ΓΕΝΙΚΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

16.12.2022

ΥΠΕΥΘΥΝΟΣ ΠΟΛΙΤΙΚΗΣ	ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ	ΕΓΚΡΙΣΗ ΔΙΟΙΚΗΣΗΣ
Πρυτανικό Συμβούλιο Πανεπιστημίου Μακεδονίας	ΜΑΡΙΑ ΜΥΛΩΣΗ	*(Θέση – Υπογραφή)*

Ημερομηνία Έκδοσης
19.12.2022

ΠΙΝΑΚΑΣ ΑΝΑΘΕΩΡΗΣΕΩΝ

ΑΡΙΘΜΟΣ ΕΚΔΟΣΗΣ	ΗΜΕΡΟΜΗΝΙΑ	ΠΕΡΙΓΡΑΦΗ ΤΡΟΠΟΠΟΙΗΣΗΣ
2	19.12.2022	Επικαιροποιημένη Έκδοση-προσθήκες-διορθώσεις

ΕΙΣΑΓΩΓΗ

Η παρακάτω Πολιτική έχει εκπονηθεί ειδικά για το Πανεπιστήμιο Μακεδονίας και μπορεί να τροποποιείται όταν υπάρχουν αλλαγές στις διεργασίες του, οργανωτικές αλλαγές, αλλαγές στα πληροφοριακά συστήματα ή άλλες αλλαγές που επηρεάζουν τις λειτουργίες του Πανεπιστημίου.

Προϋπόθεση για την τροποποίηση και εφαρμογή της είναι, κατ' αρχήν ο έλεγχος των αλλαγών από τον Υπεύθυνο Προστασίας Δεδομένων και κατόπιν η έγκρισή της από τη Διοίκηση.

Η πολιτική αποτελείται από τρία (3) διακριτά στοιχεία τα οποία είναι:

α) Η Γενική πολιτική ασφαλείας

β) Τα παραρτήματα με τις ειδικές πολιτικές ασφαλείας και ειδικότερα τα κάτωθι:

1. Πολιτική Προσβάσεων και Απορρήτου Κωδικών Χρηστών
2. Πολιτική Τήλε-Εργασίας (vpn)
3. Πολιτική Προστασίας Hardware και Δεδομένων
4. Πολιτική Χρήσης Αφαιρούμενων Μέσων
5. Πολιτική Ασφαλείας Δικτύου και Συστημάτων
6. Πολιτική Αντιγράφων Ασφαλείας
7. Πολιτική Καθαρού Γραφείου και Καθαρής Οθόνης
8. Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων
9. Πολιτική Ορθής Χρήσης Σταθμών Εργασίας
10. Πολιτική Ασφαλούς Μεταφοράς Πληροφοριών
11. Πολιτική Ασφαλούς Αποστολής Μηνυμάτων Ηλεκτρονικού Ταχυδρομείου (e-mail)
12. Πολιτική B.Y.O.D.
13. Πολιτική Κατηγοριοποίησης Συστημάτων
14. Πολιτική Τηλεδιασκέψεων
15. Πολιτική Επικοινωνίας με τις Αρχές
16. Πολιτική Διαχείρισης Ασφάλειας σε Συμφωνίες με Τρίτους

Γ) Τα συνημμένα έγγραφα , όπου αυτά υφίστανται, τα οποία συνοδεύουν συγκεκριμένες ειδικές πολιτικές ασφάλειας.

Περιεχόμενα

Α. Γενική Πολιτική Ασφάλειας

1.1 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Το Σύστημα Διαχείρισης Ασφάλειας Δεδομένων (ΣΔΑΔ) εφαρμόζεται από όλες τις Διευθύνσεις / Τμήματα / Γραφεία του Πανεπιστημίου.

1.2 ΣΥΝΤΜΗΣΕΙΣ

ΓεΠΑΔ: Γενική Πολιτική Ασφάλειας Δεδομένων (το παρόν έγγραφο)

ΥΠΔ: Υπεύθυνος Προστασίας Δεδομένων

ΙΤ: Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

1.3 ΕΦΑΡΜΟΓΗ

Η ΓεΠΑΔ εφαρμόζεται από όλο το προσωπικό του Πανεπιστημίου που εμπλέκεται στην εκτέλεση των παρεχομένων υπηρεσιών, καθώς επίσης και στο χρησιμοποιούμενο εξοπλισμό, αλλά και στις εγκαταστάσεις που χρησιμοποιεί το Πανεπιστήμιο στα πλαίσια παροχής ή

εκτέλεσης των υπηρεσιών αυτών, συμπεριλαμβανομένων των όποιων πρόσθετων όρων των σχετικών συμβάσεων.

1.4 ΝΟΜΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ

Το Νομικό και Κανονιστικό πλαίσιο προσδιορίζεται από:

- Εσωτερικός Κανονισμός ΠΑ.ΜΑΚ. Συνεδρίαση Συγκλήτου 20/17.6.2021, δημοσιευθείσα στο ΦΕΚ 3457/29.7.2021 (τ. Β΄)
- Νόμος 4624/2019 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως τροποποιήθηκε και ισχύει συμπεριλαμβανομένων και των διατάξεων του Ν. 5002/2022)
- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
- Νόμος 3471/2006 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών).

Σημείωση: Το Πανεπιστήμιο δεσμεύεται όπως δεν αποδεχτεί οιονδήποτε συμβατικό όρο που παραβιάζει το ανωτέρω Νομικό και Κανονιστικό πλαίσιο.

1.5 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- ΙΤ
- Όλο το προσωπικό και οι εξωτερικοί συνεργάτες (όταν απαιτείται σε σχέση με τους τελευταίους).

1.6 ΣΚΟΠΟΣ

Το Πανεπιστήμιο επιδιώκει την παροχή των Υπηρεσιών σύμφωνα με το ισχύον Νομικό και Κανονιστικό πλαίσιο και τις λοιπές συμβατικές υποχρεώσεις του, με τρόπο που να προστατεύονται τα πληροφοριακά δεδομένα και ιδιαίτερα τα προσωπικά από εκούσια ή ακούσια κλοπή, καταστροφή, ή χρήση κατά παράβαση των Νόμων και των Κανονιστικών Διατάξεων.

Ο σκοπός της ασφάλειας των δεδομένων είναι να διασφαλίσει την επιχειρησιακή συνέχεια του οργανισμού και να ελαχιστοποιήσει τους κινδύνους που απειλούν τα δεδομένα, αποφεύγοντας

περιστατικά ασφαλείας και μειώνοντας τις επιπτώσεις που μπορεί να έχουν τα περιστατικά αυτά.

1.7 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Στόχος της παρούσας πολιτικής είναι να προστατέψει τα Πληροφοριακά Δεδομένα του οργανισμού από όλες τις εσωτερικές, εξωτερικές, εκούσιες ή ακούσιες απειλές.

Οι επιμέρους στόχοι του Πανεπιστημίου σχετικά με την Ασφάλεια των Δεδομένων είναι:

- Τα Πληροφοριακά Δεδομένα να είναι προστατευμένα από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση.
- Να διασφαλίζεται η εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και η διατήρηση των Πληροφοριακών Δεδομένων, όπως νομίμως προβλέπεται.
- Να τηρούνται πάντα οι αρχές της νομιμότητας, αντικειμενικότητας και διαφάνειας κατά την επεξεργασία των Πληροφοριακών Δεδομένων.
- Τα Πληροφοριακά Δεδομένα να συλλέγονται μόνο για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς.
- Τα Πληροφοριακά Δεδομένα να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- Να διασφαλίζεται η τήρηση των νομικών και κανονιστικών απαιτήσεων.
- Να παρέχεται εκπαίδευση πάνω στην Ασφάλεια των Δεδομένων για όλο το προσωπικό.
- Όλα τα πραγματικά ή καθ' υποψία περιστατικά ασφαλείας να αναφέρονται στον ΥΠΔ και να διερευνώνται πλήρως.

Για την επίτευξη των παραπάνω στόχων έχουν αναπτυχθεί και εφαρμόζονται επιμέρους Τεχνικά Μέτρα, Πολιτικές Ασφαλείας και Διαδικασίες, όπου περιγράφονται όλες οι σχετικές αρμοδιότητες του προσωπικού και οι οποίες διασφαλίζουν και αποδεικνύουν ότι η διαχείριση των πληροφοριακών δεδομένων διενεργείται σύμφωνα με το Νομικό και Κανονιστικό Πλαίσιο.

Τα εν λόγω Μέτρα, Πολιτικές και Διαδικασίες επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο, όπως για παράδειγμα μετά από εκτεταμένες αλλαγές στα πληροφοριακά συστήματα, βασικές αλλαγές στα προγράμματα (software), κλπ., και κατ' ελάχιστο ανά έτος. Υπεύθυνος για την επικαιροποίηση είναι ο ΥΠΔ, συμβουλευόμενος το αρμόδιο προσωπικό του Πανεπιστημίου, αναλόγως του αντικειμένου της επικαιροποίησης και εφόσον αυτό απαιτείται.

Κατά την επισκόπηση / επικαιροποίηση, όλα τα στοιχεία που συμβάλλουν στη διαμόρφωση μιας ολοκληρωμένης εικόνας του λειτουργικού περιβάλλοντος και των συστημάτων πληροφορικής του Πανεπιστημίου κατά την τρέχουσα περίοδο θα λαμβάνονται υπόψη.

Συγκεκριμένα στοιχεία που πρέπει να ληφθούν υπόψη είναι:

- Η τρέχουσα κατάσταση και το επίπεδο προληπτικών και διορθωτικών μέτρων ασφαλείας.
- Τα αποτελέσματα προηγούμενων ελέγχων ασφαλείας που έγιναν από τη διοίκηση ή από εξωτερικούς φορείς.
- Οι συστάσεις σχετικά με την ορθή εφαρμογή της συμμόρφωσης του προγράμματος ασφαλείας των συστημάτων πληροφοριών του οργανισμού, ώστε να παραμένει ευθυγραμμισμένο με τις κανονιστικές απαιτήσεις.

Όλο το προσωπικό και οι εξωτερικοί συνεργάτες (όταν αυτό απαιτείται), είναι υποχρεωμένοι να εφαρμόζουν τις Πολιτικές Ασφαλείας που διέπουν τη λειτουργία του οργανισμού και εμπίπτουν στο πεδίο των δραστηριοτήτων τους.

