πρακτικές και πρότυπα. Το αρμόδιο προσωπικό σε συνεννόηση με τον Υπεύθυνο Ασφάλειας παραμετροποιεί και διαμορφώνει τους προαναφερόμενους μηχανισμούς και συστήματα για την άμεση εφαρμογή των απαραίτητων μέτρων και την αποτελεσματική προστασία του δικτύου, των προσωπικών δεδομένων και πληροφοριών.

Β) Απομακρυσμένη πρόσβαση

Η απομακρυσμένη πρόσβαση σε κρίσιμα συστήματα και εφαρμογές επιτρέπεται μόνο μέσω ασφαλών καναλιών με ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση (όπως VPN). Η σύνδεση με προγράμματα πρόσβασης όπως Remote Desktop, VNC, κ.λπ. επιτρέπονται μόνο σε εξουσιοδοτημένο προσωπικό και πάνω από το προβλεπόμενο για την περίπτωση VPN. Για την περαιτέρω μείωση του κινδύνου διαρροής δεδομένων ή μη εξουσιοδοτημένης πρόσβασης, προτείνεται η χρήση 2FA (Two Factor Authentication) κατά την σύνδεση μέσω VPN.

Γ) Πρωτόκολλα δικτύου

Είναι υποχρεωτική η χρήση ασφαλών πρωτοκόλλων επικοινωνίας στο δίκτυο, όπως HTTPS, SFTP, SSH, SMTPS, IMAPS. Τα πληροφοριακά συστήματα και οι εφαρμογές με διεπαφή παγκόσμιου ιστού πρέπει να λειτουργούν αποκλειστικά μέσω ασφαλούς (κρυπτογραφημένου) καναλιού (SSL/HTTPS), καθώς επίσης και οι ιστοσελίδες που περιλαμβάνουν φόρμες υποβολής προσωπικών δεδομένων.
Επίσης η μετάδοση των κωδικών πρόσβασης πάνω από το δίκτυο από εφαρμογές, στη φάση της σύνδεσης των χρηστών τους, πρέπει να γίνεται με κρυπτογράφηση, όπου είναι δυνατόν.

Δ) Ζώνες ασφάλειας

Τα συστήματα που υποστηρίζουν και λειτουργούν υπηρεσίες ευρέως προσβάσιμες από το διαδίκτυο τοποθετούνται σε συγκεκριμένες ζώνες ασφάλειας για την καλύτερη προστασία των πληροφοριών και των προσωπικών δεδομένων με την αξιοποίηση μηχανισμών και συστημάτων δικτυακής ασφάλειας.
Σε κάθε περίπτωση καταγράφεται η αρχιτεκτονική που έχει υλοποιηθεί, οι πληροφοριακοί πόροι που έχουν τοποθετηθεί στη ζώνη κι η πολιτική ασφάλειας που εφαρμόζεται στους σχετικούς μηχανισμούς και τα συστήματα που χρησιμοποιούνται.

Ε) Πρόσβαση χρηστών σε υπηρεσίες και εφαρμογές διαδικτύου τρίτων

Η πρόσβαση σε συγκεκριμένες υπηρεσίες και εφαρμογές του διαδικτύου (internet) τρίτων παρόχων από υποδίκτυα υπολογιστών των κεντρικών διοικητικών υπηρεσιών μπορεί να περιοριστεί ή και να απαγορευτεί μέσω των μηχανισμών και συστημάτων ασφάλειας, εάν θέτει αποδεδειγμένα σε κίνδυνο προσωπικά δεδομένα και ευαίσθητες πληροφορίες.

ΣΤ) Αρχεία καταγραφής (logs)

Οι κρίσιμες δικτυακές και υπολογιστικές υποδομές (εξοπλισμός, σχετικό λογισμικό) είναι υποχρεωτικό να συνδέονται με ασφάλεια και να ενημερώνουν κεντρικό σύστημα συλλογής και καταγραφής συμβάντων, όπου αυτό είναι τεχνικά εφικτό. Έτσι επιτυγχάνεται ο βέλτιστος κεντρικός έλεγχος των συμβάντων και η ολοκληρωμένη αξιολόγησή τους σε σχέση με την ασφάλεια των δικτυακών και πληροφοριακών πόρων.

