Πολιτική Αποδεκτής Χρήσης Πληροφοριακών και Επικοινωνιακών Συστημάτων

Σκοπός

Η Πολιτική Αποδεκτής Χρήσης αποτελεί αναπόσπαστο τμήμα των Πολιτικών Ασφάλειας Πληροφοριών, Προστασίας της Ιδιωτικότητας και Επιχειρησιακής Συνέχειας του ΙΝΕΒ | ΕΚΕΤΑ. Περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των χρηστών των Πληροφοριακών Συστημάτων του Ινστιτούτου, στις Πληροφορίες που είναι αποθηκευμένες στα Πληροφοριακά Συστήματα του Ινστιτούτου και στις λοιπές κρίσιμες υποδομές.

Σκοπός της Πολιτικής Αποδεκτής Χρήσης είναι να διασφαλίσει ότι οι χρήστες του Ινστιτούτου δεν θα εκμεταλλευτούν την πρόσβαση που τους παρέχεται σύμφωνα με την Πολιτική Λογικής Πρόσβασης στα Πληροφοριακά και Επικοινωνιακά Συστήματα προκειμένου να προβούν σε ενέργειες που παραβιάζουν οποιοδήποτε νόμο του κράτους, που οδηγούν στην αποκάλυψη εμπιστευτικών πληροφοριών διαταράσσουν την ομαλή λειτουργία του Ινστιτούτου ή γενικότερα βλάπτουν την εικόνα του Ινστιτούτου. Για το λόγο αυτό, κάθε εργαζόμενος του Ινστιτούτου υπογράφει κατά την πρόσληψή του Δήλωση Αποδοχής των Πολιτικών Ασφάλειας Πληροφοριών, Προστασίας της Ιδιωτικότητας και Επιχειρησιακής Συνέχειας, αφού αυτές του επεξηγηθούν.

Ειδικότερα, όσον αφορά τις πληροφορίες, οι χρήστες του Ινστιτούτου υποχρεούνται να τις χειρίζονται, να τις διακινούν και να τις αποθηκεύουν ανάλογα με τη διαβάθμισή τους (classification of information).

Οι διαβαθμίσεις που χρησιμοποιούνται για τις πληροφορίες είναι:

- **Δημόσιο** (public): Έγγραφα ή πληροφορίες τα οποία μπορούν να κοινοποιηθούν σε τρίτους χωρίς αυτό να συνεπάγεται οικονομική ή άλλης φύσεως επίπτωση στο Ινστιτούτο.
- **Εσωτερικό** (Internal): Έγγραφα ή πληροφορίες που δεν προορίζονται για διάθεση ή κοινοποίηση έξω από το Ινστιτούτο. Στην περίπτωση που δημοσιοποιηθούν Εσωτερικά Έγγραφα, οι επιπτώσεις δεν θα έχουν άμεσο οικονομικό ή νομικό αντίκτυπο στο Ινστιτούτο αλλά θέτουν σε κίνδυνο τη φήμη ή την αξιοπιστία του.
- **Εμπιστευτικό** (Confidential): Έγγραφα ή πληροφορίες που δεν επιτρέπεται να διατίθενται ή να δημοσιεύονται σε τρίτους ή αναρμόδια άτομα. Η κοινοποίηση Εμπιστευτικών Εγγράφων ή Πληροφοριών μπορεί να επιφέρει άμεσες/έμμεσες οικονομικές επιπτώσεις στο Ινστιτούτο ή ακόμη και να εμποδίσει την συνέχειά των δραστηριοτήτων του.

Η διαβάθμιση των εγγράφων αναγράφεται ευκρινώς στο header ή το footer κάθε εγγράφου. Για οποιοδήποτε έγγραφο δεν αναφέρει ρητά τη διαβάθμισή του η χρήση του ή κοινοποίησή του θα γίνεται κατόπιν εγκρίσεως του προϊστάμενου.

Για τη διαβάθμιση των emails χρησιμοποιούνται οι διαβαθμίσεις που προτείνει ο κατασκευαστής της πλατφόρμας. Παρόλα αυτά, δεν θα πρέπει η διαβάθμιση των emails να επαφίεται στις δυνατότητες του mail server και του client. Θα πρέπει ο χρήστης να το διαβαθμίζει έστω και μόνος του υποχρεωτικά.

Επιπλέον, το Ινστιτούτο διαχειρίζεται τα assets του ανάλογα με τη διαβάθμισή τους.

Πεδίο Εφαρμογής

Η Πολιτική Αποδεκτής Χρήσης και όσα την απαρτίζουν, συγκεκριμένα τα:

- Δικαιώματα Χρηστών

- Υποχρεώσεις Χρηστών
- Συνέπειες
- Δικαιώματα του Ινστιτούτου
- Υποχρεώσεις του Ινστιτούτου
- Πολιτική Διαχείρισης Αποθηκευτικών Μέσων
- Πολιτική Διαχείρισης Φορητών Μέσων Αποθήκευσης Πληροφοριών

(πλην της Πολιτικής Ασφάλειας Συνεργατών) αφορούν όλους τους χρήστες του Ινστιτούτου.

Η Πολιτική Ασφάλειας Συνεργατών αφορά τους συνεργάτες, τους προμηθευτές και τους υπεργολάβους του Ινστιτούτου.

Δικαιώματα Χρηστών

Τα δικαιώματα χρηστών αναφέρονται στις ομάδες των χρηστών του Ινστιτούτου.

Χρήστης: Χρήστης του Ινστιτούτου καλείται κάθε εργαζόμενος, συνεργάτης, προμηθευτής που έχει πρόσβαση στα Πληροφοριακά Συστήματα του Ινστιτούτου, σύμφωνα με την Πολιτική Λογικής Πρόσβασης.

Τα δικαιώματα των χρηστών για τις επιμέρους υπηρεσίες, τηρώντας τους κανόνες που τους έχουν κοινοποιηθεί, ορίζονται ως εξής:

- Χρήση ηλεκτρονικού ταχυδρομείου, χωρίς να προβαίνουν σε αποστολή μηνυμάτων, αρχείων ή φωτογραφιών που παραβιάζουν οποιοδήποτε νόμο του κράτους, οδηγούν στην αποκάλυψη εμπιστευτικών πληροφοριών ή γενικότερα βλάπτουν την εικόνα του Ινστιτούτου. Για τη χρήση του ηλεκτρονικού ταχυδρομείου και του διαδικτύου υπάρχουν γραπτές οδηγίες, οι οποίες έχουν κοινοποιηθεί στους χρήστες και αποτελούν αναπόσπαστο μέρος της παρούσας πολιτικής.
- Πρόσβαση στο διαδίκτυο, αποκλειστικά σε νόμιμους ιστότοπους.
- Πρόσβαση στο εσωτερικό δίκτυο του Ινστιτούτου, σύμφωνα με τα καθήκοντά τους.
- Πρόσβαση στο cloud του Ινστιτούτου, σύμφωνα με τα καθήκοντά τους.
- Πρόσβαση στα πληροφοριακά συστήματα του Ινστιτούτου, ανάλογα με το αντικείμενο της εργασίας τους και τα δικαιώματα που τους έχουν αποδοθεί.

Υποχρεώσεις Χρηστών

Οι υποχρεώσεις των χρηστών είναι οι ίδιες ανεξάρτητα από τη διοικητική/ερευνητική ομάδα στην οποία ανήκουν και έχουν ως ακολούθως:

- Να σέβονται και να τηρούν τους Νόμους και τους Κανονισμούς του κράτους.
- Να είναι ενήμεροι και να εφαρμόζουν τις Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών και , Προστασίας της Ιδιωτικότητας του Ινστιτούτου.
- Να υπογράφουν Δήλωση Αποδοχής των Πολιτικών Ασφάλειας Πληροφοριών και, Προστασίας της Ιδιωτικότητας του Ινστιτούτου την ημέρα της πρόσληψής τους.
- Να λαμβάνουν όλα τα κατάλληλα μέτρα για την ασφάλεια των πληροφοριών (στο μέτρο που τους αφορά), όπως απόκρυψη των μυστικών κωδικών τους, κλείδωμα του ηλεκτρονικού υπολογιστή τους

όταν απομακρύνονται, αλλαγή του κωδικού πρόσβασης σε τακτά χρονικά διαστήματα ακολουθώντας τις καλές πρακτικές που έχουν υιοθετηθεί σχετικά με την πολυπλοκότητα και τη μη επαναχρησιμοποίηση.