Η Διοίκηση δεσμεύεται για την παροχή όλων των απαραίτητων πόρων και μέσων για την εφαρμογή της παρούσας και των επιμέρους Πολιτικών Ασφαλείας.

1.8 ΑΡΜΟΔΙΟΤΗΤΕΣ

Προσδιορίζονται γενικά αρχές και κανόνες που σχετίζονται με την οργανωτική δομή και την οργανωτική διοίκηση των θεμάτων που σχετίζονται με την ασφάλεια των υπολογιστικών συστημάτων. Οι κύριοι ρόλοι που σχετίζονται με την ασφάλεια δεδομένων και τα συστήματα πληροφοριών, περιγράφονται στις ακόλουθες ενότητες.

1.8.1 Αρμοδιότητες διοίκησης

Οι βασικές αρμοδιότητες της Διοίκησης σε σχέση με τη διαχείριση της Ασφάλειας Δεδομένων στον οργανισμό είναι:

- Η διαμόρφωση της πολιτικής του Πανεπιστημίου σε σχέση με την Ασφάλεια Δεδομένων.
- Η έγκριση και η ανασκόπηση των Πολιτικών Ασφαλείας.
- Η έγκριση του Πλάνου Συμμόρφωσης και των Σχεδίων Διαχείρισης Εκτάκτων Αναγκών.
- Η διασφάλιση των πόρων που απαιτούνται για την αποτελεσματική εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Δεδομένων.

- Η δημιουργία των απαραίτητων συνθηκών στο Πανεπιστήμιο για την προώθηση της κατανόησης και εμπέδωσης από το προσωπικό του ρόλου και των ευθυνών του που συνδέονται με την Ασφάλεια Δεδομένων.
- Η μέριμνα για τη συνεχή βελτίωση του Συστήματος Διαχείρισης Ασφάλειας των Δεδομένων.

1.8.2 Αρμοδιότητες του Υπέυθυνου Προστασίας Δεδομενων

Πρόσωπο επικοινωνίας σε θέματα Ασφάλειας Δεδομένων είναι ο Υπέυθυνος Προστασίας Δεδομενων. Ο ΥΠΔ ορίζεται από τη Διοίκηση και επιπλέον των άλλων καθηκόντων, έχει τα καθήκοντα που αναφέρονται πιο κάτω.

Καθήκοντα ΥΠΔ:

- Διαμορφώνει την αρχιτεκτονική του οικοδομήματος προστασίας (by design & by default).
- Καταγράφει τις διαδικασίες συλλογής, αποθήκευσης, μεταβίβασης και επεξεργασίας των προσωπικών δεδομένων.
- Ενημερώνει και συμβουλεύει τη Διοίκηση του Πανεπιστημίου και το προσωπικό αυτού για τις υποχρεώσεις του που απορρέουν από το Νομικό και Κανονιστικό Πλαίσιο σχετικά με την προστασία δεδομένων όπως αυτά υφίστανται επεξεργασία από το προσωπικό του Πανεπιστημίου.
- Παρακολουθεί τη συμμόρφωση με το Νομικό και Κανονιστικό Πλαίσιο σχετικά με την προστασία δεδομένων και με τις πολιτικές του Πανεπιστημίου σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων.
- Μεριμνά για την ευαισθητοποίηση και εκπαίδευση του προσωπικού του Πανεπιστημίου σε θέματα Ασφάλειας Δεδομένων, Πολιτικών και Διαδικασιών και απαιτήσεων Νομικού και Κανονιστικού Πλαισίου.
- Οργανώνει, συντάσσει εκθέσεις αποτίμησης κινδύνου (Privacy Impact Assessments).
- Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την Εκτίμηση Αντικτύπου και Επικινδυνότητας, σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της.
- Συνεργάζεται με εποπτικές αρχές και επικοινωνεί με την εποπτικές αρχές για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της διαβούλευσης.

- Σχεδιάζει εσωτερικές διαδικασίες & εργαλεία συμμόρφωσης.
- Αναπτύσσει Πολιτικές Ασφαλείας, διαδικασιών και πρότυπων μεθόδων, σύμφωνα με την Γενική Πολιτική Ασφάλειας Δεδομένων του οργανισμού.
- Μεριμνά για την εφαρμογή, διατήρηση και παρακολούθηση των Πολιτικών Ασφάλειας, ώστε να διασφαλίζεται η τήρηση των νομικών και κανονιστικών απαιτήσεων, της εκάστοτε ισχύουσας νομοθεσίας και των απαιτήσεων των προτύπων.
- Ενημερώνει τη Διοίκηση για την επίδοση και βελτίωση των Πολιτικών Ασφάλειας.
- Ελέγχει τον κατάλογο πληροφοριακών στοιχείων του οργανισμού και τη διαβάθμιση της σπουδαιότητάς τους (ΕΠ.05.01 ΜΗΤΡΩΟ ΣΥΣΚΕΥΩΝ).
- Σχεδιάζει διαδικασίες αντιμετώπισης κινδύνων / παραβιάσεων / λοιπών περιστατικών και ενημέρωσης υποκειμένων.
- Καταγράφει οποιοδήποτε περιστατικό ασφαλείας και ενεργοποιεί το αντίστοιχο σχέδιο και στρατηγική για την αντιμετώπιση και την αποφυγή επανεμφάνισής του.
- Λογοδοτεί στα υποκείμενα επεξεργασίας εάν χρειαστεί.
- Παρακολουθεί την αποτελεσματικότητα των ελέγχων που εφαρμόζονται για την αντιμετώπιση των κινδύνων.

Ο ΥΠΔ αναφέρεται απευθείας στη Διοίκηση του Πανεπιστημίου για όλα τα θέματα σχετικά με την Ασφάλεια Δεδομένων και είναι εξουσιοδοτημένος να ενεργεί για λογαριασμό της σχετικά με αυτά.

1.8.3 Αρμοδιότητες Υπεύθυνου Προϊσταμένου Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

Ο υπεύθυνος του Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής είναι ένας υπάλληλος που είναι επιφορτισμένος με τη συνολική διαχείριση των συστημάτων υπολογιστών του Πανεπιστημίου. Ο υπεύθυνος διαχειριστής συνεργάζεται με το προσωπικό του Κέντρου Υπολογιστών και Δικτύου, προκειμένου να επιβάλει τα μέτρα ασφαλείας των συστημάτων και εφαρμογών του οργανισμού.

Μερικές από τις βασικές ευθύνες σχετικά με την ασφάλεια των συστημάτων πληροφορικής είναι:

- Η διατήρηση αντιγράφων ασφαλείας.
- Η ενεργοποίηση διαμόρφωσης ασφαλείας στα συστήματα (λειτουργικά συστήματα, εφαρμογές,
- βάσεις δεδομένων, δίκτυα) βάσει μεμονωμένων διαδικασιών.

- Η εφαρμογή της πολιτικής ασφάλειας και των μεμονωμένων διαδικασιών.
- Η αντιμετώπιση συμβάντων ασφαλείας.
- Η ανανέωση συστημάτων με βάση τις τελευταίες εκδόσεις ασφαλείας (ενημερώσεις λειτουργικών, ενημερώσεις κώδικα, επείγουσες επιδιορθώσεις, νέες εκδόσεις).
- Η παρακολούθηση και συντήρηση των εγκατεστημένων συστημάτων ασφαλείας (π.χ. Antivirus, IPS, λογισμικό παρακολούθησης κίνησης δικτύου, εργαλεία παρακολούθησης logging, κ.λπ.).

1.8.4 Αρμοδιότητες προσωπικού

Οι βασικές αρμοδιότητες του εμπλεκόμενου στο Σύστημα Διαχείρισης Ασφάλειας Δεδομένων προσωπικού σε σχέση με τη διαχείριση της Ασφάλειας Δεδομένων του Πανεπιστημίου είναι:

- Η εφαρμογή των Πολιτικών Ασφαλείας, των σχετικών διαδικασιών και οδηγιών εργασίας που εμπίπτουν κατά την εκτέλεση της εργασίας του.
- Η άμεση αναφορά στον ΥΠΔ, οποιουδήποτε περιστατικού ασφαλείας εμπίπτει στην αντίληψή του.

1.9 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

Ουδέν

1.10 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Οργανόγραμμα Πανεπιστημίου	Ηλεκτρονική	Επ’ αόριστον	ΥΠΔ

Β. ΠΑΡΑΡΤΗΜΑΤΑ

Ι. Ειδικές Πολιτικές Ασφάλειας

1. Πολιτική Προσβάσεων και Απορρήτου Κωδικών Χρηστών
2. Πολιτική Τηλε-Εργασίας (vpn)
3. Πολιτική Προστασίας Hardware και Δεδομένων
4. Πολιτική Χρήσης Αφαιρούμενων Μέσων
5. Πολιτική Ασφαλείας Δικτύου και Συστημάτων
6. Πολιτική Αντιγράφων Ασφαλείας
7. Πολιτική Καθαρού Γραφείου και Καθαρής Οθόνης
8. Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων
9. Πολιτική Ορθής Χρήσης Σταθμών Εργασίας
10. Πολιτική Ασφαλούς Μεταφοράς Πληροφοριών
11. Πολιτική Ασφαλούς Αποστολής Μηνυμάτων Ηλεκτρονικού Ταχυδρομείου (e-mail)
12. Πολιτική B.Y.O.D.
13. Πολιτική Κατηγοριοποίησης Συστημάτων
14. Πολιτική Τηλεδιασκέψεων

ΙΙ. Λίστα Προγραμμάτων

1. Εγκεκριμένα

2. Πρόσθετα

ΠΑΡΑΡΤΗΜΑ Ι

Ειδικές Πολιτικές Ασφάλειας Δεδομένων

1. Πολιτική Προσβάσεων και Απορρήτου Κωδικών Χρηστών

1.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγράψει τη μεθοδολογία που ακολουθείται στη χρήση των κωδικών από τους χρήστες τους. Ιδιαίτερα περιγράφονται οι μέθοδοι που εφαρμόζονται για τη διαχείριση αυτών των κωδικών στο Πανεπιστήμιο. Επίσης περιγράφονται οι λογικές προσβάσεις που υπάρχουν στο Πανεπιστήμιο και ο τρόπος πρόσβασης των υπηρεσιών αυτών από τους χρήστες.

