ΟΔΗΓΟΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΜΕΤΡΑ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΜΑΪΟΣ 2019

Σχέδιο Ασφάλειας (Security Plan)

Το Σχέδιο Ασφάλειας (Security Plan) είναι το έγγραφο στο οποίο περιγράφονται τα οργανωτικά και τεχνικά μέτρα, καθώς και τα μέτρα φυσικής ασφάλειας που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν με ακρίβεια για την προστασία των πληροφοριών και των προσωπικών δεδομένων, ευαίσθητων και μη, που τηρούνται από το Πανεπιστήμιο Πατρών, καθώς και οι απαραίτητες ενέργειες για την υλοποίησή τους.

Το Σχέδιο Ασφάλειας συντάχθηκε με βάση το πρότυπο της "Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα", τα παραδοτέα του έργου παροχής υπηρεσιών "Εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων στο Πανεπιστήμιο Πατρών και παροχή υπηρεσιών Υπεύθυνου Προστασίας Δεδομένων" Μελέτη συμμόρφωσης και Μελέτη επικινδυνότητας - εκτίμησης αντίκτυπου και την κείμενη νομοθεσία.

Το Σχέδιο αυτό έχει το χαρακτήρα του επείγοντος λόγω της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ-GDPR) και θα ισχύει μέχρι το Πανεπιστήμιο να εφαρμόσει Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με το πρότυπο ISO 27K και Σχεδίου Επιχειρησιακής Συνέχειας.

Το Σχέδιο Ασφάλειας αποτελείται από την περιγραφή του συστήματος επεξεργασίας προσωπικών δεδομένων του Πανεπιστημίου, τα οργανωτικά, τα τεχνικά μέτρα ασφάλειας, τα μέτρα φυσικής ασφάλειας που εφαρμόζονται, μέτρα ανάκαμψης από καταστροφές και το πλάνο υλοποίησης και εφαρμογής των μέτρων ασφάλειας.

I) Περιγραφή του συστήματος επεξεργασίας προσωπικών δεδομένων

Σύντομη περιγραφή της τεχνολογικής υποδομής και των πληροφοριακών συστημάτων που υποστηρίζουν την επεξεργασία των προσωπικών δεδομένων συμπεριλαμβάνεται στο Παράρτημα Ι.

II) Μέτρα Ασφάλειας

Περιγράφονται τα μέτρα ασφάλειας που εφαρμόζονται από το Πανεπιστήμιο Πατρών και εντάσσονται στις παρακάτω τρεις κύριες κατηγορίες:

Α. Οργανωτικά Μέτρα Ασφάλειας

1. Υπεύθυνος Ασφάλειας
2. Οργάνωση / Διαχείριση προσωπικού
3. Διαχείριση πληροφοριακών αγαθών
4. Καταστροφή δεδομένων και αποθηκευτικών μέσων
5. Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων
6. Εκπαίδευση προσωπικού
7. Έλεγχος

Β. Τεχνικά Μέτρα Ασφάλειας

1. Έλεγχος πρόσβασης
2. Αντίγραφα ασφάλειας

3. Διαμόρφωση υπολογιστών
4. Αρχεία καταγραφής ενεργειών χρηστών και συμβάντων ασφάλειας
5. Ασφάλεια επικοινωνιών
6. Αρχεία σε αποσπώμενα μέσα αποθήκευσης και στο δίκτυο
7. Ασφάλεια λογισμικού
8. Διαχείριση αλλαγών

Γ. Μέτρα Φυσικής Ασφάλειας

1. Έλεγχος φυσικής πρόσβασης
2. Περιβαλλοντική ασφάλεια
3. Έκθεση εγγράφων
4. Προστασία φορητών μέσων αποθήκευσης

Δ. Βασικά μέτρα ανάκαμψης από καταστροφές

Αναλυτικότερα τα μέτρα ασφάλειας κατά κατηγορία:

Α. ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

1. Υπεύθυνος Ασφάλειας

Α) Ορισμός Υπεύθυνου Ασφάλειας
Με βάση το πρότυπο ISO27K που ακολουθήθηκε στην μελέτη συμμόρφωσης (compliance plan) προβλέπεται ορισμός διακριτής θέσης υπεύθυνου ασφάλειας (ή, ενδεχομένως, αντίστοιχης ομάδας ατόμων) εντός του Πανεπιστημίου με αρχικές αρμοδιότητες την επίβλεψη και τον έλεγχο της εφαρμογής του σχεδίου ασφάλειας και των μέτρων ασφάλειας πληροφοριών.