- Σχετικά με τους κωδικούς ασφαλείας έχει εκδοθεί σχετική οδηγία και παρότρυνση προς τους χρήστες που έχουν να διαχειριστούν περισσότερα του ενός passwords, για χρήση ειδικού λογισμικού password management το οποίο εκτός όλων των άλλων ευκολιών διαθέτει και σύστημα γένεσης passwords με τυχαίο τρόπο περιλαμβάνοντας κανόνες υψίστης ασφάλειας.
- Να μην εγκαθιστούν στον εξοπλισμό που τους έχει παραχωρηθεί από το Ινστιτούτο για την τέλεση των καθηκόντων τους (προσωπικοί υπολογιστές / εργαστηριακός εξοπλισμός κ.λπ.) μη εγκεκριμένο ή παράνομο λογισμικό.
- Να ενημερώνουν αμέσως τον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας στα Πληροφοριακά Συστήματα ή τις διαδικασίες του Ινστιτούτου, που θέτει σε κίνδυνο τις πληροφορίες του.
- Να μην επιχειρούν την απόκτηση πρόσβασης σε Πληροφοριακά Συστήματα ή πληροφορίες οι οποίες δεν τους είναι απαραίτητες για την τέλεση των καθηκόντων τους ή δεν είναι δημοσίως ανακοινώσιμες.
- Απαγορεύεται να επιχειρούν να εκμεταλλευτούν πιθανά κενά ασφάλειας των Πληροφοριακών Συστημάτων του Ινστιτούτου προκειμένου να αποκτήσουν πρόσβαση σε πληροφορίες άλλων χρηστών του Ινστιτούτου, να διαταράξουν την ομαλή λειτουργία των Πληροφοριακών Συστημάτων, να εκτελέσουν κακόβουλο λογισμικό και γενικά να υποβαθμίσουν το επίπεδο ασφάλειας των Πληροφοριακών Συστημάτων.
- Να μην αποκαλύπτουν σε μη εξουσιοδοτημένα άτομα οποιαδήποτε εμπιστευτική ή εσωτερική πληροφορία ή στοιχείο υποπίπτει στην αντίληψή τους ή έρχεται την κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.
- Κατά την αποχώρησή τους (οικειοθελή ή μη) από το Ινστιτούτο οφείλουν να επιστρέφουν σε καλή κατάσταση όλον τον εξοπλισμό που έχουν παραλάβει, καθώς και να παραδίδουν κάθε πληροφορία / έγγραφο του Ινστιτούτου.
- Να μην επιτρέπουν τη χρήση του κωδικού που τους έχει ορίσει το Ινστιτούτο σε τρίτους χρήστες έτσι ώστε να αποκτήσουν πρόσβαση σε εφαρμογές ή άλλες πληροφορίες του Ινστιτούτου. Αντίστοιχα να μην αποδέχονται τη χρήση κωδικών πρόσβασης άλλων χρηστών για προσωπική τους χρήση.

Συνέπειες

Σε περίπτωση μη συμμόρφωσης των χρηστών με τις υποχρεώσεις τους, όπως αυτές αναφέρονται στην Πολιτική Αποδεκτής Χρήσης, ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών πραγματοποιεί τις παρακάτω ενέργειες:

1. Γίνεται σύσταση στο χρήστη από τον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών (ΥΔΑΠ) και ενημέρωση του Υπεύθυνου Τομέα/Τμήματος του χρήστη.
2. Σε περίπτωση μη συμμόρφωσης του χρήστη ή επανάληψης του συμβάντος, γίνεται σύσταση στον Υπεύθυνο Τομέα/Τμήματος του χρήστη και ενημέρωση της Ανώτατης Διοίκησης του Ινστιτούτου, από τον ΥΔΑΠ.
3. Σε περίπτωση που συνεχίζεται η μη συμμόρφωση, γίνεται ενημέρωση της Ανώτατης Διοίκησης, από τον ΥΔΑΠ.

Η επιβολή κυρώσεων ορίζεται από τον εκάστοτε Υπεύθυνο Τομέα/Τμήματος του χρήστη στον οποίο γίνεται η σύσταση, σε συνεργασία με την Ανώτατη Διοίκηση και τον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών.

Για την επιβολή κυρώσεων σε εργαζόμενο συνεκτιμώνται η επίπτωση του παραπτώματος, η σκοπιμότητα, οι ιδιαιτέρες συνθήκες τέλεσης του παραπτώματος, η εν γένει προσωπικότητα του εργαζομένου, καθώς και η υπηρεσιακή του εικόνα όπως προκύπτει από το προσωπικό του μητρώο και τηρείται η αρχή της αναλογικότητας.

Δικαιώματα του Ινστιτούτου

Το ΙΝΕΒ | ΕΚΕΤΑ παρέχει στους χρήστες του Ινστιτούτου πρόσβαση στα Πληροφοριακά Συστήματα για την οποία ισχύουν τα παρακάτω:

- Το Ινστιτούτο έχει δικαίωμα να αφαιρεί ή να διαγράφει άμεσα, μερικά ή ολικά, εγγραφές, φωτογραφίες, δεδομένα ή οποιοδήποτε άλλο υλικό και εν γένει περιεχόμενο, που εκθέτει πολιτικές απόψεις, θρησκευτικά στοιχεία, εθνικά χαρακτηριστικά, διακρίσεις φύλου και άλλα προσωπικά δεδομένα που έρχονται σε αντίθεση με διατάξεις της εθνικής και κοινοτικής Νομοθεσίας ή προσβάλλουν τα χρηστά ήθη.
- Το Ινστιτούτο έχει δικαίωμα βάσει των πολιτικών πρόσβασης να παρέχει ή να αφαιρεί δικαιώματα πρόσβασης σε χρήστες ανάλογα με τα υπηρεσιακά τους καθήκοντα.

Υποχρεώσεις του Ινστιτούτου

- Οφείλει να συμμορφώνεται με όλο το θεσμικό και νομικό πλαίσιο σχετικά με την Ασφάλεια των Πληροφοριών, την Επιχειρησιακή Συνέχεια και την προστασία των προσωπικών δεδομένων.
- Δίνει πρόσβαση στα Πληροφοριακά του Συστήματα μόνο εφόσον ο χρήστης έχει λάβει γνώση και έχει αποδεχθεί τις Πολιτικές Αποδεκτής Χρήσης και Ασφάλειας Πληροφοριών. Το γεγονός αυτό αποδεικνύεται με έγγραφη δήλωσή του, η οποία φέρει την πρωτότυπη υπογραφή του.
- Οφείλει να ενημερώνει τους χρήστες, συνεργάτες και ασθενείς με σαφήνεια και πληρότητα σε περίπτωση που συλλέξει ή επεξεργαστεί πληροφορίες που εμπίπτουν στην κατηγορία των προσωπικών δεδομένων και βρίσκονται στα Πληροφοριακά του Συστήματα ή σε έντυπο αρχείο.
- Οφείλει να ενημερώνει τους χρήστες της, συνεργάτες και ασθενείς για τα δεδομένα επικοινωνίας τα οποία πιθανόν αποθηκεύονται σε αντίγραφα ασφαλείας και τα οποία είναι ανακτήσιμα ακόμα και μετά τη διαγραφή τους από το χρήστη. Οι χρήστες πρέπει να είναι ενήμεροι σχετικά με τη διαδικασία δημιουργίας αντιγράφων ασφαλείας δεδομένων.
- Οφείλει να καταβάλλει κάθε δυνατή προσπάθεια για την καλή λειτουργία των Πληροφοριακών Συστημάτων και να προβαίνει σε αποκατάσταση τυχόν βλαβών.
- Οφείλει να συντηρεί, ανανεώνει, επικαιροποιεί και επεκτείνει τις Πολιτικές Διαχείρισης Ασφάλειας Πληροφοριών, Προστασίας της Ιδιωτικότητας και Επιχειρησιακής Συνέχειας .
- Οφείλει να ενημερώσει το σύνολο του προσωπικού του για τη συγκεκριμένη πολιτική καθώς και να προβεί σε όλες τις απαραίτητες δράσεις για την εκπαίδευση των χρηστών.
- Οφείλει να υλοποιεί τις πολιτικές ασφάλειας πληροφοριών χρησιμοποιώντας σύγχρονες και δοκιμασμένες τεχνολογίες και διαδικασίες ασφάλειας πληροφοριών.