1.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται για τους κωδικούς πρόσβασης όλων των χρηστών στους προσωπικούς σταθμούς εργασίας, στο εσωτερικό δίκτυο του Πανεπιστημίου, για την πρόσβαση στο διαδίκτυο και την ειδική πρόσβαση σε εξειδικευμένες εφαρμογές.

Η ανασκόπηση των δικαιωμάτων των χρηστών που απορρέουν από την παρούσα πολιτική ορίζεται ότι θα εκτελείται σε ετήσια βάση.

1.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- Προσωπικό Πανεπιστημίου (διοικητικό-εκπαιδευτικό)
- Εξωτερικοί Συνεργάτες

1.4 Δικαιώματα ηλεκτρονικών προσβάσεων

Τα δικαιώματα ηλεκτρονικών προσβάσεων στο Πανεπιστήμιο είναι διαφόρων ειδών και απαριθμούνται ακολούθως:

1. Πρόσβαση στο λειτουργικό σύστημα στους σταθμούς εργασίας
2. Πρόσβαση σε υπηρεσία e-mail
3. Πρόσβαση σε ειδικές εφαρμογές:

a) Cardisoft (λογισμικό διαχείρισης στοιχείων φοιτητών)
b) RESCOM (λογισμικό διαχείρισης έργων χρησιμοποιούμενο από ΕΛΚΕ)
c) OTS (λογισμικό διαχείρισης προσωπικού)

Οι παραπάνω προσβάσεις αφορούν τα στελέχη και το προσωπικό που εργάζεται στο Πανεπιστήμιο. Οι προσβάσεις αυτές καταγράφονται στο έντυπο προσβάσεων χρηστών (Έντυπο Προσβάσεων Χρηστών ΕΠ.01.01).

Επίσης, ειδική ηλεκτρονική πρόσβαση μπορεί να έχουν οι εξωτερικοί συνεργάτες με τους οποίους υπάρχει συγκεκριμένη σύμβαση έργου (π.χ. ανάπτυξη λογισμικού, παροχή συμβουλευτικών υπηρεσιών, κτλ). Στην περίπτωση αυτή ακολουθείται η ιδία διαδικασία για την έγκριση των προσβάσεων όπως αυτή που ισχύει για τα στελέχη και τους υπαλλήλους του οργανισμού και συμπληρώνεται και η Ατομική Καρτέλα Προσβάσεων Χρηστών. Η πρόσβαση εξωτερικών συνεργατών πρέπει να διακόπτεται άμεσα μετά την ολοκλήρωση του έργου για το οποίο δόθηκε.

1.4.1 Πρόσβαση στο λειτουργικό σύστημα και στο εσωτερικό δίκτυο

Τα δικαιώματα πρόσβασης σε λειτουργικό σύστημα κάθε προσωπικού σταθμού εργασίας ελέγχονται με κατάλληλο κωδικό, τον οποίο δημιουργεί ο ίδιος ο χρήστης κατά την πρώτη πρόσβαση (σε περιβάλλον domain) και εναλλακτικά από τον IT (σε περιβάλλον workgroup). Όταν πρόκειται για root χρήστη συστήματος η ανάθεση του κωδικού γίνεται από τον IT. Ο κωδικός είναι μοναδικός και γνωστός μόνο στον ίδιο τον χρήστη.

1.4.2 Πρόσβαση σε ηλεκτρονικό ταχυδρομείο (email)

Τα δικαιώματα πρόσβασης στους λογαριασμούς ηλεκτρονικού ταχυδρομείου του Πανεπιστημίου ελέγχονται με κρυπτογραφημένο συνθηματικό, το οποίο είναι αυστηρά προσωπικό ανά χρήστη. Σε περίπτωση απώλειας του συνθηματικού, για οποιονδήποτε λόγο, η επανέκδοσή του γίνεται με ενέργειες της αρμόδιας υπηρεσίας του Πανεπιστημίου.
Οι λογαριασμοί του ακαδημαϊκού και διοικητικού προσωπικού, μετά την αποχώρησή του, διατηρούνται για όσο χρονικό διάστημα απαιτηθεί ώστε να διεκπεραιωθούν οι ακαδημαϊκές και υπηρεσιακές εκκρεμότητες.
Για τους λογαριασμούς ηλεκτρονικού ταχυδρομείου των αποφοίτων του Πανεπιστημίου ακολουθείται η παρακάτω διαδικασία:
α) διατηρούνται ενεργοί για ένα έτος μετά την αποφοίτηση. Στη διάρκεια αυτού του έτους ο χρήστης θα λάβε δύο ειδοποιήσεις για την επικείμενη κατάργηση,

β) ακολουθεί ένα μήνας αναστολής λειτουργίας του λογαριασμού, στη διάρκεια της οποίας ο χρήστης δεν έχει πρόσβαση στο λογαριασμό του, αλλά τα δεδομένα διατηρούνται,
γ) μετά την παρέλευση του χρονικού διαστήματος της αναστολής, ο λογαριασμός διαγράφεται οριστικά χωρίς δυνατότητα επαναφοράς.

1.4.3 Πρόσβαση στο διαδίκτυο

Τα δικαιώματα πρόσβασης στο διαδίκτυο ελέγχονται από τον Προϊστάμενο του Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής του Πανεπιστημίου και δεν απαιτείται η χρήση κωδικού. Περαιτέρω έλεγχος της πρόσβασης σε διάφορους ιστότοπους μπορεί να εκτελείται μέσω ειδικής εφαρμογής φιλτραρίσματος περιεχομένου (Content Filtering).

1.4.4 Πρόσβαση σε Εφαρμογές (ERP, κλπ.)

Στο Πανεπιστήμιο λειτουργούν διάφορα πληροφοριακά συστήματα και εφαρμογές που ελέγχονται από την αρμόδια για την υλοποίηση Διεύθυνση. Οι χρήστες των συστημάτων αυτών έχουν κωδικό πρόσβασης ο οποίος είναι μοναδικός και προσωπικός. Αρμόδιος για τη διαχείριση των κωδικών πρόσβασης, είναι αυτός που ορίζεται από την κάθε Διεύθυνση ως διαχειριστής του συστήματος, ο οποίος θα πρέπει να διατηρεί μητρώο των χρηστών που έχουν πρόσβαση στο σύστημα καταγράφοντας και τα δικαιώματα που έχουν (ανάγνωση ή/και μεταβολή ή/και δημιουργία ή/και διαγραφή πληροφοριών), στο έντυπο ΕΠ.02 Έντυπο Προσβάσεων Εφαρμογής.

1.5 Διαχείριση των κωδικών

Οι κωδικοί είναι προσωπικοί δεν πρέπει να γνωστοποιούνται ή να κοινοποιούνται σε καμία περίπτωση. Τα ηλεκτρονικά μέσα στα οποία έχει πρόσβαση ο κάθε χρήστης καταγράφονται στο Έντυπο ΕΠ.01.01 «Έντυπο Προσβάσεων Χρηστών» με ευθύνη του Υπεύθυνου Προστασίας Δεδομένων και σε συνεργασία με τον Υπεύθυνο Διαχείρισης Πληροφοριακών Συστημάτων και Δικτύων. Το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής του Πανεπιστημίου, ενημερώνει τον χρήστη ότι ο κωδικός είναι αυστηρά προσωπικός. Για τη διασφάλιση του αυστηρά προσωπικού κωδικού το ως άνω Τμήμα φροντίζει να είναι ενεργοποιημένη η επιλογή για αλλαγή κωδικού πριν από την πρώτη είσοδο. Ο κάθε χρήστης φέρει την ευθύνη για τη διαφύλαξη των προσωπικών του κωδικών ασφαλείας. Σε περίπτωση απώλειας κάποιου κωδικού ή/και σε περίπτωση υποψίας υποκλοπής κωδικού, ο χρήστης ενημερώνει άμεσα τον αρμόδιο υπάλληλο του σχετικού πληροφοριακού συστήματος (help

desk του Πανεπιστημίου), ο οποίος αρχικοποιεί τη διαδικασία επιλογής κωδικού, ώστε να μπορεί ο χρήστης να ορίσει νέο κωδικό.

Το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής του Πανεπιστημίου, πρέπει να ενημερώνει τους χρήστες για τις οδηγίες που θα πρέπει να ακολουθούν έτσι ώστε να αποτρέψουν την υποκλοπή των κωδικών τους. Οι οδηγίες αυτές είναι :

- *Να μη χρησιμοποιούν εύκολα προβλέψιμους κωδικούς (π.χ. ονοματεπώνυμα, ημερομηνία γεννήσεως κ.λπ.)*
- *Να διαμορφώνουν τους κωδικούς ώστε να περιέχουν συνδυασμό από γράμματα, σύμβολα και αριθμούς.*
- *Να απομνημονεύουν τους κωδικούς και μην τους καταγράφουν σε μέρη που μπορεί να υποκλαπούν (ατζέντες, σημειωματάρια κ.λπ.)*
- *Να αλλάζουν συχνά τους κωδικούς.*

Οι ανωτέρω αρχές για την διαχείριση των κωδικών ισχύουν και στην περίπτωση των πληροφοριακών συστημάτων με ευθύνη του αρμόδιου διαχειριστή του Συστήματος.

1.6 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

- ΕΠ.01.01 Έντυπο Προσβάσεων Χρηστών
- ΕΠ.01.02 Έντυπο Προσβάσεων Εφαρμογής
- ΕΠ.01.03 Έντυπο Δικαιωμάτων Πρόσβασης Χρήστη

1.7 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Έντυπο Ατομική Καρτέλα Προσβάσεων ΕΠ.01.01	Έντυπη / Ηλεκτρονική	Επ' αόριστον	Προϊστάμενος του Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
Έντυπο Προσβάσεων	Έντυπη / Ηλεκτρονική	Επ' αόριστον	Προϊστάμενος του Τμήματος Στατιστικής,

Εφαρμογής ΕΠ.01.02			Μηχανοργάνωσης και Πληροφορικής
Έντυπο Δικαιωμάτων Πρόσβασης Χρήστη ΕΠ.01.03	Έντυπη / Ηλεκτρονική	Επ' αόριστον	Προϊστάμενος του Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

2 Πολιτική Απομακρυσμένης Σύνδεσης (VPN)

2.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφεί η μεθοδολογία διασύνδεσης από απομακρυσμένους υπολογιστές στο εσωτερικό δίκτυο και στα υπολογιστικά συστήματα του οργανισμού.