2. Οργάνωση/Διαχείριση προσωπικού

Α) 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.

Β) 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.

Γ) 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.

Δ) 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.

3. 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 Ασφάλειας, καθορίζουν τα μέτρα που είναι απαραίτητα για την προστασία του πόρου (εξοπλισμός, λογισμικό ή πληροφορία).

Κατά την καταγραφή των πόρων ιδιαίτερη προσοχή δίνεται, ανάλογα με το είδος του πόρου (σύστημα, εφαρμογή, αρχείο, κλπ) , στις ορισμένες κατηγορίες χρηστών και τα δικαιώματα πρόσβασης και εκτέλεσης ενεργειών που αποδίδονται σε αυτές. Καταγράφεται επίσης η αντιστοίχιση των ορισμένων στο σύστημα εργαζομένων με την πρόσβαση και τις ενέργειες που μπορούν να εκτελέσουν, είτε αυτή πραγματοποιείται από προσωπικό λογαριασμό πρόσβασης είτε από κοινό ή προκαθορισμένο λογαριασμό. Επίσης καταγράφεται η διαδικασία διαχείρισης χρηστών, στην οποία περιγράφεται κάθε περίπτωση προσθήκης, αλλαγής ή διαγραφής χρηστών και η απονομή και η μεταβολή των δικαιωμάτων ή επιπέδων πρόσβασης.

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).

Στα ψηφιακά μέσα αποθήκευσης πρέπει να τοποθετείται σήμανση, η οποία θα υποδηλώνει το επίπεδο της διαβάθμισης της πληροφορίας που εμπεριέχεται.

Σε περιπτώσεις που μεταφέρονται διαβαθμισμένες πληροφορίες πρέπει να χρησιμοποιούνται συγκεκριμένοι μεταφορείς για την αποστολή εντύπων και ψηφιακών μέσων αποθήκευσης εκτός του Πανεπιστημίου.

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).

4. 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.

5. 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 Υπεύθυνο Ασφάλειας 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
Ο Υπεύθυνος Ασφάλειας ενημερώνει τον ΥΠΔ και εφόσον το γνωστοποιημένο συμβάν αφορά προσωπικά δεδομένα τότε το αξιολογούν από κοινού. Σε περίπτωση που το συμβάν αφορά παραβίαση προσωπικών δεδομένων ο ΥΠΔ ακολουθεί την διαδικασία Διαχείρισης Παραβιάσεων Προσωπικών Δεδομένων (Δ 04).

Ο Υπεύθυνος Ασφάλειας εφαρμόζει τη διαδικασία Διαχείρισης Περιστατικών Ασφάλειας, η οποία ενεργοποιείται αμελλητί σε κάθε περίπτωση που αξιολογηθεί θετικά η αναφορά συμβάντος ασφάλειας και προβλέπει τις ακόλουθες ενέργειες:

- τον καθορισμό των ρόλων των εργαζομένων που θα συμμετάσχουν στην αντιμετώπιση του περιστατικού ασφάλειας (παραλείπεται στην περίπτωση ορισμού Ομάδας Αντιμετώπισης Περιστατικών Ασφάλειας),
- την καταγραφή στοιχείων για κάθε περιστατικό ασφάλειας,
- τη διερεύνηση των αιτιών και τον προσδιορισμό των τεχνικών ή/και οργανωτικών αδυναμιών στις οποίες ενδεχομένως οφείλεται το περιστατικό ασφάλειας,
- την υλοποίηση των ενεργειών αποκατάστασης με συγκεκριμένο χρονοδιάγραμμα ,
- την ενημέρωση των αρμοδίων διοικητικών οργάνων,
- τη διατήρηση των πληροφοριών (έγγραφα ή/και αρχεία) που σχετίζονται με το περιστατικό ασφάλειας, ώστε να τεκμηριώνεται η εκτέλεση των αντίστοιχων προβλεπόμενων ενεργειών .

Ο Υπεύθυνος Ασφάλειας δημιουργεί και συντηρεί μια λίστα (ηλεκτρονική ή μη, ανά τμήμα ή συνολικά) που να περιλαμβάνει τις αρχές, τους οργανισμούς, τους εργαζόμενους, τους συνεργάτες τους ερευνητές που μπορεί να συμμετάσχουν (εμπλακούν) στην αντιμετώπιση ενός Περιστατικού Ασφάλειας Πληροφοριών.