Πολιτική Ασφάλειας Συνεργατών – Προμηθευτών - Υπεργολάβων

Σκοπός

Σκοπός της Πολιτικής Ασφάλειας Συνεργατών – Προμηθευτών – Υπεργολάβων είναι:

- Η διατήρηση, μεταξύ του Ινστιτούτου και των συνεργατών / προμηθευτών / υπεργολάβων του, ενός συμφωνημένου επιπέδου παροχής υπηρεσιών (Service Level Agreement) και ασφάλειας πληροφοριών, στο πλαίσιο μίας υπογεγραμμένης Σύμβασης Συνεργασίας.
- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από τις δραστηριότητες των συνεργατών / προμηθευτών / υπεργολάβων του Ινστιτούτου.
- Να διασφαλιστούν οι εμπιστευτικές πληροφορίες και τα προσωπικά δεδομένα των ασθενών/εξεταζόμενων/συμμετεχόντων σε έρευνες και των εργαζομένων του Ινστιτούτου.

Πεδίο εφαρμογής

Η πολιτική αφορά τους συνεργάτες, τους προμηθευτές και τους υπεργολάβους του Ινστιτούτου (στο εξής θα αναφέρονται όλοι ως συνεργάτες, για λόγους συντομίας), είτε πρόκειται για φυσικά είτε για νομικά πρόσωπα που έχουν ή μπορεί να αποκτήσουν πρόσβαση στα Πληροφοριακά Συστήματα και στις πληροφορίες που συλλέγει και επεξεργάζεται το ΙΝΕΒ | ΕΚΕΤΑ.

Η εφαρμογή της πολιτικής είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της σύμβασης συνεργασίας.

Περιεχόμενο

Οι δραστηριότητες των συνεργατών του Ινστιτούτου, είτε πρόκειται για φυσικά πρόσωπα είτε για εταιρίες που αναλαμβάνουν διάφορες εργασίες, όπως εργασίες ανάπτυξης, αναβάθμισης και συντήρησης Πληροφοριακών Συστημάτων, εκτυπωτικές εργασίες κλπ., καθώς και των προμηθευτών υπηρεσιών, όπως οι τηλεπικοινωνιακές υπηρεσίες, μπορεί να θέσουν σε κίνδυνο την εφαρμογή των Πολιτικών Ασφάλειας Πληροφοριών του οργανισμού.

Προκειμένου να διασφαλιστεί ότι οι συνεργάτες συμμορφώνονται με τις Πολιτικές Ασφάλειας Πληροφοριών του Ινστιτούτου υπογράφουν Συμφωνία Εμπιστευτικότητας και τους κοινοποιείται η παρούσα Πολιτική.

Το ΙΝΕΒ | ΕΚΕΤΑ διατηρεί ενημερωμένο αρχείο στο οποίο καταγράφονται οι συνεργάτες που έχουν αποκτήσει ή τους έχει παρασχεθεί η δυνατότητα πρόσβασης στα πληροφοριακά συστήματα του Ινστιτούτου, προκειμένου να προσφέρουν τις υπηρεσίες τους.

Υποχρεώσεις συνεργατών

Οι συνεργάτες του Ινστιτούτου έχουν τις ίδιες υποχρεώσεις αναφορικά με την ασφάλεια των Πληροφοριών και των Πληροφοριακών Συστημάτων του Ινστιτούτου, την Προστασία της Ιδιωτικότητας και την Επιχειρησιακή Συνέχεια που έχουν και οι εργαζόμενοι του Ινστιτούτου.

Ειδικά για την περίπτωση της απομακρυσμένης πρόσβασης οι συνεργάτες – προμηθευτές – υπεργολάβοι οφείλουν να ακολουθούν πιστά τη διαδικασία αιτήματος πρόσβασης δηλώνοντας το σκοπό ή εργασία που αφορά και το χρονικό διάστημα που απαιτείται.

Οι συνεργάτες του Ινστιτούτου επιτρέπουν στον οργανισμό, μετά από έγκαιρη ενημέρωση και κατόπιν συνεννοήσεως, την επιθεώρηση των εγκαταστάσεων, των πολιτικών και των διαδικασιών τους, ώστε να επιβεβαιώσει το Ινστιτούτο την τήρηση των όρων της Συμφωνίας Εμπιστευτικότητας, των Service Level Agreements (SLAs) και της Σύμβασης Συνεργασίας που έχουν υπογραφεί μεταξύ των δύο μερών (Right to audit).

Η επιθεώρηση θα διεξάγεται από τον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών και, πιθανόν, εξειδικευμένα μέλη της ομάδας του.

Διασφάλιση της ασφάλειας των πληροφοριών, Προστασίας της Ιδιωτικότητας και της επιχειρησιακής συνέχειας

Το ΙΝΕΒ | ΕΚΕΤΑ προβαίνει σε όλες τις ενέργειες που διασφαλίζουν ότι οι δραστηριότητες των συνεργατών του δε θέτουν σε κίνδυνο τα δικαιώματα των ενδιαφερόμενων μερών του συστήματος, αναφορικά με την υγεία τους, την ασφάλεια των πληροφοριών, την επιχειρησιακή συνέχεια και την προστασία των προσωπικών τους δεδομένων.

Προστασία Πληροφοριακών Συστημάτων από ενέργειες συνεργατών

Το Ινστιτούτο αναγνωρίζει τους κινδύνους που προέρχονται από τις δραστηριότητες των συνεργατών της και λαμβάνει όλα τα μέτρα ώστε να τους περιορίσει.

Υποχρεώσεις συνεργατών

- Οι συνεργάτες του Ινστιτούτου οφείλουν να γνωρίζουν και να εφαρμόζουν όλους τους όρους για την Ασφάλεια των Πληροφοριών, την Προστασία της Ιδιωτικότητας και την Επιχειρησιακή Συνέχεια του Ινστιτούτου, που τους έχουν κοινοποιηθεί. Για το προσωπικό των συνεργατών που εκτελεί εργασίες στα Πληροφοριακά και Επικοινωνιακά Συστήματα του Ινστιτούτου ισχύουν οι ίδιοι κανόνες με το προσωπικό του Ινστιτούτου.
- Οι συνεργάτες του Ινστιτούτου οφείλουν να αναφέρουν στο Ινστιτούτο κάθε περιστατικό που μπορεί να θέσει σε κίνδυνο τις Πληροφορίες ή τα Πληροφοριακά Συστήματά του.
- Οι συνεργάτες του Ινστιτούτου οφείλουν να σέβονται τη διαβάθμιση των πληροφοριών / δεδομένων στα οποία αποκτούν πρόσβαση και να τα διαχειρίζονται σύμφωνα με αυτή.
- Οι συνεργάτες του Ινστιτούτου απαγορεύεται να αποκαλύπτουν πληροφορίες ή άλλα στοιχεία που συνδέονται με (α) προσωπικά δεδομένα ασθενών (β) στοιχεία σχετικά με υπηρεσίες υγείας που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο, (γ) άλλα προσωπικά δεδομένα χρηστών των Πληροφοριακών Συστημάτων.
- Οι συνεργάτες του Ινστιτούτου επιτρέπουν στο Ινστιτούτο, μετά από έγκαιρη ενημέρωση και κατόπιν συνεννοήσεως, την επιθεώρηση των εγκαταστάσεων και των διαδικασιών τους, ώστε να επιβεβαιωθεί την τήρηση των όρων της Συμφωνίας Εμπιστευτικότητας, των Service Level Agreements (SLAs) και της Σύμβασης Συνεργασίας που έχει υπογραφεί μεταξύ των δύο μερών (Right to audit).
- Ειδικά για την περίπτωση της απομακρυσμένης πρόσβασης οι συνεργάτες – προμηθευτές – υπεργολάβοι οφείλουν να ακολουθούν πιστά τη διαδικασία αιτήματος πρόσβασης δηλώνοντας το σκοπό ή εργασία που αφορά και το χρονικό διάστημα που απαιτείται.