2.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται για όλα τα μέσα που δύνανται να συνδέονται στο δίκτυο του Πανεπιστημίου, ήτοι διαδραστικές οθόνες, φορητοί υπολογιστές (laptops), κινητά τηλέφωνα, tablets κλπ.

2.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- ΔΙΟΙΚΗΣΗ ΠΑΝΕΠΙΣΤΗΜΙΟΥ

2.4 Χρήση Συσκευών που χορηγεί το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

Η σύνδεση μπορεί να εκτελείται μόνο από εγκεκριμένες, από το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής συσκευές. Μετά την έγκριση χρήσης οποιασδήποτε συσκευής, τυχόν τροποποιήσεις και εγκαταστάσεις νέων προγραμμάτων γίνονται με την συνδρομή του ως άνω Τμήματος. Οι εξουσιοδοτημένες συσκευές μπορεί να ελέγχονται ανά τακτά χρονικά διαστήματα από τον ΙΤ. Σε περίπτωση που οι χρήστες χρησιμοποιούν ιδιωτικό

εξοπλισμό, οφείλουν να συμμορφώνονται με τα πρότυπα ασφάλειας του Πανεπιστημίου. Ειδικά οι φορητές συσκευές οποιασδήποτε μορφής (κινητά τηλέφωνα, laptops, tablets, κλπ) που συνδέονται με δυναμική IP διεύθυνση στο δίκτυο έχουν διαφορετικά δικαιώματα πρόσβασης.

2.4.1 Ρυθμίσεις συσκευής

Για να μπορεί να συνδεθεί μια συσκευή απομακρυσμένα στο δίκτυο του Πανεπιστημίου με την υλοποίηση της τεχνολογίας vpn, θα πρέπει η συσκευή να ελεγχθεί από τον IT ότι καλύπτει ορισμένα ελάχιστα κριτήρια ασφάλειας.

2.4.2 Ελάχιστα κριτήρια ασφάλειας Η/Υ

Σαν ελάχιστα κριτήρια ασφάλειας ορίζονται τα παρακάτω:

Α. Λειτουργικό σύστημα:

Windows 10, έκδοση 1809 και νεότερη
Android έκδοση 6.0 (Marshmallow) ή iOS έκδοση 11 για κινητές συσκευές

Β. Ισχυρός κωδικός log-in χρήστη, όπως προβλέπεται από την Πολιτική Απορρήτου Κωδικών Χρηστών (Παράρτημα Α1 παρόντος).

Γ. Εγκατεστημένο πρόγραμμα antivirus

Δ. Ενεργό firewall (μόνο για υπολογιστές)

2.4.3 Ρυθμίσεις ασφαλείας vpn σύνδεσης

Όπου είναι εφικτό η σύνδεση πρέπει να ασφαλίζεται με τη χρήση ιδιωτικού / δημόσιου κλειδιού.

Για την εξασφάλιση της ασφαλούς σύνδεσης θα πρέπει να ρυθμιστεί η επίτευξη της να υλοποιείται με την χρήση του ασφαλούς πρωτοκόλλου (παράδειγμα IPSec, SSLVPN).

Με τη χρήση της VPN τεχνολογίας με προσωπικό εξοπλισμό, οι χρήστες θα πρέπει να κατανοήσουν ότι τα μηχανήματα που χρησιμοποιούν για την πραγματοποίηση της σύνδεσης τους, καθίστανται προέκταση του δικτύου του Πανεπιστημίου. Συνέπεια αυτού είναι ότι πρέπει να ακολουθούν τις πολιτικές ασφαλείας του Πανεπιστημίου και ο ιδιωτικός εξοπλισμός τους υπόκειται στους ίδιους κανόνες που εφαρμόζονται για τον εξοπλισμό του Πανεπιστημίου.

2.5 Συνημμένα έντυπα

3 Πολιτική Προστασίας Hardware και Δεδομένων

3.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγράψει τα μέσα και τις μεθόδους που χρησιμοποιούνται για τη φυσική προστασία του Hardware που χρησιμοποιείται από τον οργανισμό, καθώς επίσης και για την προστασία των δεδομένων που είναι αποθηκευμένα στα υπολογιστικά συστήματα του.

3.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε προσωπικούς σταθμούς εργασίας, σε laptops και servers ιδιοκτησίας του οργανισμού.

3.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- ΔΙΟΙΚΗΣΗ

3.4 ΠΕΡΙΓΡΑΦΗ

3.4.1 Φυσική προστασία Hardware

Η περιγραφόμενη πολιτική φυσικής προστασίας του Hardware περιλαμβάνει μέτρα που διασφαλίζουν τη λειτουργικότητα του συστήματος στις κάτωθι περιπτώσεις:

- Διακύμανση / πτώση ηλεκτρικού ρεύματος
- Συνθήκες λειτουργίας (θερμοκρασία και υγρασία)
- Πυρκαγιά
- Βλάβη σε επιμέρους Hardware component (πχ δίσκος, μνήμη, κάρτα)
- Απώλεια δεδομένων από λογική διαγραφή τους (εσκεμμένη ή από αμέλεια)

3.4.2 Datacenters

Τα συστήματα που είναι εγκατεστημένα σε Datacenters εξωτερικών συνεργατών του Πανεπιστημίου είναι το GUNET και το GRNET στις εγκαταστάσεις του GRNET καλύπτονται

από τη σύμβαση παροχής υπηρεσιών με ετήσια συνδρομή προς το GUNET, του οποίου το Πανεπιστήμιο είναι μέλος.

Στα πλαίσια των συμβάσεων, οι εξωτερικοί συνεργάτες θα πρέπει να αναλαμβάνουν:

- Την παροχή αδιάλειπτης παροχής ηλεκτρικής τάσης με χρήση UPS και γεννήτριας επαρκούς φορτίου.
- Τη διατήρηση ιδανικών συνθηκών θερμοκρασίας και υγρασίας.
- Την παροχή επαρκούς πυροπροστασίας.
- Την ελεγχόμενη πρόσβαση

ΣΗΜΕΙΩΣΗ: Όλες οι παραπάνω απαιτήσεις θα πρέπει να αποτυπώνονται και στη σύμβαση με τον συνεργάτη

3.4.3 Διόρθωση/επισκευή βλαβών

Στην περίπτωση που ένα σύστημα τεθεί εκτός λειτουργίας χωρίς να υπάρχει δυνατότητα αποτροπής της βλάβης, με μέριμνα του IT εξετάζεται κατά πόσον αυτό μπορεί να επισκευαστεί με ίδια μέσα. Εφόσον η επισκευή απαιτεί κόστος, ελέγχεται η ύπαρξη εγγύησης. Εφόσον η εγγύηση είναι σε ισχύ, ενημερώνεται ο ανάδοχος ο οποίος πρέπει να προβεί στην επιδιόρθωση της βλάβης βάσει των συμβατικών υποχρεώσεών του. Αν η εγγύηση έχει λήξει, πραγματοποιείται αίτημα δέσμευσης δαπάνης για την επιδιόρθωση αναλόγως των διαθέσιμων πόρων.

3.5 Προστασία δεδομένων

Για την προστασία των δεδομένων που βρίσκονται αποθηκευμένα στα υπολογιστικά συστήματα του οργανισμού χρησιμοποιούνται τα ακόλουθα μέτρα:

- Κρυπτογράφηση των βάσεων δεδομένων των εξυπηρετητών (όπου κρίνεται σκόπιμο, βάσει διενέργειας εκτίμησης επικινδυνότητας και είναι εφικτό).
- Εγκατάσταση Firewall.

- Έλεγχος πρόσβασης όπως περιγράφεται στο Παράρτημα Α1, Πολιτική Προσβάσεων και Απορρήτου Κωδικών.
- Τήρηση αντιγράφων ασφαλείας όπως περιγράφεται στο Παράρτημα Α8, Πολιτική Αντιγράφων Ασφαλείας.
- Εγκατάσταση και λειτουργία antivirus & antispam: Ο IT είναι αρμόδιος για την εγκατάσταση λογισμικού antivirus και antispam στους servers. Η ενημέρωση των εφαρμογών antivirus και antispam θα γίνεται αυτόματα τουλάχιστον σε ημερήσια βάση, ενώ θα πρέπει να εκτελείται και περιοδικός έλεγχος της ενημέρωσης του antivirus.

3.6 Προστασία & Αποτροπή Ιών

1. Όλοι οι σταθμοί εργασίας (Workstations και laptops) έχουν εγκατεστημένο το *Antivirus (Microsoft Essentials ή όποιο άλλο ορίσει το τμήμα IT).*
2. Με κάθε εγκατάσταση νέου σταθμού εργασίας γίνεται εγκατάσταση του *εκάστοτε ενδεδειγμένο Antivirus* και λαμβάνονται τα τελευταία Definition Updates.
3. Το χρησιμοποιούμενο λογισμικό antivirus είναι ρυθμισμένο να εκτελεί Quick Scan και ενημέρωση, κάθε 7 ημέρες στους σταθμούς εργασίας ή και χειροκίνητα όποτε επιλέξει ο χρήστης ή ο διαχειριστής.

3.7 Firewall Desktop PC’s & Laptops

3.7.1 Firewall

Στα Desktops και Laptops έχει ενεργοποιηθεί το firewall του λειτουργικού συστήματος (Microsoft firewall).

3.7.2 Εγκατάσταση και λειτουργία antivirus & antispam

Ο IT είναι αρμόδιος για την εγκατάσταση λογισμικού antivirus και antispam στους φορητούς και τους προσωπικούς σταθμούς εργασίας του προσωπικού. Η ενημέρωση των virus definitions θα γίνεται αυτόματα σε ημερήσια βάση, ενώ ο IT είναι αρμόδιος για τον περιοδικό έλεγχο της ενημέρωσης του antivirus.

Στους σταθερούς σταθμούς εργασίας (PC), έχει εγκατασταθεί το *Antivirus (Microsoft Essentials ή όποιο άλλο ορίσει το τμήμα IT).* το οποίο ενημερώνεται αυτόματα από το site του προμηθευτή.