Κάθε συμβάν καταγράφεται σε αρχείο, που περιλαμβάνει τη χρονική στιγμή που έλαβε χώρα, το πρόσωπο που το ανέφερε, σε ποιον το ανέφερε, εκτίμηση των συνεπειών και της κρισιμότητας του περιστατικού, διαδικασίες ανάκαμψης/διόρθωσης που ακολουθήθηκαν, καθώς και ενδεχόμενη διαδικασία ενημέρωσης των θιγομένων ατόμων ανάλογα με την έκταση του περιστατικού, κ.ο.κ.

Προβλέπεται διαδικασία ανασκόπησης της διαχείρισης του περιστατικού ασφάλειας μετά το πέρας των ενεργειών αντιμετώπισής του. Στο σημείο αυτό θα γίνεται αξιολόγηση των μεθόδων αντιμετώπισης καθώς και αναφορά των μέτρων που ελήφθησαν για την αποτροπή μελλοντικών συμβάντων.

6. Εκπαίδευση προσωπικού

Α) Βασική εκπαίδευση
Το Πανεπιστήμιο πρέπει να διοργανώνει εκπαιδευτικά σεμινάρια μία τουλάχιστον φορά κατά έτος σε χώρο της Πανεπιστημιούπολης, με σκοπό την ορθή εφαρμογή των προβλεπόμενων οργανωτικών και τεχνικών μέτρων ασφάλειας. Η εκπαίδευση θα καλύπτει θέματα προστασίας προσωπικών δεδομένων, καθώς και θέματα ασφάλειας όπως π.χ. χρήση ισχυρών κωδικών πρόσβασης και συνθηματικών, τρόπο εντοπισμού και αναφοράς των περιστατικών παραβίασης της ασφάλειας, σωστή χρήση των e-mail και των αποσπώμενων μέσων αποθήκευσης, social engineering, phishing, vishing, ασφαλής χρήση εφαρμογών και ιστοτόπων, λογισμικά ασφάλειας, κλπ.

Η περιγραφή των βασικών διαδικασιών και των τεχνικών μέτρων ασφάλειας που πρέπει να γνωρίζουν τα μέλη του προσωπικού αναρτώνται σε κατάλληλο διαμορφωμένο δικτυακό τόπο (web portal).

Β) Εξειδικευμένη εκπαίδευση
Πρέπει να παρέχονται οι απαραίτητοι πόροι για την εξειδικευμένη εκπαίδευση του προσωπικού που έχει αναλάβει τη διαχείριση της ασφάλειας και την διαρκή ενημέρωσή του σχετικά με τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών.

Γ) Ενημερώσεις σε θέματα ασφάλειας
Πρέπει να πραγματοποιούνται συχνά και συστηματικά ενημερώσεις ασφάλειας του προσωπικού από ενημερωμένες και έγκυρες πηγές για την ασφάλεια πληροφοριών, ώστε κάθε εργαζόμενος να είναι σε θέση να προστατέψει τόσο το ίδρυμα όσο και τα προσωπικά δεδομένα που αυτό διαχειρίζεται, ιδιαίτερα από τυχόν νέους κινδύνους που εμφανίζονται στο διαδίκτυο.

7. Έλεγχος

Α) Διαδικασία ελέγχων
Ο Υπεύθυνος Ασφάλειας εφαρμόζει τουλάχιστον ετησίως διαδικασία εσωτερικού ελέγχου τήρησης των μέτρων ασφάλειας και της αποτελεσματικότητά τους στην προστασία των πληροφοριακών συστημάτων, των υπηρεσιών τηλεματικής και δικτύων, σύμφωνα με τα ακόλουθα στάδια:
α) προετοιμασία του ελέγχου (καθορισμός πληροφοριακών πόρων/επιμέρους πολιτικών που θα ελεγχθούν, χρονοδιάγραμμα, κλπ),
β) διεξαγωγή του ελέγχου,
γ) αποτελέσματα του ελέγχου (τυχόν ευρήματα, προτεινόμενες ενέργειες κλπ).

Τα αποτελέσματα των ελέγχων διαβιβάζονται ως πόρισμα στα αρμόδια διοικητικά όργανα και ο Υπεύθυνος Ασφάλειας τα αξιοποιεί προβαίνοντας στον προγραμματισμό των αναγκαίων τροποποιήσεων και προσθηκών στα μέτρα ασφάλειας καθώς και στο σχέδιο ασφάλειας.