Συμβάσεις

Όλες οι απαιτήσεις λειτουργίας των Πληροφοριακών Συστημάτων περιγράφονται αναλυτικά στις συμβάσεις με τους συνεργάτες. Οι συμβάσεις περιέχουν τις παρακάτω προβλέψεις

- Δικαίωμα Ελέγχου (Right to Audit)
- Όρους Εμπιστευτικότητας (Confidentiality)
- Όρους μη αποκάλυψης (Non-Disclosure)

- Συμφωνίες Επιπέδου υπηρεσιών (Service Level Agreements)
- Ασφαλιστική Κάλυψη (όπου απαιτείται)

Επίσης, στις συμβάσεις γίνονται ιδιαίτερες αναφορές σχετικά με:

- Τις απαιτήσεις και τα μέτρα που λαμβάνονται για την ασφάλεια των πληροφοριών και την επιχειρησιακή συνέχεια, ώστε να διασφαλίζεται η εμπιστευτικότητα, η διαθεσιμότητα και η ακεραιότητα των πληροφοριών, κατά την πρόσβαση σε αυτές και την επεξεργασία τους από τους συνεργάτες του Ινστιτούτου, καθώς και η οριστική διαγραφή και καταστροφή τους μετά τη λήξη της συνεργασίας.
- Με την υπογραφή της σύμβασης ο συνεργάτης αναλαμβάνει την υποχρέωση τήρησης κατάλληλων μέτρων για την ασφάλεια των πληροφοριών και τη διασφάλιση της επιχειρησιακής συνέχειας, όπως ορίζεται στη σύμβαση.

Στην περίπτωση ανάθεσης μέρους ή όλης της ανάπτυξης πληροφοριακού συστήματος σε συνεργάτη, η σχετική σύμβαση θα πρέπει να περιλαμβάνει:

- Περιγραφή και μεθοδολογία της διαδικασίας ανάπτυξης
- Ορισμό των ρόλων και των αρμοδιοτήτων
- Προδιαγραφές ασφάλειας του περιβάλλοντος ανάπτυξης
- Διεργασίες διασφάλισης ότι ο συνεργάτης ικανοποιεί τις απαιτήσεις ασφάλειας πληροφοριών του Ινστιτούτου, όπως αυτές ορίζονται στις Πολιτικές και Διαδικασίες του.

Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των Πληροφοριακών Συστημάτων του Ινστιτούτου περιλαμβάνουν όρους που εξασφαλίζουν συμβατικά και τεχνικά την τήρηση των Πολιτικών και Διαδικασιών Ασφάλειας Πληροφοριών του Ινστιτούτου. Στις συμβάσεις γίνεται ιδιαίτερη αναφορά στην Προστασία Προσωπικών Δεδομένων.

Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των παραπάνω Συστημάτων περιλαμβάνουν ρήτρες σε περίπτωση μη συμμόρφωσης με τις Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών.

Για την πρόσβαση σε προσωπικά δεδομένα ασθενών/ εξεταζόμενων/ συμμετεχόντων σε έρευνες του Ινστιτούτου εφαρμόζεται η ισχύουσα νομοθεσία Προστασίας Προσωπικών Δεδομένων.

Οι συνεργάτες, οι οποίοι αποκτούν πρόσβαση στις Πληροφορίες ή τα Πληροφοριακά και Επικοινωνιακά Συστήματα και τα δεδομένα που αφορούν τις επικοινωνίες των ασθενών δεν επιτρέπεται να αποκαλύπτουν οποιαδήποτε πληροφορία ή στοιχείο υποπίπτει στην αντίληψή τους ή την κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

Ο Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών ελέγχει και γνωμοδοτεί για την επάρκεια των όρων της σύμβασης σε σχέση με την ασφάλεια Πληροφοριών, των Πληροφοριακών Συστημάτων, όπως επίσης και για τη δυνατότητα του συνεργάτη να ανταποκριθεί στις απαιτήσεις ασφάλειας και επιχειρησιακής συνέχειας που θέτει το Ινστιτούτο.

Το ΙΝΕΒ | ΕΚΕΤΑ ορίζει συγκεκριμένο φυσικό πρόσωπο που είναι υπεύθυνο για την εποπτεία του εκάστοτε συνεργάτη.

Οι όροι που αφορούν την τήρηση των Πολιτικών Ασφάλειας Πληροφοριών περιλαμβάνονται και στις προκηρύξεις των έργων.

Για το προσωπικό των συνεργατών που έχουν πρόσβαση στις εγκαταστάσεις της Πληροφορικής του Ινστιτούτου (π.χ. Computer Room), στον Εργαστηριακό εξοπλισμό, και τα Πληροφοριακά Συστήματα απαιτείται άδεια και παραχωρείται προσωρινή πρόσβαση (μέσω RFID tag, με αρχεία καταγραφής) από τον Υπεύθυνο Ασφάλειας Πληροφοριών του Ινστιτούτου.

Εξωτερικά συνεργεία συντήρησης ή και επισκευών στους χώρους και τις υποδομές της Πληροφορικής συνοδεύονται διαρκώς από άτομα του Ινστιτούτου.

Ο συνεργάτης δε μπορεί να εκχωρήσει δικαιώματα χρήσης ή πρόσβασης στον εξοπλισμό του Ινστιτούτου σε τρίτους χωρίς ρητή άδεια από την πλευρά της Διοίκησης του Ινστιτούτου.

Οι συνεργασίες του Ινστιτούτου αναθεωρούνται σε ετήσια βάση, έτσι ώστε να είναι εφικτή η αξιολόγηση και βελτίωσή τους. Η Ανώτατη Διοίκηση και οι Υπεύθυνοι Τομέων/ Τμημάτων παρακολουθούν σε ετήσια βάση την πρόοδο των συμβάσεων με τους συνεργάτες του Ινστιτούτου.

Πιθανές αλλαγές στις υπηρεσίες που παρέχουν οι συνεργάτες ή η αναθεώρηση και βελτίωση των υπαρχουσών πολιτικών ασφάλειας πληροφοριών και των σχετικών διαδικασιών και ελέγχων, εξετάζονται υπό το πρίσμα της κρισιμότητας των επιχειρηματικών πληροφοριών και διεργασιών που αφορούν και της επαναξιολόγησης των κινδύνων (re-assessment of the risks).

Το αρμόδιο προσωπικό του Ινστιτούτου ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας για κάθε παραβίαση των συμβατικών όρων για την ασφάλεια των πληροφοριών και των όρων εμπιστευτικότητας που αναφέρονται στις προηγούμενες παραγράφους.

Πολιτική Διαχείρισης Αποθηκευτικών Μέσων

Σκοπός

Η διαχείριση, αποθήκευση, απόσυρση ή καταστροφή των αποθηκευτικών μέσων πρέπει να γίνεται με τέτοιο τρόπο ώστε να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων που φιλοξενούνται σε αυτά, σύμφωνα με τις Πολιτικές Διαχείρισης Ασφάλειας Πληροφοριών, Προστασίας της Ιδιωτικότητας και Επιχειρησιακής Συνέχειας του Ινστιτούτου

Το INEB | EKETA κατέχει και διαχειρίζεται εμπιστευτικά δεδομένα στα πλαίσια διεξαγωγής των ερευνητικών έργων και των υπηρεσιών που παρέχει. Τα δεδομένα αυτά, τα οποία μπορεί εν δυνάμει να φιλοξενηθούν σε διάφορα αποθηκευτικά μέσα, πρέπει να προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη, καταστροφή ή κατάχρηση. Το Ινστιτούτο χρησιμοποιεί μηχανισμούς ασφάλειας που παρέχουν το κατάλληλο επίπεδο προστασίας για τα αποθηκευτικά μέσα.

Πεδίο εφαρμογής

Η Πολιτική Διαχείρισης Αποθηκευτικών Μέσων ισχύει για όλα τα μέσα που αξιοποιούνται για την αποθήκευση δεδομένων και πληροφοριών του Ινστιτούτου και αφορά όλους τους χρήστες του Ινστιτούτου.