3.7.3 Καθορισμός δικαιωμάτων πρόσβασης

Σε κάθε σταθερό και φορητό ηλεκτρονικό υπολογιστή καθορίζονται δικαιώματα (κωδικοί) πρόσβασης στον υπολογιστή και πρόσβασης στο δίκτυο. Τα σχετικά με τα δικαιώματα πρόσβασης περιγράφονται στο Παράρτημα Α1. (Πολιτική Προσβάσεων και Απορρήτου Κωδικών Χρηστών – Π.01).

3.8 Κρυπτογράφηση

Η κρυπτογράφηση δεδομένων χρησιμοποιείται στην ηλεκτρονική αλληλογραφία και στα κινούμενα δεδομένα (όχι στα αποθηκευμένα).

Στην ιστοσελίδα του Πανεπιστημίου και όσες φιλοξενούνται σε διακομιστές του Πανεπιστημίου προστατεύονται από το πρωτόκολλο Secure Socket Layer (SSL).

Περισσότερες λεπτομέρειες σχετικά με τις μορφές κρυπτογράφησης για τον οργανισμό, παραθέτονται στην Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων (Π.08).

3.9 Συνημμένα Έντυπα

Ουδέν

4 Πολιτική Χρήσης Συσκευών και Αφαιρούμενων Μέσων

4.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφεί η μεθοδολογία διαχείρισης των φορητών μέσων που επεξεργάζονται, αποθηκεύουν ή δύνανται να έχουν πρόσβαση σε δεδομένα που είναι αποθηκευμένα στα υπολογιστικά συστήματα του οργανισμού.

4.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε όλα τα φορητά μέσα που δύνανται να επεξεργάζονται / διαχειρίζονται / αποθηκεύουν πληροφοριακά δεδομένα, ήτοι φορητοί υπολογιστές (laptops), κινητά τηλέφωνα και αφαιρούμενοι δίσκοι και μέσα (εξωτερικοί δίσκοι, CDs, DVDs, USB flash disks κλπ).

4.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- Προσωπικού Πανεπιστημίου (διοκητικό-εκπαιδευτικό)

4.4 ΠΕΡΙΓΡΑΦΗ

4.4.1 Χρήση Laptops

Επιτρέπεται η χρήση ιδιωτικών φορητών υπολογιστών υπό την προϋπόθεση ότι η χρήστης τους ακολουθεί τα πρότυπα ασφάλειας του Πανεπιστημίου. Ειδικά οι φορητές συσκευές οποιασδήποτε μορφής (κινητά τηλέφωνα, laptops, tablets, κλπ) που συνδέονται με δυναμική IP διεύθυνση στο δίκτυο έχουν διαφορετικά δικαιώματα πρόσβασης.

4.4.2 Χρήση Κινητών Τηλεφώνων

Η χρήση των κινητών τηλεφώνων από το διοικητικό και εκπαιδευτικό προσωπικό προβλέπεται υπό την προϋπόθεση που συνδέονται με δυναμική IP διεύθυνση στο δίκτυο έχουν διαφορετικά δικαιώματα πρόσβασης.

4.4.3 Χρήση Αφαιρούμενων Δίσκων και μέσων (εσωτερικοί και εξωτερικοί δίσκοι, CDs, DVDs, USB flash disks κλπ)

Επιτρέπεται στο προσωπικό η εγγραφή μόνο πληροφοριακών δεδομένων που δεν έχουν χαρακτηρισθεί ως εμπιστευτικά ή απόρρητα, σε εξωτερικούς δίσκους ή αποθηκευτικά μέσα οποιασδήποτε μορφής και η μεταφορά του φορητού μέσου αποθήκευσης εκτός των χώρων του Πανεπιστημίου.

Δεν επιτρέπεται στο προσωπικό η εγγραφή πληροφοριακών δεδομένων που έχουν χαρακτηρισθεί σαν εμπιστευτικά σε εξωτερικούς δίσκους ή αποθηκευτικά μέσα οποιασδήποτε μορφής και η μεταφορά του φορητού μέσου αποθήκευσης εκτός των χώρων του οργανισμού χωρίς εξουσιοδότηση / άδεια από τον Διευθυντή της Διεύθυνσης.

Η μόνη μεταφορά πληροφοριακών δεδομένων που επιτρέπεται είναι, εάν απαιτείται αποθήκευση του Backup σε εξωτερικό χώρο.

Έγγραφα που έχουν χαρακτηρισθεί ως απόρρητα απαγορεύεται να μεταφερθούν με φορητό αποθηκευτικό μέσο εάν αυτό δεν είναι κρυπτογραφημένο.

Τα αφαιρούμενα μέσα εφόσον είχαν αποθηκευμένα δεδομένα, αυτά διαγράφονται οριστικά με ενέργειες του προσωπικού του ΚΥΔ (δεν υπάρχει δυνατότητα ανάκτησής τους) και είτε επαναχρησιμοποιούνται εφόσον βρίσκονται σε λειτουργική κατάσταση, είτε αποσύρονται. Σε περίπτωση που η οριστική διαγραφή των δεδομένων δεν είναι εφικτή (βλάβη του μέσου), αυτό καταστρέφεται με φυσικό τρόπο και αποσύρεται για ανακύκλωση.

5 Πολιτική Ασφαλείας Δικτύου και Συστημάτων

5.1 ΣΚΟΠΟΣ

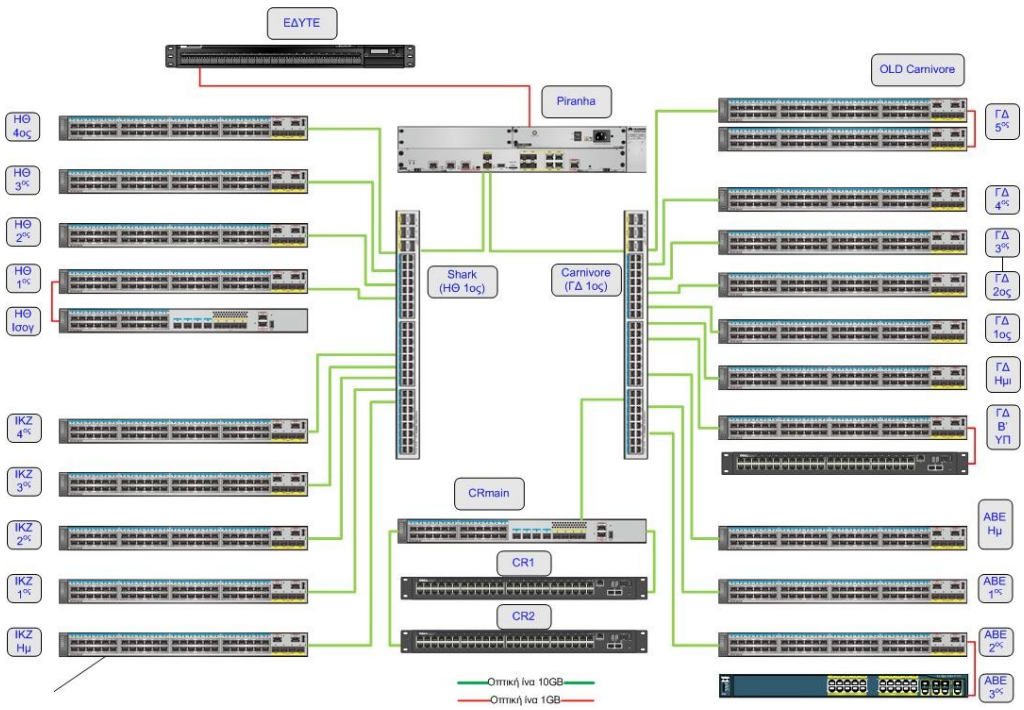
Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι η περιγραφή των τεχνικών που ακολουθούνται για την ασφάλεια του Δικτύου και των Συστημάτων του οργανισμού.

5.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε όλα σε όλα τα συστήματα και τα δίκτυα που χρησιμοποιούνται κατά τις λειτουργίες του οργανισμού.

Η τοπολογία του δικτύου και των συστημάτων απεικονίζεται παρακάτω:

ΑΠΛΟΥΣΤΕΥΜΕΝΟ ΔΙΑΓΡΑΜΜΑ ΔΙΚΤΥΟΥ



5.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

5.4 ΠΕΡΙΓΡΑΦΗ

5.4.1 Ασφάλεια Περιμέτρου

Σκοπός της πολιτικής ασφάλειας περιμέτρου είναι να διατηρήσει ένα ικανοποιητικό επίπεδο ασφάλειας, ιδιαίτερα όσον αφορά την πρόσβαση από και προς το Internet. Η πολιτική ασφάλειας περιμέτρου ορίζει τους μηχανισμούς (σε υλικό και λογισμικό) που χρησιμοποιούνται για το σκοπό αυτό καθώς και τους τρόπους διαμόρφωσης και ανανέωσης αυτών. Τέτοιοι μηχανισμοί είναι τα συστήματα Firewall και η κατάτμηση του δικτύου σε χωριστά λογικά δίκτυα, στα οποία επιτρέπεται η διακίνηση ορισμένου είδους πληροφορίας και μόνο.

Η διαθεσιμότητα και η προστασία του πληροφοριακού συστήματος του Πανεπιστημίου εξασφαλίζεται σε δύο επίπεδα:

Α. Σε επίπεδο λογισμικού εφαρμογών με τη χρήση του ενσωματωμένου firewall των Windows

Β. Σε επίπεδο συσκευών με τη χρήση του firewall on demand, υπηρεσία του GRNET που παρέχεται χωρίς χρέωση στους συμβεβλημένους φορείς, όπως το Πανεπιστήμιο Μακεδονίας.

Πρόσβαση στο διαδίκτυο έχουν όλες οι φορητές συσκευές. Η πρόσβαση σε αυτές γίνεται με χρήση του πρωτοκόλλου NAT (Network Address Translation) ώστε όλα τα πακέτα δεδομένων να εξέρχονται με την public IP address αυτού και να μη γίνονται γνωστές οι διευθύνσεις των υπολογιστών.