Υποχρεωτικά ο εσωτερικός έλεγχος της τήρησης των μέτρων ασφάλειας και της αποτελεσματικότητά τους
θα γίνεται στις κρίσιμες πληροφοριακές και δικτυακές υποδομές από κατάλληλα εξουσιοδοτημένο προσωπικό και κατά ελάχιστον θα συμπεριλαμβάνει ελέγχους:

- Ανίχνευσης Ευπαθειών (Vulnerability Scans)
- Δοκιμών Παρείσδυσης (Penetration Testing)

Β. ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

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.
    - Κεφαλαία γράμματα.
    - Αριθμοί.
    - Ειδικοί χαρακτήρες.
3. Να αλλάζουν οπωσδήποτε εντός διαστήματος μικρότερου του ενός έτους
4. 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 (π.χ. LDAP, AD). 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 την ασφαλή αποθήκευση κωδικών πρόσβαση μπορεί να χρησιμοποιούν το λογισμικό Keepass.

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
Πρέπει να 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.

Η πολιτική διαβιβάζεται υποχρεωτικά στον Υπεύθυνο Ασφάλειας για τον σχετικό έλεγχο.

Σε περίπτωση λήψης αντιγράφων σε φορητά μέσα (εξωτερικοί δίσκοι, κλπ) επισημαίνονται επί αυτών η ημερομηνία λήψης των δεδομένων, το εύρος των λαμβανόμενων δεδομένων, το είδος του αντιγράφου (incremental, full), η περιοδικότητα λήψης του κάθε αντιγράφου (ημερήσιο, εβδομαδιαίο, μηνιαίο, ετήσιο), ο αριθμός των συνολικών αντιγράφων, καθώς και τόπος/τρόπος αποθήκευσης πχ χρηματοκιβώτιο.

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.

Στους υπολογιστές που τηρούν ή επεξεργάζονται προσωπικά δεδομένα και κυρίως δεδομένα ειδικών κατηγοριών λειτουργεί λογισμικό ελέγχου, εντοπισμού και παρεμπόδισης μη εξουσιοδοτημένων/λανθασμένων ενεργειών διακίνησης/μεταφοράς πληροφοριών εκτός του Πανεπιστημίου (DLP – Data Loss Prevention) του οποίου η λειτουργία καθορίζεται αυτόματα από κεντρική πολιτική προστασίας.

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 διαδικασιες.

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) Ειδικές ενέργειες που πρέπει να καταγράφονται
Στα αρχεία καταγραφής ενεργειών (log files) των πληροφοριακών συστημάτων και των υπηρεσιών διαδικτύου τηρούνται οπωσδήποτε, κατ' ελάχιστο, τα εξής: το αναγνωριστικό του χρήστη που αιτήθηκε την σύνδεση/προσπέλαση (δεδομένων προσωπικού χαρακτήρα), η ημερομηνία και ώρα του σχετικού αιτήματος, το σύστημα μέσω του οποίου αιτήθηκε την πρόσβαση (υπολογιστής, πρόγραμμα λογισμικού, κ.λπ.), καθώς και αν τελικά συνδέθηκε/προσπέλασε την πληροφορία που αιτήθηκε. Επίσης, πρέπει να καταγράφονται στοιχεία που αφορούν τις προσπάθειες μη εξουσιοδοτημένης πρόσβασης και γενικότερα κάθε ενέργεια η οποία μπορεί να υποδηλώνει διενέργεια επίθεσης.

Στα αρχεία καταγραφής κεντρικών συσκευών που συνδέουν το δίκτυο με τα εξωτερικά δίκτυα ή με εσωτερικές ζώνες ασφάλειας δύναται να τηρούνται, για περίοδο ενός έτους, αποκλειστικά: η ημερομηνία και η ώρα της κάθε σύνδεσης/αποσύνδεσης, η διάρκειά της, η διεύθυνση δικτύου

(προέλευσης-προορισμού) και το είδος (πρωτόκολλο-πόρτες TCP/IP) της επικοινωνίας. Τα αρχεία αυτά τηρούνται σε κρυπτογραφημένο κατάλογο του οποίου το κλειδί αποκρυπτογράφησης είναι αποκλειστικά γνωστό στον Υπεύθυνο Ασφάλειας και σε σύστημα που έχει διαχειριστικά δικαιώματα συγκεκριμένος εργαζόμενος. Για το έλεγχο των αρχείων απαιτείται ταυτόχρονη πρόσβαση των παραπάνω δύο, σε σύστημα και αρχεία, και με υποχρεωτική τη παρουσία του διοικητικά υπεύθυνου του αρμόδιου για την λειτουργία του δικτύου τμήματος.