Περιεχόμενο

Διαδικασίες και Οδηγίες

1) Διαχείριση Αποθηκευτικών Μέσων:
   (1) Οι χρήστες θα πρέπει να λαμβάνουν όλα τα εύλογα μέτρα για την προστασία των αποθηκευτικών μέσων που τους έχουν ανατεθεί, είτε από ενέργειες παραβίασης / κλοπής είτε από τυχαία καταστροφή.
   (2) Πρέπει να προβλέπονται τα κατάλληλα φυσικά και περιβαλλοντικά μέτρα προστασίας για τα αποθηκευτικά μέσα που τοποθετούνται σε χώρο φύλαξης.
   (3) Διαχείριση αποθηκευτικών μέσων που φιλοξενούν εμπιστευτικά δεδομένα:
      - Τα αποθηκευτικά μέσα που περιέχουν εμπιστευτικά δεδομένα πρέπει να είναι προσβάσιμα μόνο από εξουσιοδοτημένους χρήστες. Σε περίπτωση που αυτό δεν μπορεί να διασφαλιστεί θα πρέπει να είναι κρυπτογραφημένα, με επαρκείς μεθόδους, σύμφωνα με το τρέχον επίπεδο τεχνολογίας.
      - Τα αποθηκευτικά μέσα που περιέχουν εμπιστευτικά δεδομένα, σε περίπτωση που αφαιρεθούν από το μηχάνημα στο οποίο είναι εγκατεστημένα, θα πρέπει να φέρουν κατάλληλη σήμανση με το επίπεδο διαβάθμισής τους. Η επισήμανση πρέπει να περιλαμβάνει όλες τις ειδικές οδηγίες χειρισμού.
      - Τα αποθηκευτικά μέσα που περιέχουν εμπιστευτικά δεδομένα, όταν δεν χρησιμοποιούνται θα πρέπει να προστατεύονται κατάλληλα (π.χ. να διατηρούνται σε κλειδωμένο συρτάρι, ντουλάπι ή κιβώτιο ασφαλείας).
      - Τα αποθηκευτικά μέσα που περιέχουν εμπιστευτικές πληροφορίες θα πρέπει να τίθενται εκτός θέας όταν στο χώρο υπάρχουν επισκέπτες.
2) Καταστροφή Αποθηκευτικών Μέσων:
   (1) Οι χρήστες πρέπει να είναι ενήμεροι ότι η τοπική διαγραφή των δεδομένων από τα μέσα αποθήκευσης δεν τα καταργεί πλήρως ή οριστικά από το μέσο. Τα διαγραμμένα αρχεία είναι ευάλωτα σε ενέργειες μη εξουσιοδοτημένης ανάκτησης, σε περίπτωση που δεν αποσυρθούν-καταστραφούν κατάλληλα. Για το λόγο αυτό η καταστροφή των αποθηκευτικών μέσων γίνεται από τον Υπεύθυνο Πληροφορικής με φυσική καταστροφή αυτών.

(2) Τα μέσα αποθήκευσης που περιέχουν εμπιστευτικά δεδομένα καταστρέφονται με φυσική καταστροφή, όταν πλέον δεν αξιοποιούνται για την αποθήκευση εμπιστευτικών δεδομένων.
(3) Για οποιοδήποτε εξοπλισμό πληροφορικής που διαχειρίζεται ο Υπεύθυνος Πληροφορικής και μεταβιβάζεται, δωρίζεται ή με οποιονδήποτε άλλο τρόπο αποσύρεται, τα μέσα αποθήκευσης που σχετίζονται με τον εξοπλισμό αυτό υπόκεινται σε διαδικασία φυσικής καταστροφής.

Ρόλοι και Αρμοδιότητες

Οι Ιδιοκτήτες Πληροφοριών φέρουν την ευθύνη για τη ορθή διαβάθμιση της πληροφορίας και τη διακίνηση αυτής, βάσει της διαβάθμισής της. Ο κάτοχος της διαβαθμισμένης πληροφορίας οφείλει να τη διαχειρίζεται βάσει της διαβάθμισης που της έχει δοθεί από τον ιδιοκτήτη της πληροφορίας.

Οι κάτοχοι μέσων αποθήκευσης οφείλουν να τα χειρίζονται και να τα καταστρέφουν σύμφωνα με τις πολιτικές και διαδικασίες του Ινστιτούτου.

1) Οι **Υπεύθυνοι των Συστημάτων** φέρουν την ευθύνη για:
   (1) Παροχή βοήθειας στους Ιδιοκτήτες Πληροφοριών σχετικά με τον κατάλληλο χειρισμό των πληροφοριών και των μέσων αποθήκευσης, σύμφωνα με τις εταιρικές πολιτικές και διαδικασίες.
   (2) Την εφαρμογή των πολιτικών και διαδικασιών για όλα τα αποθηκευτικά μέσα που έχουν ανατεθεί σε αυτούς.
   (3) Την άμεση ενημέρωση του Υπεύθυνου Ασφάλειας Πληροφοριών σε περίπτωση απώλειας, καταστροφής ή κλοπής οποιουδήποτε αποθηκευτικού μέσου που τους έχει ανατεθεί.
2) Οι **Χρήστες** φέρουν την ευθύνη για:
   (1) Την προστασία των αποθηκευτικών μέσων που έχουν στην κατοχή τους.
   (2) Την ενημέρωση του Υπεύθυνου Ασφάλειας Πληροφοριών σε περίπτωση απώλειας, καταστροφής ή κλοπής οποιουδήποτε αποθηκευτικού μέσου που τους έχει ανατεθεί.
   (3) Τη μη αποθήκευση διαβαθμισμένων πληροφοριών σε φορητά αποθηκευτικά μέσα, που δεν έχουν προηγουμένως κρυπτογραφηθεί.
3) Οι **Διευθυντές/ Υπεύθυνοι Τομέων/Τμημάτων** οφείλουν:

   Να διασφαλίζουν ότι οι υφιστάμενοί τους γνωρίζουν τον κατάλληλο τρόπο χειρισμού και απόσυρσης των αποθηκευτικών μέσων, σύμφωνα με τις πολιτικές και διαδικασίες του Ινστιτούτου.

4) Ο **Υπεύθυνος Ασφάλειας Πληροφοριών** φέρει την ευθύνη για την ανάπτυξη πολιτικών και διαδικασιών διαχείρισης των αποθηκευτικών μέσων, για την εκπαίδευση και διαρκή ενημέρωση των χρηστών σε αυτές, καθώς και τη διενέργεια ελέγχων εφαρμογής τους.

Πολιτική Διαχείρισης Φορητών (Αποσπώμενων) Μέσων Αποθήκευσης Πληροφοριών

Σκοπός

Σκοπός της Πολιτικής Διαχείρισης Φορητών Μέσων Αποθήκευσης Πληροφοριών είναι να ορίσει και να θέσει σε εφαρμογή τα κατάλληλα μέτρα σχετικά με τη χρήση, τη διακίνηση και την καταστροφή των φορητών αποθηκευτικών μέσων ώστε να αποτρέπεται η αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα.

Πεδίο εφαρμογής

Η Πολιτική Διαχείρισης Φορητών Μέσων Αποθήκευσης Πληροφοριών αφορά όλους τους χρήστες του Ινστιτούτου.

Περιεχόμενο

Το ΙΝΕΒ | ΕΚΕΤΑ επιτρέπει τη χρήση μη κρυπτογραφημένων φορητών μέσων αποθήκευσης πληροφοριών αποκλειστικά για τη μεταφορά παρουσιάσεων / πληροφοριών δημόσιου χαρακτήρα.

Σε περίπτωση που υπάρξει ανάγκη μεταφοράς πληροφοριών άλλης διαβάθμισης σε φορητό μέσο αποθήκευσης, τότε γίνεται αίτημα προς τον Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών, ο οποίος εφ' όσον εγκρίνει το αίτημα, προμηθεύει τον αιτούντα με κρυπτογραφημένο εξωτερικό σκληρό δίσκο ή usb stick.

Σε οποιαδήποτε άλλη περίπτωση απαγορεύεται αυστηρά η χρήση φορητών μέσων αποθήκευσης για τη μεταφορά πληροφοριών.

Κάθε φορητό μέσο αποθήκευσης που για οποιοδήποτε λόγο έχει τεθεί σε αχρηστία, παραδίδεται στον Υπεύθυνο Πληροφορικής, η οποία φροντίζει για τη φυσική καταστροφή του και την ανακύκλωσή του. Το ΙΝΕΒ | ΕΚΕΤΑ κάνει, κατά περίπτωση, σχετική συμφωνία με εταιρία ανακύκλωσης.