Η διαμόρφωση και ανανέωση των firewalls ακολουθεί τις διεθνώς αποδεκτές πρακτικές, όπως οι παρακάτω:

1. Η διαμόρφωση των firewall δεν επιτρέπει την εισερχόμενη κίνηση σε κανένα πακέτο και σύνδεση εκτός εάν ο τύπος της κίνησης και της σύνδεσης έχει ρητώς επιτραπεί.
2. Οι κανόνες του firewall καθορίζονται από την πολιτική ασφάλειας δικτύου.
3. Η πρόσβαση στο εσωτερικό δίκτυο του Πανεπιστημίου διαχωρίζεται σε τομείς που ο καθένας έχει διαφορετική πολιτική ασφαλείας. Ο πρώτος τομέας έχει ελεύθερη πρόσβαση με κρυπτογράφηση (ιστοσελίδα του Πανεπιστημίου). Ο δεύτερος τομέας απαιτεί η είσοδος από το διαδίκτυο προς το εσωτερικό δίκτυο μόνο εκείνων των δικτυακών συνόδων (session) οι οποίες έχουν σταθερή IP διεύθυνση και σχετική συμφωνία με τον αιτούντα της επικοινωνίας από το εξωτερικό. Ο τρίτος τομέας δεν επιτρέπει καμία πρόσβαση από το εξωτερικό στο εσωτερικό δίκτυο (πχ φοιτητολόγιο).

4. Ο IT τηρεί γραπτή τεκμηρίωση της διαμόρφωσης και λειτουργίας των firewalls, διάγραμμα του δικτύου και των διευθύνσεων IP, καθώς και των υπηρεσιών και των τύπων κίνησης που εξουσιοδοτούνται να διατρέξουν τα firewalls. Επίσης τηρεί στοιχεία που αφορούν τις υπηρεσίες και τους σταθμούς εργασίας, οι οποίοι εξουσιοδοτούνται να επικοινωνούν για λόγους παραμετροποίησης με την συσκευή Firewall.

5.4.2 Πολιτική ασφάλειας συστημάτων

Όλες οι προμήθειες συστημάτων βασίζονται σε προδιαγραφές, οι οποίες λαμβάνουν υπόψη και τα ζητήματα ασφάλειας. Οι προδιαγραφές ασφάλειας ελέγχονται από τον IT.

Όλα τα συστήματα ελέγχονται και τίθενται σε δοκιμαστική λειτουργία πριν τεθούν σε παραγωγική λειτουργία.

5.4.3 Παρακολούθηση (Monitoring) και Έλεγχος

Όλα τα γεγονότα που σχετίζονται με την ασφάλεια ευαίσθητων συστημάτων πρέπει να καταγράφονται και να ελέγχονται σύμφωνα με τα παρακάτω.

- Όλα τα security logs θα πρέπει να παραμένουν διαθέσιμα στο δίκτυο για τουλάχιστον ένα εξάμηνο.
- Προγραμματισμένα (προσθετικά) backups θα πρέπει να λαμβάνονται για τουλάχιστον ένα μήνα.
- Τα backups του κάθε μήνα θα πρέπει να διατηρούνται έως ένα έτος.
- Γεγονότα που σχετίζονται με την ασφάλεια των συστημάτων θα πρέπει να αναφέρονται στους υπεύθυνους κι έπειτα να εξετάζονται. Στην συνέχεια θα πρέπει να οριστούν διορθωτικά μέτρα.

Μερικά χαρακτηριστικά γεγονότα που σχετίζονται με την ασφάλεια είναι:

- ❖ Στοιχεία μη εγκεκριμένης πρόσβασης σε διαχειριστικούς λογαριασμούς
- ❖ Ασυνήθιστα περιστατικά που δεν προέρχονται από τη συνήθη χρήση κάποιας συγκεκριμένης εφαρμογής του συστήματος.

Σε τακτά χρονικά διαστήματα θα πρέπει να διενεργούνται έλεγχοι στα μηχανήματα του Πανεπιστημίου. Τα αποτελέσματα θα πρέπει να μελετώνται και στη συνέχεια να παρέχονται λύσεις. Κάθε δυνατή προσπάθεια πρέπει να καταβάλλεται ώστε κατά την διάρκεια των ελέγχων να μην εμποδίζεται η ομαλή λειτουργία του οργανισμού

5.4.4 Επιτρεπόμενη και μη χρήση των συστημάτων

Η παρακάτω λίστα δεν είναι εξαντλητική αλλά παρέχει ένα πλαίσιο ενεργειών που θεωρούνται μη αποδεκτές. Δεν επιτρέπεται:

- Να χρησιμοποιείτε τα συστήματα του Πανεπιστημίου για παράνομες δραστηριότητες.
- Να χρησιμοποιείτε συσκευές ή λογισμικό που δεν έχει εγκριθεί.
- Να χρησιμοποιείτε συστήματα που δεν ανήκουν στο Πανεπιστήμιο για την εκτέλεση εργασιών του Πανεπιστημίου.
- Να χρησιμοποιείτε συστήματα του Πανεπιστήμιο για προσωπικές εργασίες.
- Να αποκαλύπτετε οποιαδήποτε δεδομένα αφορούν το Πανεπιστήμιο σε τρίτους.
- Να παραβιάζονται κανόνες των πνευματικών δικαιωμάτων κάθε ιδιώτη ή εταιρίας τα οποία προστατεύονται από copyright, εμπορικό απόρρητο, πατέντες, νόμους και κανονισμούς.
- Η μη εξουσιοδοτημένη αντιγραφή προστατευόμενου από copyright υλικού όπως φωτογραφίες, βιβλία, προγράμματα-κώδικες, λογισμικό, τεχνικές πληροφορίες.
- Να χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο για την αποστολή εμπιστευτικών πληροφοριών σε παραλήπτες εκτός του Πανεπιστημίου, πλην φορέων της δημόσιας διοίκησης που σχετίζονται με τις δραστηριότητες του Πανεπιστημίου.
- Η αποστολή οποιουδήποτε άλλου e-mail εκτός αυτών που είναι απαραίτητα για την διεκπεραίωση των καθηκόντων του εργαζόμενου.
- Η αποστολή fake-mails, η προώθηση οποιουδήποτε e-mail τύπου “chain letter” κλπ
- Να επισκέπτεστε Ιστότοπους (Web Sites) με παράνομο λογισμικό, μη πρέπον υλικό ή άλλο πειρατικό οπτικοακουστικό υλικό.
- Η αποκάλυψη των κωδικών πρόσβασης σε τρίτους ή χρήση του προσωπικού λογαριασμού από άλλους.
- Η παράκαμψη της ταυτοποίησης του χρήστη ή οποιασδήποτε διαδικασίας ασφάλειας για κάθε υπολογιστή ή λογαριασμό.
- Η εισαγωγή κακόβουλων προγραμμάτων στο δίκτυο και τους υπολογιστές του οργανισμού (πχ ιοί ή άλλα βλαβερά προγράμματα – malware)
- Η διαφήμιση απατηλών προσφορών μέσω του Internet, χρησιμοποιώντας την υποδομή του οργανισμού

- Η άσκηση εμπορικών δραστηριοτήτων μέσω του δικτύου δεδομένων του Πανεπιστημίου όπως η πώληση αγαθών ή υπηρεσιών, η υπεκμίσθωση χωρητικότητας.

5.4.5 Ενημέρωση λογισμικού

Ο IT αξιολογεί κάθε νέα έκδοση του λογισμικού των συστημάτων που αφορούν τις υπηρεσίες και αποφασίζει εάν είναι αναγκαία η ανανέωσή του. Όλες οι προτεινόμενες από τον κατασκευαστή τροποποιήσεις (patches), αναγκαίες για την ασφάλεια του συστήματος υλοποιούνται το συντομότερο δυνατό.

5.5 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Σε περίπτωση διαπίστωσης παραβίασης κάποιας από τις υποχρεώσεις των χρηστών, ο οργανισμός έχει δικαίωμα, όταν κρίνεται απαραίτητο, ακόμη και χωρίς προειδοποίηση λόγω διαχειριστικών αναγκών, να αναστείλει τη σύνδεση του χρήστη στο δίκτυο δεδομένων ή τη πρόσβαση του σε συγκεκριμένες υπηρεσίες και να προβεί σε ενέργειες για την άρση του απορρήτου.

5.6 Σχετικά έντυπα

- Ουδέν

6. ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Τοπολογία Δικτύου	Ηλεκτρονική	Επ’ αόριστον	IT
Λίστα Κανόνων Firewall	Ηλεκτρονική	Επ’ αόριστον	IT

6 Πολιτική Αντιγράφων Ασφαλείας

6.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας πολιτικής είναι η περιγραφή των απαραίτητων ενεργειών για τη λήψη, τον έλεγχο και την ανάκτηση αντιγράφων ασφαλείας κάθε τύπου δεδομένων που χρήζουν δημιουργίας αντιγράφων ασφαλείας του οργανισμού.

6.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα πολιτική εφαρμόζεται μόνο στα κεντρικά συστήματα του Πανεπιστημίου (κεντρικοί εξυπηρετητές και δικτυακές συσκευές). Δεν εφαρμόζεται πολιτική αντιγράφων ασφαλείας για τους σταθμούς εργασίας των υπαλλήλων.

6.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

6.4 Δημιουργία Αντιγράφων Ασφαλείας Συστημάτων

Με σκοπό την εξασφάλιση των δεδομένων σε μορφή backup υπάρχουν δύο σημεία που διατηρούνται αντίγραφα ασφαλείας, εντός και εκτός των εγκαταστάσεων του Πανεπιστημίου.

Στο Πανεπιστήμιο λειτουργεί υποδομή διατήρησης αντιγράφων ασφαλείας συνολικής χωρητικότητας 86TB και ειδικού λογισμικού για τη συλλογή αυτών, που λειτουργεί ανεξάρτητα.

Με αυτό τον τρόπο δημιουργείται ένα full image backup όλων των διακομιστών του Πανεπιστημίου. Στο προσεχές διάστημα και προς μεγαλύτερη εξασφάλιση της διατήρησης των αντιγράφων ασφαλείας θα δημιουργηθεί και εξωτερική υποδομή διατήρησης αντιγράφων ασφαλείας εκτός των κτιριακών εγκαταστάσεων του Πανεπιστημίου στη Θεσσαλονίκη, επί της Εγνατίας 156.

6.5 Παρακολούθηση αντιγράφων ασφαλείας

Εάν δεν έχει ολοκληρωθεί επιτυχώς η δημιουργία αντιγράφων ασφαλείας, η διαδικασία που ακολουθείται είναι η παρακάτω:

- Πραγματοποιείται έλεγχος του σφάλματος που εμφανίζεται.

- Πραγματοποιείται έλεγχος στο αρχείο καταγραφής των υπολογιστών.
- Γίνεται επιδιόρθωση του προβλήματος που επηρέασε την διαδικασία αντιγράφων ασφαλείας.