6. Αρχεία σε αποσπώμενα μέσα αποθήκευσης και στο δίκτυο

Α) Χρήση κρυπτογράφησης

Η προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών και των προσωπικών δεδομένων βελτιώνεται σε μεγάλο βαθμό με την χρήση κρυπτογραφικών τεχνικών και προγραμμάτων.
Στους προσωπικούς υπολογιστές του προσωπικού πρέπει να λειτουργεί λογισμικό κρυπτογράφησης, το οποίο θα χρησιμοποιείται υποχρεωτικά για την προστασία αρχείων με ευαίσθητες πληροφορίες και προσωπικά δεδομένα, ειδικά στις παρακάτω περιπτώσεις:

1) αποθήκευση αρχείων σε φορητά μέσα (π.χ. USB δίσκους κ.ο.κ.), αφού για αυτές τις περιπτώσεις ο κίνδυνος διαρροής δεδομένων αυξάνεται.
2) αποθήκευση αρχείων στο cloud ή σε ιστότοπους που προσφέρουν υπηρεσίες αποθήκευσης 3) αποθήκευση αρχείων σε κοινόχρηστους φακέλους

Σε περιπτώσεις ύπαρξης αναγκών πρόσβασης από περισσότερους από ένα εργαζόμενο σε κρυπτογραφημένα αρχεία ή folder, εγκαθίσταται στους υπολογιστές των χρηστών κατάλληλο λογισμικό κρυπτογράφησης με αυτά τα ειδικά χαρακτηριστικά.
Στους υπολογιστές που γίνεται επεξεργασία προσωπικών δεδομένων ειδικών κατηγοριών εγκαθίσταται υποχρεωτικά, από εξειδικευμένο προσωπικό, λογισμικό κρυπτογράφησης (Endpoint Encryption) του οποίου η λειτουργία καθορίζεται από κεντρική πολιτική προστασίας και εκπαιδεύεται σε αυτό ο χρήστης.
Επίσης η χρήση κρυπτογραφικών προγραμμάτων προτείνεται στις περιπτώσεις: ·

- στην ηλεκτρονική αποθήκευση κωδικών πρόσβασης
- στην αποστολή συνημμένων αρχείων που περιέχουν ευαίσθητες πληροφορίες (π.χ. προσωπικά δεδομένα) μέσω email
- στους σκληρούς δίσκους των φορητών υπολογιστών ώστε να ελαχιστοποιείται ο κίνδυνος διαρροής πληροφοριών ή μη εξουσιοδοτημένης πρόσβασης σε περίπτωση κλοπής ή απώλειας της συσκευής.

Β) Αρχεία σε δίκτυα

Τα αρχεία με κρίσιμες πληροφορίες και προσωπικά δεδομένα προτείνεται να αποθηκεύονται από τον χρήστη του υπολογιστή σε κεντρικό σύστημα δικτυακών δίσκων, κατάλληλα διαμορφωμένο ως προς

την ασφάλεια και τα δικαιώματα πρόσβασης σε επίπεδο δίσκου, καταλόγων και αρχείων. Στο ίδιο σύστημα (σε άλλους όμως δικτυακούς δίσκους) προτείνεται να αποθηκεύονται τα κοινά αρχεία ή τα αρχεία που ανταλλάσσονται μεταξύ του προσωπικού του ίδιου τμήματος ή της ίδιας διεύθυνσης.
Η χρήση εφαρμογών διαδικτύου αποθήκευσης και ανταλλαγής αρχείων (cloud storage) για υπηρεσιακούς σκοπούς, όπως dropbox, Gdirve,Onedrive, WeTransfer κλπ απαγορεύεται εκτός εάν υπάρχει σχετική σύμβαση/συμφωνία του Πανεπιστημίου με τον πάροχο της υπηρεσίας.