Τα φορητά μέσα αποθήκευσης που περιέχουν εμπιστευτικά δεδομένα θα πρέπει, επίσης, να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, κατάχρηση ή αλλοίωση κατά τη μεταφορά τους.

Το ΙΝΕΒ | ΕΚΕΤΑ :

- Χρησιμοποιεί αξιόπιστους μεταφορείς ή εταιρίες courier .
- Χρησιμοποιεί κατάλληλες συσκευασίες, που ακολουθούν τις οδηγίες των κατασκευαστών, ώστε να προστατεύεται το περιεχόμενο από οποιαδήποτε φυσική ζημία που ενδέχεται να προκύψει κατά τη διάρκεια της μεταφοράς.

Το προσωπικό που είναι υπεύθυνο για τη μεταφορά των φορητών αποθηκευτικών μέσων:

- Φροντίζει τα μεταφερόμενα μέσα να μη μένουν αφύλακτα σε καμία χρονική στιγμή.
- Οφείλει να αναφέρει στο Ινστιτούτο οποιαδήποτε ασυνήθιστα συμβάντα ή περιστατικά που αφορούν την ασφάλεια των μεταφερόμενων αποθηκευτικών μέσων.

Πολιτική χρήσης της πλατφόρμας επικοινωνίας/οργάνωσης ομάδων και διαχείρισης εργασιών του INEB

1. Σκοπός

Σκοπός αυτής της πολιτικής είναι να διασφαλίσει την ασφαλή και αποτελεσματική χρήση των πλατφορμών επικοινωνίας και διαχείρισης εργασιών, όπως η υπηρεσία Slack, Trello και παρόμοιων υπηρεσιών, από όλα τα μέλη του INEB. Αυτή η πολιτική στοχεύει στη διαφύλαξη ευαίσθητων πληροφοριών, στη διασφάλιση της συμμόρφωσης με τις κανονιστικές απαιτήσεις και στην προώθηση της αποτελεσματικής επικοινωνίας και συνεργασίας εντός του Ινστιτούτου.

2. Πεδίο εφαρμογής

Αυτή η πολιτική ισχύει για όλο το προσωπικό, το ερευνητικό προσωπικό, τους φοιτητές και κάθε άλλο άτομο στα οποία έχει παραχωρηθεί πρόσβαση στις πλατφόρμες επικοινωνίας και διαχείρισης εργασιών του Ινστιτούτου. Καλύπτει τη χρήση αυτών των πλατφορμών τόσο εντός των εγκαταστάσεων του Ινστιτούτου όσο και εξ αποστάσεως.

3. Δήλωση Πολιτικής

Το Ινστιτούτο δεσμεύεται να παρέχει ένα ασφαλές και παραγωγικό περιβάλλον για όλα τα μέλη του. Η χρήση πλατφορμών επικοινωνίας και διαχείρισης εργασιών, ενθαρρύνεται για τη διευκόλυνση της συνεργασίας, της ανταλλαγής πληροφοριών και της διαχείρισης έργου. Ωστόσο, είναι επιτακτική ανάγκη αυτά τα εργαλεία να χρησιμοποιούνται υπεύθυνα και σύμφωνα με τις ακόλουθες οδηγίες για την προστασία των πληροφοριών και των πόρων του Ινστιτούτου.

4. Οδηγίες χρήσης

4.1. Ασφάλεια λογαριασμού

Οι χρήστες πρέπει να διατηρούν εμπιστευτικά τα διαπιστευτήρια του λογαριασμού τους και απαγορεύεται να μοιράζονται τα στοιχεία σύνδεσης με άλλους.

Ο έλεγχος ταυτότητας δύο παραγόντων πρέπει να είναι ενεργοποιημένος για όλους τους λογαριασμούς, όπου είναι διαθέσιμος, για να παρέχεται ένα πρόσθετο επίπεδο ασφάλειας.

Οι χρήστες που έχουν πρόσβαση σε παρόμοιες υπηρεσίες, όπως και τα σχετικά του δικαιώματα, πρέπει να είναι καταγεγραμμένα.

4.2. Χειρισμός δεδομένων και εμπιστευτικότητα

Ευαίσθητες ή εμπιστευτικές πληροφορίες θα πρέπει να κοινοποιούνται μόνο σε ιδιωτικά κανάλια ή απευθείας μηνύματα και μόνο με άτομα που έχουν νόμιμη ανάγκη να τα γνωρίζουν.

Οι χρήστες πρέπει να συμμορφώνονται με όλους τους ισχύοντες νόμους περί προστασίας δεδομένων και απορρήτου όταν χειρίζονται προσωπικές ή ευαίσθητες πληροφορίες.

4.3. Αποδεκτή χρήση

Οι πλατφόρμες θα πρέπει να χρησιμοποιούνται αποκλειστικά για δραστηριότητες που σχετίζονται με το Ινστιτούτο και όχι για προσωπικές επικοινωνίες.

Οι χρήστες πρέπει να απέχουν από τη δημοσίευση περιεχομένου που είναι προσβλητικό, μεροληπτικό ή με άλλο τρόπο ακατάλληλο.

4.4. Συμμόρφωση και Αναφορά

Οποιαδήποτε ύποπτη δραστηριότητα, παραβιάσεις δεδομένων ή παραβιάσεις πολιτικής πρέπει να αναφέρεται αμέσως στην Ομάδα Ασφάλειας IT του Ινστιτούτου.

Οι χρήστες αναμένεται να συμμορφώνονται με όλες τις συμφωνίες αδειοδότησης λογισμικού και τους όρους παροχής υπηρεσιών για τις πλατφόρμες που χρησιμοποιούνται.

4.5. Κατάρτιση και Ευαισθητοποίηση

Όλοι οι χρήστες υποχρεούνται να ολοκληρώσουν μια αρχική εκπαίδευση σχετικά με την ασφαλή και αποτελεσματική χρήση των πλατφορμών επικοινωνίας και διαχείρισης εργασιών. Οι εκπαιδευτικές συνεδρίες ανανέωσης θα πραγματοποιούνται ετησίως ή ανάλογα με τις ανάγκες.

4.6. Παρακολούθηση και επιβολή

Το Ινστιτούτο διατηρεί το δικαίωμα να παρακολουθεί τη χρήση της πλατφόρμας για να διασφαλίσει τη συμμόρφωση με αυτήν την πολιτική. Οποιεσδήποτε παραβιάσεις ενδέχεται να οδηγήσουν σε πειθαρχικά μέτρα, έως και τερματισμό πρόσβασης, απασχόληση ή εγγραφή.

5. Εφαρμογή

Το Τμήμα Πληροφορικής είναι υπεύθυνο για την εφαρμογή και επιβολή αυτής της πολιτικής. Αυτό περιλαμβάνει την παροχή της απαραίτητης εκπαίδευσης, την παρακολούθηση της χρήσης της πλατφόρμας και τη λήψη διορθωτικών μέτρων όταν συμβαίνουν παραβιάσεις.

6. Αναθεώρηση και αναθεώρηση

Αυτή η πολιτική θα επανεξετάζεται ετησίως ή πιο συχνά, όπως απαιτείται, για να αντικατοπτρίζει τις αλλαγές στις κανονιστικές απαιτήσεις, τις τεχνολογικές εξελίξεις ή τις επιχειρησιακές ανάγκες. Οι τροποποιήσεις αυτής της πολιτικής θα κοινοποιηθούν σε όλα τα ενδιαφερόμενα μέρη εγκαίρως.

7. Αναγνώριση

Με την πρόσβαση και τη χρήση των πλατφορμών επικοινωνίας και διαχείρισης εργασιών του Ινστιτούτου, οι χρήστες αναγνωρίζουν ότι έχουν διαβάσει, κατανοήσει και συμφωνήσει να συμμορφωθούν με αυτήν την πολιτική.

Προστασία προσωπικών δεδομένων (συμμόρφωση με GDPR & ISO 27701)

1. Σκοπός

Η παρούσα πολιτική καθορίζει τις αρχές και τις κατευθυντήριες γραμμές για την υπεύθυνη και νόμιμη χρήση των πληροφοριακών συστημάτων, δικτύων και πόρων του Ινστιτούτου , διασφαλίζοντας τη συμμόρφωση με τον GDPR και το ISO 27701 όσον αφορά την προστασία των προσωπικών δεδομένων. Σκοπός της είναι να μετριάσει τους κινδύνους που συνδέονται με μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις δεδομένων και κατάχρηση των προσωπικών δεδομένων, ενώ παράλληλα υποστηρίζει τη δέσμευση του Ινστιτούτου για προστασία της ιδιωτικής ζωής, της ασφάλειας και της κανονιστικής συμμόρφωσης.