6.6 Ανάκτηση αντιγράφων ασφαλείας

Στην περίπτωση που απαιτείται η ανάκτηση αντιγράφων ασφαλείας για υπηρεσίες εσωτερικής χρήσης, η διαδικασία που ακολουθείται είναι η κάτωθι:

- Έλεγχος των αντιγράφων ασφαλείας για δυνατότητα επαναφοράς τους σε τριμηνιαία βάση.
- Ανάκτηση της υπηρεσίας ή του συστήματος σε δοκιμαστικό περιβάλλον με χρήση του λογισμικού ACRONIS.
- Έλεγχος ορθής λειτουργίας της υπηρεσίας ή του συστήματος σε εβδομαδιαία βάση.
- Ανάκτηση της υπηρεσίας ή του συστήματος στο περιβάλλον παραγωγής, όταν προκύψει η ανάγκη.

6.7 Έλεγχος αντιγράφων ασφαλείας

Για τον έλεγχο ορθής αντιγραφής υπηρεσιών και συστημάτων πραγματοποιείται ετήσιος έλεγχος. Η διαδικασία που ακολουθείται είναι η παρακάτω:

- Ανάκτηση τυχαίων υπηρεσιών και συστημάτων σε δοκιμαστικό περιβάλλον.
- Έλεγχος ορθής λειτουργίας υπηρεσιών και συστημάτων.
- Καταγραφή υπηρεσιών και συστημάτων που ελέγχθηκαν.

6.8 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Αντίγραφο Ασφαλείας	Ηλεκτρονική	Έως 1 έτος, ανάλογα με την περίπτωση (Εξαιρούνται τα e-mail της GOOGLE)	Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

7 Πολιτική Καθαρού Γραφείου και Καθαρής Οθόνης

7.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφούν οι διαδικαστικές λεπτομέρειες για την τήρηση των απαιτήσεων «καθαρού γραφείου και καθαρής οθόνης» τις οποίες έχει θέσει το Πανεπιστήμιο, ώστε να επιτυγχάνεται η ελαχιστοποίηση των κινδύνων για την ασφάλεια των δεδομένων.

7.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται από όλο το προσωπικό το οποίο απασχολείται με εργασίες γραφείου και / ή χειρίζεται Η/Υ.

7.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- ΥΠΔ
- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- Προσωπικό Πανεπιστημίου (διοικητικό-εκπαιδευτικό)

7.4 ΠΕΡΙΓΡΑΦΗ

Οι υπάλληλοι όλων των τμημάτων, που εκτελούν εργασίες γραφείου και / ή χειρίζονται Η/Υ θα πρέπει με δική τους ευθύνη:

- ✓ Να μην αφήνουν στον χώρο εργασίας τους εμπιστευτικά και απόρρητα έγγραφα πριν αποχωρήσουν από το γραφείο τους για σχετικά μεγάλο χρονικό διάστημα μέσα στην ημέρα. Στην περίπτωση αυτή θα πρέπει να κλειδώνεται η πόρτα του γραφείου.
- ✓ Να μην αφήνουν στον χώρο εργασίας τους εμπιστευτικά και απόρρητα έγγραφα πριν αποχωρήσουν στο τέλος της ημέρας αλλά να τα τοποθετούν μέσα σε ειδικούς αποθηκευτικούς χώρους και να τα κλειδώνουν.
- ✓ Να χρησιμοποιούν τους ειδικούς καταστροφείς εγγράφων για εμπιστευτικά και απόρρητα έγγραφα τα οποία δεν χρειάζονται πλέον.
- ✓ Να γίνεται χρήση του συνδυασμού πλήκτρου WIN+L για το άμεσο κλείδωμα του Η/Υ (σε συστήματα windows).

- ✓ Να διασφαλίζουν ότι σε περίπτωση απουσίας τους από τη θέση εργασίας τους για πάνω από 15 λεπτά, ο Η/Υ που χρησιμοποιούν κλειδώνει και η επανενεργοποίησή του απαιτεί χρήση κωδικού, ο οποίος τηρείται μυστικός.

8 Πολιτική Ασφαλείας Κρυπτογραφικών Ελέγχων

8.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να αναφέρει τους κρυπτογραφικούς αλγόριθμους που χρησιμοποιούνται στα πληροφοριακά συστήματα του οργανισμού και τις θέσεις φύλαξης κλειδιών και κωδικών.

8.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται στους διακομιστές του Πανεπιστημίου, στα αφαιρούμενα μέσα και στα έγγραφα που περιέχουν προσωπικά δεδομένα και βρίσκονται σε αφαιρούμενα μέσα.

8.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

8.4 ΠΕΡΙΓΡΑΦΗ

8.4.1. Πολιτική Χρήσης Κρυπτογραφικών Αλγόριθμων

8.4.1.1. Σε όλες τις εφαρμογές παγκόσμιου ιστού (Web based applications) οι οποίες φιλοξενούνται στους διακομιστές του οργανισμού ή σε συνεργάτη, γίνεται χρήση του πρωτοκόλλου Secure Sockets Layer (SSL) και πρωτίστως κατά την πιστοποίηση του εκάστοτε χρήστη που επιθυμεί πρόσβαση σε κάποια από τις παρεχόμενες υπηρεσίες.

8.4.1.2. Ειδικότερα, και για περιπτώσεις όπου λαμβάνει χώρα τραπεζική συναλλαγή, όπως απευθείας πληρωμή μέσω πιστωτικής κάρτας, η δικτυακή σύνοδος του χρήστη ανακατευθύνεται σε άλλη διαδικτυακή τοποθεσία, εξολοκλήρου ασφαλή σε συνεργασία με την εκάστοτε τράπεζα ή χρηματοπιστωτικό ίδρυμα.

8.4.1.3. Όλα τα ψηφιακά αφαιρούμενα μέσα που πρόκειται να μεταφερθούν εκτός των εγκαταστάσεων του Πανεπιστημίου, πρέπει να είναι κρυπτογραφημένα. Το άτομο που προετοίμασε το αφαιρούμενο μέσο, φέρει την ευθύνη κρυπτογράφησής του και το άτομο που θα εκτελέσει τη μεταφορά φέρει την ευθύνη επιβεβαίωσης της εφαρμογής κρυπτογράφησης.

8.4.2. Πολιτική Διατήρησης Κωδικών Πρόσβασης

8.4.2.1. Με σκοπό την ασφαλή φύλαξη των κωδικών ασφαλείας η αυστηρή σύσταση είναι να απομνημονεύεται. Αν αυτό δεν είναι εφικτό συνίσταται η αποθήκευσή τους είτε σε χώρο που κλειδώνει, είτε με τη χρήση ειδικού λογισμικού με τη χρήση κωδικών ασφάλειας.

8.4.2.2. Όλοι οι διαχειριστές που κάνουν χρήση κλειδιού ή κωδικού θα παραδίδουν το κλειδί ή κωδικό τους, μέσα σε δύο σφραγισμένους φακέλους οι οποίοι θα αποθηκεύονται στις ορισμένες θέσεις. Η μόνη ένδειξη στο εξωτερικό του φακέλου θα είναι μόνο το ονοματεπώνυμο του χρήστη.

8.5 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

Ουδέν

8.6 ΑΡΧΕΙΑ

Ουδέν

9 Πολιτική Ορθής Χρήσης Σταθμών Εργασίας

9.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής είναι να θέσει το πλαίσιο και τους κανονισμούς βάσει των οποίων γίνεται χρήση των Σταθμών Εργασίας από τα στελέχη και τους υπαλλήλους του οργανισμού καθώς και η πρόσβαση αυτών στο Διαδίκτυο.

9.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται από όλους τους χρήστες του δικτύου πληροφορικής του Πανεπιστημίου.

9.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Προσωπικό του Πανεπιστημίου (διοικητικό και εκπαιδευτικό)

9.4 ΠΕΡΙΓΡΑΦΗ

9.4.1 *Αποδεκτή Χρήση Σταθμών Εργασίας και Πρόσβασης στο Διαδίκτυο*

Σκοπός της παρούσας Πολιτικής είναι να θέσει το πλαίσιο και τους κανονισμούς βάσει των οποίων γίνεται χρήση των Σταθμών Εργασίας από τους υπαλλήλους του Πανεπιστημίου (διοικητικό και διδακτικό προσωπικό) καθώς και η πρόσβαση αυτών στο Διαδίκτυο.

9.4.2 Πεδίο Εφαρμογής

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε όλους τους χρήστες του Πανεπιστημίου.

9.4.3 Υπεύθυνος Εφαρμογής της Πολιτικής

- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

9.4.4 *Αποδεκτή Χρήση Σταθμών Εργασίας και Πρόσβασης στο Διαδίκτυο από το διοικητικό προσωπικό*

1. Όλοι οι χρήστες του Πανεπιστημίου, εκτός από τον IT, δεν μπορούν να εκτελέσουν κάποιο άλλο εκτελέσιμο αρχείο εκτός από αυτά που είναι ήδη εγκατεστημένα στον υπολογιστή τους.
2. Όλοι οι σταθμοί εργασίας κλειδώνουν όταν είναι ανενεργός ο χρήστης για περισσότερο από 15’ ή έχει παρέλθει το ωράριο εργασίας. Στην πρώτη περίπτωση για να ξεκλειδώσουν χρειάζεται να εισαχθεί το *Username* και *Password* από τον χρήστη, ενώ στη δεύτερη θα πρέπει να έχει προηγηθεί συνεννόηση με το IT για την επέκταση του ωραρίου εργασίας.
3. Κάθε σταθμός εργασίας έχει εγκατεστημένο Antivirus software για προστασία από ιούς, trojans κλπ.

9.4.5 Μη αποδεκτή χρήση συστημάτων

Η παρακάτω λίστα δεν είναι εξαντλητική αλλά παρέχει ένα πλαίσιο ενεργειών που θεωρούνται μη αποδεκτές. Δεν επιτρέπεται:

- Να χρησιμοποιείτε τα συστήματα του οργανισμού για παράνομες δραστηριότητες.
- Να χρησιμοποιείτε συσκευές ή λογισμικό που δεν έχει εγκριθεί.
- Να χρησιμοποιείτε συστήματα που δεν ανήκουν στο Πανεπιστήμιο για την εκτέλεση εργασιών του Πανεπιστημίου.