7. Ασφάλεια λογισμικού

Α) Σχεδιασμός εφαρμογών

Ο σχεδιασμός των εφαρμογών που χρησιμοποιούνται στην επεξεργασία προσωπικών δεδομένων πρέπει να πραγματοποιείται λαμβάνοντας υπόψη τις βασικές αρχές της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας (privacy by design). Ως εκ τούτου, οι εφαρμογές πρέπει να ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων (data minimization), καθώς και της ποιότητας των δεδομένων και να περιλαμβάνουν τη δυνατότητα της διαγραφής δεδομένων μετά το χρονικό διάστημα που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Επίσης, πρέπει να επιτρέπουν την υλοποίηση όλων των απαιτούμενων τεχνικών μηχανισμών ασφάλειας για την προστασία των δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

Β) Ασφαλής ανάπτυξη εφαρμογών

Σε περίπτωση ανάπτυξης εφαρμογών, είτε εσωτερικά στον οργανισμό είτε από εξωτερικό συνεργάτη, θα πρέπει να προβλέπεται μεθοδολογία ασφαλούς ανάπτυξης λογισμικού, ώστε να αποφευχθούν τυχόν ευπάθειες αυτού ως προς την ασφάλεια προτού αυτό υλοποιηθεί.
Η εσωτερική ανάπτυξη εφαρμογών γίνεται αποκλειστικά σε κατάλληλα διαμορφωμένο, ανεξάρτητο, συνεργατικό προγραμματιστικό περιβάλλον και με βάση συγκεκριμένη μεθοδολογία ανάπτυξης κώδικα.
Στις περιπτώσεις όπου η ανάπτυξη των εφαρμογών γίνεται από εξωτερικό συνεργάτη, θα πρέπει να υπάρχουν προδιαγραφές ασφάλειας της εφαρμογής στο έγγραφο περιγραφής απαιτήσεων λογισμικού, το οποίο θα εμπεριέχεται στη σύμβαση με τον εκάστοτε ανάδοχο.

Γ) Αναβάθμιση λογισμικού

Το εμπορικό λογισμικό και το λογισμικό των κεντρικών υπολογιστικών και δικτυακών υποδομών πρέπει να ενημερώνεται συχνά με τις νέες εκδόσεις ασφάλειας μέσω των προβλεπόμενων διαδικασιών αναβάθμισης. Ως εκ τούτου θα πρέπει να διασφαλίζεται η συνέχεια της άδειας χρήσης του εμπορικού λογισμικού μέσω έγκαιρης σύναψης συμβάσεων συντήρησης για τη παροχή των νέων εκδόσεων, ενημερώσεων και τεχνικής υποστήριξης. Σε περίπτωση που υπάρχει ενημέρωση ότι σταματά η υποστήριξη συγκεκριμένου λογισμικού τότε προγραμματίζεται από το αρμόδιο τμήμα η άμεση αντικατάστασή του με νέα έκδοση του ίδιου λογισμικού (major upgrade, θεωρείται νέο/άλλο λογισμικό) ή με αντίστοιχο λογισμικό.

8. Διαχείριση αλλαγών

Α) Πολιτική διαχείρισης αλλαγών

Ο υπεύθυνος κάθε πληροφοριακού συστήματος έχει την ευθύνη της διαχείρισης των αλλαγών (Change Management) σε αυτό και οφείλει να μεριμνά κατ’ ελάχιστον για:

- την καταγραφή των αιτημάτων αλλαγής.
- τον καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών
- τον καθορισμό των κριτηρίων αποδοχής της αλλαγής
- το χρονοδιάγραμμα υλοποίησης

Ευθύνη του υπεύθυνου να ακολουθείται συγκεκριμένη διαδικασία διαχείρισης αλλαγών σύμφωνα με τα παρακάτω βήματα:

1. Ενέργειες που απαιτούνται για την υλοποίηση της αλλαγής
2. Αξιολόγηση των πιθανών επιπτώσεων στη λειτουργικότητα και στην ασφάλεια πληροφοριών. 3. Πλάνο επαναφοράς σε προηγούμενη κατάσταση σε περίπτωση αποτυχίας υλοποίησης της αλλαγής.
3. Ενέργειες δοκιμών.
4. Αποτελέσματα δοκιμών.
5. Έγκριση αλλαγών.