2. Πεδίο εφαρμογής

Η παρούσα πολιτική ισχύει για όλους τους φοιτητές, το ερευνητικό προσωπικό, τους εργαζόμενους, τους εξωτερικούς συνεργάτες και τους τρίτους που έχουν πρόσβαση ή χρησιμοποιούν την υποδομή ΤΠ του Ινστιτούτου, τα αποθετήρια δεδομένων, τις υπηρεσίες cloud ή οποιαδήποτε συσκευή (συμπεριλαμβανομένων των προσωπικών συσκευών στο πλαίσιο του BYOD) που συνδέεται στο δίκτυο του Ινστιτούτου. Καλύπτει όλες τις μορφές επεξεργασίας προσωπικών δεδομένων, συμπεριλαμβανομένης της συλλογής, αποθήκευσης, διαβίβασης και διάθεσης, είτε μέσω συσκευών που παρέχονται από το Ινστιτούτο είτε μέσω προσωπικών συσκευών. Όλα τα πληροφοριακά συστήματα, οι ψηφιακές επικοινωνίες, οι λύσεις αποθήκευσης δεδομένων και τα σημεία πρόσβασης - είτε βρίσκονται στις εγκαταστάσεις είτε βασίζονται στο νέφος - πρέπει να συμμορφώνονται με τα πρότυπα GDPR και ISO 27701 για την προστασία της ιδιωτικής ζωής, την ασφάλεια και τη διακυβέρνηση των δεδομένων. Οποιοσδήποτε χειρισμός προσωπικών πρέπει να είναι ρητά εξουσιοδοτημένος, να παρακολουθείται και να τεκμηριώνεται, ώστε να διασφαλίζεται η συμμόρφωση με τις νομικές και θεσμικές απαιτήσεις.

3. Δήλωση της πολιτικής

Οι χρήστες πρέπει να διασφαλίζουν ότι δεν επεξεργάζονται, αποθηκεύουν ή διαβιβάζουν PII εκτός εάν έχουν λάβει ρητή εξουσιοδότηση και είναι απαραίτητο για ακαδημαϊκούς, ερευνητικούς ή διοικητικούς σκοπούς. Η χρήση των προσωπικών δεδομένων πρέπει να συμμορφώνεται με τις αρχές ελαχιστοποίησης των δεδομένων, και οι χρήστες πρέπει να χρησιμοποιούν κατάλληλους τεχνικά και οργανωτικά μέτρα (π.χ. κρυπτογράφηση, έλεγχοι πρόσβασης, ασφαλής πιστοποίηση ταυτότητας κλπ). Απαγορεύεται αυστηρά η μη εξουσιοδοτημένη πρόσβαση, τροποποίηση, κοινή χρήση ή αποθήκευση προσωπικών δεδομένων εκτός εγκεκριμένων και ασφαλών περιβαλλόντων. Όλοι οι χρήστες πρέπει να αναφέρουν αμέσως κάθε υποψία παραβίασης δεδομένων, μη εξουσιοδοτημένης πρόσβασης ή περιστατικών ασφαλείας.

Οι χρήστες πρέπει να τηρούν τις ακόλουθες αρχές όταν έχουν πρόσβαση ή επεξεργάζονται προσωπικά δεδομένα:

Νομιμότητα, αμεροληψία και διαφάνεια: Η επεξεργασία των ΠΔ πρέπει να γίνεται μόνο για νόμιμους, νόμιμους και ρητά καθορισμένους σκοπούς.

Ελαχιστοποίηση δεδομένων: Θα πρέπει να συλλέγονται, να υποβάλλονται σε επεξεργασία ή να αποθηκεύονται μόνο τα ελάχιστα απαραίτητα προσωπικά δεδομένα και η πρόσβαση θα πρέπει να περιορίζεται στο εξουσιοδοτημένο προσωπικό.

Ασφάλεια και εμπιστευτικότητα: Όλα τα προσωπικά δεδομένα πρέπει να κρυπτογραφούνται, να ελέγχονται ως προς την πρόσβαση και να προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή απώλεια. Κατά την

απομακρυσμένη πρόσβαση σε προσωπικά δεδομένα πρέπει να χρησιμοποιείται έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) και πρωτόκολλα ασφαλούς μετάδοσης.

Διατήρηση και διάθεση: Τα προσωπικά δεδομένα πρέπει να διατηρούνται μόνο για την τεκμηριωμένη και νομικά καθορισμένη περίοδο και να διαγράφονται με ασφάλεια όταν δεν χρειάζονται πλέον.

Αναφορά περιστατικών: Οποιαδήποτε ύποπτη ή επιβεβαιωμένη παραβίαση που αφορά PII πρέπει να αναφέρεται αμέσως σύμφωνα με το πρωτόκολλο αντιμετώπισης περιστατικών του Ινστιτούτου.

4. Οδηγίες χρήσης

- Έλεγχοι πρόσβασης: Η πρόσβαση στα PII χορηγείται με βάση την ανάγκη γνώσης, με ελέγχους πρόσβασης βάσει ρόλων (RBAC) και έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) που εφαρμόζονται όπου απαιτείται.
- Μετάδοση και αποθήκευση δεδομένων: Τα προσωπικά δεδομένα πρέπει να διαβιβάζονται με ασφάλεια (π.χ. κρυπτογραφημένο ηλεκτρονικό ταχυδρομείο, VPN) και να αποθηκεύονται μόνο σε εγκεκριμένες θέσεις αποθήκευσης. Οι υπηρεσίες cloud πρέπει να ελέγχονται για συμμόρφωση με τον GDPR πριν από τη χρήση.
- Διατήρηση και διάθεση δεδομένων: Τα προσωπικά δεδομένα πρέπει να διατηρούνται μόνο για την τεκμηριωμένη διάρκεια που είναι απαραίτητη για τον επιδιωκόμενο σκοπό τους. Κατά τη διάθεση των δεδομένων πρέπει να χρησιμοποιούνται ασφαλείς μέθοδοι διαγραφής για την αποτροπή μη εξουσιοδοτημένης ανάκτησης.
- Παρακολούθηση & έλεγχος: Το Ινστιτούτο διατηρεί το δικαίωμα να παρακολουθεί, να ελέγχει και να καταγράφει δραστηριότητες που σχετίζονται με την πρόσβαση και την επεξεργασία προσωπικών δεδομένων για να διασφαλίζει τη συμμόρφωση. Οι χρήστες οφείλουν να συνεργάζονται με τους ελέγχους ασφαλείας και τις έρευνες όταν απαιτείται.
- Χρήση προσωπικών συσκευών (BYOD): Εάν χρησιμοποιείται προσωπική συσκευή για πρόσβαση σε προσωπικά δεδομένα, πρέπει να λαμβάνεται ρητή γραπτή εξουσιοδότηση και οι χρήστες πρέπει να συμμορφώνονται με την πολιτική BYOD, συμπεριλαμβανομένης της εφαρμογής των απαιτούμενων μέτρων ασφαλείας.
- Απαγορευμένες δραστηριότητες: Οι χρήστες δεν πρέπει να μοιράζονται, να αποθηκεύουν ή να διαβιβάζουν προσωπικά δεδομένα εκτός εξουσιοδοτημένων συστημάτων, να χρησιμοποιούν προσωπικό ηλεκτρονικό ταχυδρομείο για ανταλλαγή ΠΔ ή να παρακάμπτουν τους ελέγχους ασφαλείας.
- Παρακολούθηση και συμμόρφωση: Όλες οι δραστηριότητες του συστήματος που σχετίζονται με προσωπικά δεδομένα υπόκεινται σε παρακολούθηση, καταγραφή και ελέγχους για τη διασφάλιση της συμμόρφωσης. Οι παραβάσεις της παρούσας πολιτικής μπορεί να οδηγήσουν σε πειθαρχικά μέτρα και νομικές συνέπειες.
- Ευθύνες χρηστών: Κάθε χρήστης που χειρίζεται προσωπικά δεδομένα πρέπει να ολοκληρώσει την υποχρεωτική εκπαίδευση για την προστασία των δεδομένων και να αναγνωρίσει το ρόλο του στην προστασία των ευαίσθητων πληροφοριών.
- Με την πρόσβαση στους πόρους πληροφορικής του Ινστιτούτου, οι χρήστες επιβεβαιώνουν την κατανόηση και την αποδοχή αυτών των υποχρεώσεων προστασίας των ΠΔ σύμφωνα με τον GDPR και το ISO 27701.