Γ) 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 ΕΛ/ΛΑΚ 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

Προτείνεται σε όλα τα πληροφοριακά συστήματα και τις εφαρμογές με 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.
4. Ενέργειες δοκιμών.
5. Αποτελέσματα δοκιμών.
6. Έγκριση αλλαγών.

Β) Περιβάλλον δοκιμών

Οι δοκιμές του λογισμικού, τόσο σε επίπεδο επιμέρους εφαρμογών όσο και σε επίπεδο λειτουργιών διεξάγονται αποκλειστικά σε δοκιμαστικό περιβάλλον. Επίσης συμπεριλαμβάνουν μεθοδολογία επαλήθευσης της ασφάλειας των εφαρμογών και επισκόπηση του κώδικα, όπου αυτό είναι τεχνικά εφικτό.

Το λογισμικό ελέγχεται σε επικαιροποιημένο μη παραγωγικό σύστημα και χρησιμοποιούνται δοκιμαστικά και όχι πραγματικά δεδομένα ή δεδομένα του παραγωγικού συστήματος, εκτός εάν κάτι τέτοιο είναι απολύτως απαραίτητο και δεν υπάρχει εναλλακτική λύση. Αν είναι αναγκαίο μπορούν να χρησιμοποιηθούν πραγματικά δεδομένα σε ανωνυμοποιημένη μορφή ή διαφορετικά πρέπει να περιορίζονται στα απολύτως απαραίτητα για τους σκοπούς του ελέγχου.

Γ) Συντήρηση λογισμικού συστήματος / ενδιάμεσου λογισμικού / εφαρμογών

Η ενημέρωση, αναβάθμιση και συντήρηση του λογισμικού των κεντρικών υπολογιστικών και δικτυακών συστημάτων και των παρεχόμενων υπηρεσιών τηλεματικής γίνεται από εξειδικευμένο προσωπικό πληροφορικής, χωρίς να διακόπτεται η λειτουργία τους, όπου αυτό είναι τεχνικά εφικτό ή σε ώρες χαμηλής χρήσης/κίνησης.

Γ. ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

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.

Δ. ΜΕΤΡΑ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ

Για την προστασία των προσωπικών δεδομένων σε περίπτωση κάποιου έκτακτου περιστατικού, όπως φυσικές καταστροφές (π.χ. σεισμός, πυρκαγιά, πλημμύρα) ή μεγάλης εμβέλειας περιστατικά ασφάλειας (π.χ. καταστροφή από ιομορφικό λογισμικό) είναι απαραίτητη η λειτουργία κατάλληλα διαμορφωμένου κεντρικού υπολογιστικού και δικτυακού εξοπλισμού σε εναλλακτική εγκατάσταση (χώρο). Σε αυτό το χώρο θα γίνει ανάκαμψη και αποκατάσταση των κρίσιμων πληροφοριακών συστημάτων του Πανεπιστημίου σε περιπτώσεις έκτακτης ανάγκης.

Για την ταχύτερη δυνατή αντιμετώπιση των έκτακτων περιστάσεων στους χώρους λειτουργίας της κρίσιμης υπολογιστικής και δικτυακής υποδομής (π.χ. σεισμός, πυρκαγιά, πλημμύρα, κλοπή), είναι απαραίτητα:

1. να υπάρχουν συσκευές ή μέθοδοι που ελέγχουν τη θερμοκρασία, την πίεση, την υγρασία και άλλους περιβαλλοντικούς παράγοντες. Παραδείγματα είναι τα κλιματιστικά, οι ελεγκτές υγρασίας και οι ιονιστές της ατμόσφαιρας.
2. η τοποθέτηση συναγερμών, οι οποίοι χρησιμοποιούνται τόσο για την ανίχνευση (επικείμενης) ζημιάς λόγω των φαινομένων αυτών, αλλά και για την ανίχνευση εισβολών στα συστήματα.
3. η τοποθέτηση πυροσβεστήρων, ειδικών αφρών, ειδικών χρηματοκιβωτίων για την αποθήκευση σπουδαίων εγγράφων, αντιγράφων ασφάλειας και άλλων σημαντικών αντικειμένων, και εγκαταστάσεις αποθήκευσης νερού, οι οποίες να έχουν και δυνατότητες άντλησης.
4. η χρήση ups και ειδικών γεννητριών, για την αδιάλειπτη παροχή ηλεκτρικής ενέργειας στον εξοπλισμού.