Γ. Μέτρα Φυσικής Ασφάλειας

1. Έλεγχος φυσικής πρόσβασης

Α) Φυσική πρόσβαση σε εγκαταστάσεις και computer room

Στους χώρους που βρίσκεται κεντρικός υπολογιστικός και δικτυακός εξοπλισμός (συμπεριλαμβανομένης της δικτυακής καλωδίωσης) εφαρμόζονται κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης, έτσι ώστε να επιτρέπεται η πρόσβαση μόνο σε κατάλληλα εξουσιοδοτημένο προσωπικό, για παράδειγμα χώροι που βρίσκεται περιφερειακός δικτυακός ενεργητικός και παθητικός εξοπλισμός πρέπει να είναι μόνιμα κλειδωμένοι.
Στις περιπτώσεις των Κέντρων Δεδομένων (Data centers) και των Κέντρων Δικτύων (Network centers), λόγω της φύσης του εξοπλισμού, των δεδομένων και των υπαρχόντων κινδύνων, είναι απαραίτητο να ελέγχεται και να καταγράφεται κάθε πρόσβαση στους συγκεκριμένους χώρους.

Β) Τήρηση καταλόγου

Διατηρείται με ευθύνη του διοικητικά και τεχνικά υπεύθυνου επικαιροποιημένος κατάλογος με τα δικαιώματα φυσικής πρόσβασης του προσωπικού καθώς και με το προσωπικό που διαθέτει κωδικούς, κάρτες εισόδου και κλειδιά για πρόσβαση σε χώρους που λειτουργεί ο κεντρικός υπολογιστικός και δικτυακός εξοπλισμός και οι κτιριακοί κατανεμητές δικτύου. Οι κατάλογοι αυτοί υπόκεινται σε τακτική αναθεώρηση.

2. Περιβαλλοντική ασφάλεια

Α) Προστασία από φυσικές καταστροφές

Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για την προστασία των κτιρίων, των κρίσιμων χώρων, των computer rooms, των γραφείων του προσωπικού, του εξοπλισμού πληροφορικής και του χώρου τήρησης φυσικού αρχείου από ζημιές που μπορούν να προκληθούν από φυσικές καταστροφές ή κακόβουλες ενέργειες, όπως πλημμύρα, υπερθέρμανση, πυρκαγιά, σεισμός, έκρηξη, διαρροή νερού, διακοπή ρεύματος, διάρρηξη/κλοπή, βανδαλισμός, κ.λπ.
Ενδεικτικά μέτρα που πρέπει να τηρούνται προς αυτή την κατεύθυνση είναι τα εξής: συναγερμός, πόρτες και παράθυρα ασφάλειας, πυροπροστασία, απομάκρυνση εξοπλισμού από υδροσωληνώσεις και πηγές σκόνης, ανιχνευτές υγρασίας και πλημμύρας, αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών, κ.λπ.

3. Έκθεση εγγράφων

Α) Τοποθέτηση φακέλων

Οι φάκελοι που περιέχουν προσωπικά δεδομένα (φυσικό αρχείο) πρέπει να είναι τοποθετημένοι σε φωριαμούς που να μπορεί να κλειδώνουν και να μην εκτίθενται σε κοινή θέα.

Β) Μεταφορά φακέλων

Θα πρέπει να καταγράφεται η μεταφορά των φυσικών φακέλων σε διαφορετικά γραφεία ή σε άλλες υπηρεσιακές μονάδες.

Γ) Clean desk policy

Δεν θα πρέπει να αφήνονται εκτεθειμένα, χωρίς επίβλεψη, έγγραφα και φορητά μέσα αποθήκευσης πάνω σε γραφεία.

Δ) Συσκευές αναπαραγωγής εγγράφων

Λοιπές συσκευές που δύναται να χρησιμοποιηθούν για υποκλοπή ή για την έκθεση προσωπικών δεδομένων σε κοινή θέα, όπως φωτοαντιγραφικά, συσκευές fax, εκτυπωτές, κ.λπ. θα πρέπει να προστατεύονται κατάλληλα.

4. Προστασία φορητών μέσων αποθήκευσης

Α) Ασφάλεια φορητών μέσων

Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για τη φυσική ασφάλεια και προστασία των φορητών αποθηκευτικών μέσων - όπως να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση και να είναι πάντα υπό επίβλεψη κατά τη διάρκεια της χρήσης τους.