Πολιτική φυσικής μεταφοράς δεδομένων - (συμμόρφωση με ISO 27001:2022, GDPR & ISO 27701)

1. Σκοπός

Η παρούσα πολιτική καθορίζει τους μέτρα ασφαλείας και τις απαιτήσεις συμμόρφωσης για τη φυσική μεταφορά δεδομένων, είτε περιέχουν απλές είτε προσωπικά δεδομένα που μπορούν να ταυτοποιηθούν, εξασφαλίζοντας την εναρμόνιση με τα πρότυπα ISO 27001:2022, GDPR και ISO 27701. Αποσκοπεί στην πρόληψη μη εξουσιοδοτημένης πρόσβασης, παραβίασης δεδομένων, απώλειας ή αλλοίωσης κατά τη φυσική μεταφορά δεδομένων μέσω αφαιρούμενων μέσων, εκτυπωμένων εγγράφων, εξωτερικών μονάδων δίσκων ή άλλων φυσικών συσκευών αποθήκευσης.

2. Πεδίο εφαρμογής και πεδίο εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλους τους διδάσκοντες, το προσωπικό, τους φοιτητές, τους εργολάβους και τους τρίτους που μεταφέρουν δεδομένα με φυσικό τρόπο χρησιμοποιώντας οποιοδήποτε μέσο, συμπεριλαμβανομένων, ενδεικτικά, των μονάδων USB, των εξωτερικών σκληρών δίσκων, των CD/DVD, των έντυπων αρχείων, των φορητών υπολογιστικών συσκευών (φορητοί υπολογιστές, ταμπλέτες) και των εγγράφων σε χαρτί. Καλύπτει τόσο τις εσωτερικές μεταφορές εντός του Ινστιτούτου όσο και τις εξωτερικές μεταφορές σε τρίτους, προμηθευτές ή ρυθμιστικούς φορείς.

3. Δήλωση πολιτικής

Η φυσική μεταφορά απλών δεδομένων ή πρέπει να γίνεται μόνο όταν είναι απολύτως απαραίτητο και μόνο μέσω ασφαλών, εγκεκριμένων μεθόδων. Οι μη κρυπτογραφημένες ή μη ασφαλείς φυσικές μεταφορές απαγορεύονται αυστηρά. Τα προσωπικά δεδομένα δεν πρέπει να αντιγράφονται ή να μεταφέρονται, εκτός εάν υπάρχει ρητή εξουσιοδότηση, με τεκμηριωμένη αιτιολόγηση, περίοδο διατήρησης και έγκριση από τον ορισθέντα υπεύθυνο προστασίας δεδομένων (DPO) . Οποιαδήποτε φυσική μεταφορά δεδομένων πρέπει να καταγράφεται, να παρακολουθείται και να παρακολουθείται για τη διατήρηση της λογοδοσίας και την αποτροπή απώλειας δεδομένων ή μη εξουσιοδοτημένης αποκάλυψης.

4. Οδηγίες χρήσης

- Ταξινόμηση και έγκριση δεδομένων:
    - Πριν από κάθε φυσική μεταφορά, τα δεδομένα πρέπει να ταξινομούνται με βάση την ευαισθησία τους και η μεταφορά πρέπει να αιτιολογείται.
    - Για τη μεταφορά προσωπικών δεδομένων ή ευαίσθητων δεδομένων απαιτείται προηγούμενη γραπτή έγκριση από το αρμόδιο τμήμα ή τον υπεύθυνο προστασίας δεδομένων (DPO).
    - Οι εξωτερικές διαβιβάσεις προς τρίτους πρέπει να συμμορφώνονται με τους κανόνες του ΓΚΠΔ για τη διαβίβαση δεδομένων, συμπεριλαμβανομένης της υπογραφής κατάλληλων συμφωνιών επεξεργασίας δεδομένων (DPA).
- Εγκεκριμένα μέσα αποθήκευσης και μεταφοράς:
    - Μόνο εγκεκριμένα από το Ινστιτούτο κρυπτογραφημένα μέσα αποθήκευσης (π.χ. κρυπτογραφημένες μονάδες USB, εξωτερικοί δίσκοι με κρυπτογράφηση υλικού) μπορούν να χρησιμοποιούνται για τη μεταφορά ευαίσθητων δεδομένων.
    - Σε περίπτωση μεταφοράς εκτυπωμένων εγγράφων, αυτά πρέπει να αποθηκεύονται σε κλειδωμένα, απαραβίαστα δοχεία και να τα χειρίζεται μόνο εξουσιοδοτημένο προσωπικό.
    - Η μεταφορά φυσικών δεδομένων εκτός των εγκαταστάσεων του Ινστιτούτου πρέπει να τεκμηριώνεται και να παρακολουθείται, εξασφαλίζοντας ένα ελεγχόμενο αρχείο φύλαξης.

- Μέτρα κρυπτογράφησης και ασφάλειας:
    - Όλα τα ευαίσθητα δεδομένα ή τα προσωπικά δεδομένα πρέπει να κρυπτογραφούνται πριν από τη φυσική μεταφορά τους.
    - Για τις αφαιρούμενες συσκευές αποθήκευσης πρέπει να χρησιμοποιούνται ισχυρές μέθοδοι κρυπτογράφησης (AES-256 ή υψηλότερη).
    - Οι κωδικοί πρόσβασης για κρυπτογραφημένα αρχεία ή συσκευές πρέπει να αποστέλλονται χωριστά μέσω ασφαλούς καναλιού (π.χ. κρυπτογραφημένο ηλεκτρονικό ταχυδρομείο, ασφαλής πλατφόρμα ανταλλαγής μηνυμάτων).
- Φυσική ασφάλεια και μεταφορά:
    - Οι φυσικές συσκευές αποθήκευσης δεν πρέπει να αφήνονται αφύλακτες σε δημόσιους χώρους, οχήματα ή μη ασφαλείς περιοχές.
    - Κατά τη μεταφορά ευαίσθητων δεδομένων μέσω ταχυμεταφορών ή ταχυδρομικών υπηρεσιών, πρέπει να χρησιμοποιούνται συσκευασίες με προστασία από παραβίαση και το πακέτο πρέπει να αποστέλλεται μέσω υπηρεσίας παρακολούθησης και ασφαλούς παράδοσης.
    - Μόνο εξουσιοδοτημένο προσωπικό μπορεί να χειρίζεται φυσικές μεταφορές δεδομένων και πρέπει να υπογράφει δήλωση αναγνώρισης ευθύνης.
- Διατήρηση και διάθεση δεδομένων:
    - Τα φυσικά δεδομένα πρέπει να αποθηκεύονται μόνο για την απαραίτητη διάρκεια, σύμφωνα με τις τεκμηριωμένες πολιτικές διατήρησης.
    - Οποιαδήποτε ξεπερασμένα ή περιττά φυσικά δεδομένα πρέπει να απορρίπτονται με ασφάλεια με καταστροφή, αποτέφρωση ή πιστοποιημένες μεθόδους καταστροφής δεδομένων για μέσα αποθήκευσης.
    - Πρέπει να τηρείται ημερολόγιο διάθεσης για ελέγχους συμμόρφωσης.
- Αναφορά περιστατικών:
    - Οποιαδήποτε απώλεια, κλοπή ή μη εξουσιοδοτημένη πρόσβαση σε φυσικά μεταφερόμενα δεδομένα πρέπει να αναφέρεται αμέσως στον Υπεύθυνο Προστασίας Δεδομένων (DPO) και στον ΥΔΑΠ.
    - Το Ινστιτούτο θα διεξάγει έρευνα και, εάν είναι απαραίτητο, θα αναφέρει το περιστατικό στην αρμόδια Αρχή Προστασίας Δεδομένων σύμφωνα με τις απαιτήσεις του ΓΚΠΔ.