- Να χρησιμοποιείτε συστήματα του Πανεπιστημίου για προσωπικές εργασίες.
- Να αποκαλύπτετε οποιαδήποτε δεδομένα αφορούν το Πανεπιστήμιο σε τρίτους.
- Να παραβιάζονται κανόνες των πνευματικών δικαιωμάτων κάθε ιδιώτη ή εταιρίας τα οποία προστατεύονται από copyright, εμπορικό απόρρητο, πατέντες, νόμους και κανονισμούς.
- Η μη εξουσιοδοτημένη αντιγραφή προστατευόμενου από copyright υλικού όπως φωτογραφίες, βιβλία, προγράμματα-κώδικες, λογισμικό, τεχνικές πληροφορίες.
- Να χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο για την αποστολή εμπιστευτικών πληροφοριών σε παραλήπτες εκτός του Πανεπιστημίου.
- Η αποστολή οποιουδήποτε άλλου e-mail εκτός αυτών που είναι απαραίτητα για την διεκπεραίωση των καθηκόντων του εργαζόμενου, είτε πρόκειται για διοικητικό είτε για διδακτικό προσωπικό.
- Η αποστολή fake-mails, η προώθηση οποιουδήποτε e-mail τύπου “chain letter” κλπ
- Να επισκέπτεστε Ιστότοπους (Web Sites) με παράνομο λογισμικό, μη πρέπον υλικό ή άλλο πειρατικό οπτικοακουστικό υλικό.
- Η αποκάλυψη των κωδικών πρόσβασης σε τρίτους ή χρήση του προσωπικού λογαριασμού από άλλους.
- Η παράκαμψη της ταυτοποίησης του χρήστη ή οποιασδήποτε διαδικασίας ασφάλειας για κάθε υπολογιστή ή λογαριασμό.
- Η εισαγωγή κακόβουλων προγραμμάτων στο δίκτυο και τους υπολογιστές του οργανισμού (πχ ιοί ή άλλα βλαβερά προγράμματα – malware).
- Ενέργειες όπως το port-scanning, network monitoring απαγορεύονται αυστηρά, εκτός και αν περιλαμβάνονται στα καθήκοντα του εργαζόμενου και έχει προηγουμένως ειδοποιηθεί η ομάδα IT η άδεια της οποίας απαιτείται.
- Οποιαδήποτε κακόβουλη ενέργεια προς υπολογιστές άλλους από αυτούς του χρήστη, όπως άρνησης παροχής υπηρεσιών (DoS attacks), terminating user sessions.
- Η διαφήμιση απατηλών προσφορών μέσω του Internet, χρησιμοποιώντας την υποδομή του οργανισμού.
- Η άσκηση εμπορικών δραστηριοτήτων μέσω του δικτύου δεδομένων του οργανισμού όπως η πώληση αγαθών ή υπηρεσιών, η υπεκμίσθωση χωρητικότητας.

9.4.6 Πρόσβαση Διαδικτυακών Τόπων

Σύμφωνα με την παρούσα Πολιτική Ασφάλειας, στους χρήστες του Πανεπιστημίου επιτρέπεται η πρόσβαση στο διαδίκτυο χωρίς περιορισμούς.

9.5 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

Ουδέν

9.6 ΑΡΧΕΙΑ

Ουδέν

10 Πολιτική Ασφαλούς Διαβίβασης Πληροφοριών

10.1 Γενικά

Υπάρχουν πολλές περιπτώσεις κατά τις οποίες διαβιβάζονται πληροφορίες εξωτερικά, σε εταιρείες και σε ιδιώτες. Αυτό γίνεται χρησιμοποιώντας μια ευρεία ποικιλία μέσων και μεθόδων. Η διαβίβαση μπορεί να γίνεται με ηλεκτρονικά μέσα ή και σε μορφή εγγράφου μέσω ταχυδρομικής αποστολής.

Σε κάθε διαβίβαση υπάρχει ο κίνδυνος απώλειας, υποκλοπής ή τυχαίας δημοσίευσης των πληροφοριών σε μη εξουσιοδοτημένα γι' αυτό άτομα.

Το Πανεπιστήμιο έχει την υποχρέωση να φροντίζει για τη διαχείριση των πληροφοριών αυτών, για νομικούς λόγους, σύμφωνα και με το πνεύμα του Γενικού Κανονισμού αλλά και για τη διατήρηση της εμπιστοσύνης των συναλλασσομένων μαζί της, όπως επίσης είναι απαραίτητο η μεταφορά να πραγματοποιείται κατά τρόπο που να προστατεύει επαρκώς τις πληροφορίες.

Ο ρόλος του Πανεπιστημίου σαν αποστολέας είναι να αξιολογήσει τους κινδύνους και να διασφαλίσει την ύπαρξη κατάλληλων μέτρων προστασίας. Αυτή η πολιτική περιγράφει τις ευθύνες και τις ελάχιστες απαιτήσεις ασφάλειας για την ασφαλή μεταφορά των πληροφοριών αυτών.

10.2 Σκοπός

Αυτή η πολιτική ορίζει τις ελάχιστες απαιτήσεις ασφαλείας για τη φυσική μεταφορά πληροφοριών από και προς τον οργανισμό, σε οποιαδήποτε μορφή.

Για τους σκοπούς του παρόντος εγγράφου, οι πληροφορίες αφορούν και τις πληροφορίες κειμένου (π.χ. έγγραφα, αναφορές και υπολογιστικά φύλλα) και τα ακατέργαστα μη μορφοποιημένα δεδομένα (π.χ. εξωτερικοί δίσκοι backup), σε οποιαδήποτε μορφή και σε οποιοδήποτε μέσο, ηλεκτρονικό ή μη.

Αυτή η πολιτική ισχύει για όλο το προσωπικό του Πανεπιστημίου (διοικητικό και διδακτικό), όπως και για κάθε τρίτο που επεξεργάζεται πληροφορίες του.

10.3 Εξαιρέσεις

Αυτή η πολιτική δεν καλύπτει τη διαβίβαση πληροφοριών μέσω του εσωτερικού δικτύου του Πανεπιστημίου, το οποίο έχει τους δικούς του ελέγχους ασφαλείας. Επίσης δεν καλύπτει τυχόν χρηματικές συναλλαγές που έχουν τις δικές τους ξεχωριστές απαιτήσεις ασφάλειας, ή συναλλαγές που υλοποιούνται σαν μέρος σύμβασης των οποίων οι όροι ασφάλειας καθορίζονται από τρίτο μέρος.

10.4 Ορισμοί

ΠΑΡΑΛΗΠΤΗΣ: Κάθε φυσικό ή νομικό πρόσωπο το οποίο ζητά πληροφορίες από κάποια διεύθυνση του Πανεπιστημίου. Μπορεί να είναι εξωτερικός συνεργάτης, κάποια εταιρεία ή κάποια άλλη διεύθυνση εντός του Πανεπιστημίου.

ΑΠΟΣΤΟΛΕΑΣ: Είναι το φυσικό πρόσωπο το οποίο για λογαριασμό του Πανεπιστημίου, ξεκινά την αποστολή της πληροφορίας. Θα πρέπει να έχει ήδη την εξουσιοδότηση της διεύθυνσης και την απαραίτητη γνώση ως προς το να διακρίνει την κατηγοριοποίηση της πληροφορίας και αν μπορεί αυτή να μεταδοθεί με τον επιλεγμένο τρόπο. Προσοχή πρέπει να δίνεται στην περίπτωση αναμετάδοσης μιας πληροφορίας από άτομο που δεν έχει την εξουσιοδότηση ή τη γνώση να διακρίνει την κρισιμότητά της. Όταν ο υπάλληλος δεν μπορεί να αποφασίσει για την πληροφορία θα πρέπει πάντα να συμβουλεύεται τον προϊστάμενό του, τον υπεύθυνο προστασίας δεομένων ή τον πρώτο αποστολέα της πληροφορίας.

10.5 Ρόλοι και Αρμοδιότητες

Οι κατάλληλοι ορισμοί των ρόλων και των ευθυνών είναι ουσιώδεις για τη διασφάλιση της συμμόρφωσης με την παρούσα πολιτική.

10.5.1 Αποστολέας

Ο αποστολέας είναι υπεύθυνος για την τήρηση των ακόλουθων απαιτήσεων της παρούσας πολιτικής:

- Για την αξιολόγηση των πληροφοριών που πρέπει να αποσταλούν.
- Για την εξασφάλιση της επίσημης επιβεβαίωσης της ταυτότητας και της εξουσιοδότησης λήψης του παραλήπτη
- Για τη λήψη της συγκατάθεσης του ιδιοκτήτη δεδομένων για τη μεταφορά.
- Για να εξασφαλίσει ότι οι πληροφορίες αποστέλλονται με τον πιο κατάλληλο τρόπο.

10.5.2 Υπεύθυνος Ασφάλειας

Ο Υπεύθυνος ασφαλείας θα πρέπει να παρακολουθεί και να ελέγχει τα τμήματα του οργανισμού για να εξασφαλίσει τη συμμόρφωσή τους με όλες τις υποχρεωτικές και νομικές/κανονιστικές απαιτήσεις και τις εσωτερικές πολιτικές ασφαλείας.

10.5.3 Υπάλληλοι

Οι υπάλληλοι είναι υπεύθυνοι ώστε να εξοικειωθούν με την παρούσα πολιτική και να εξασφαλίσουν ότι οποιαδήποτε μεταφορά πληροφοριών για την οποία είναι αυτοί υπεύθυνοι γίνεται κατά τρόπο συμβατό με την παρούσα πολιτική.

Οι υπάλληλοι πρέπει να αναφέρουν τυχόν ύποπτες ή πραγματικές παραβιάσεις ασφαλείας που σχετίζονται με τη μεταφορά δεδομένων άμεσα, στον Υπεύθυνο Ασφαλείας ή στον προϊστάμενό τους, σύμφωνα με τις διαδικασίες αντιμετώπισης συμβάντων ασφαλείας του οργανισμού.

10.6 Αρμοδιότητες Αποστολέα

Σε κάθε μεταφορά υπάρχει ο κίνδυνος απώλειας, υποκλοπής ή τυχαίας δημοσίευσης των πληροφοριών σε μη εξουσιοδοτημένο άτομο. Είναι ευθύνη του αποστολέα να αξιολογήσει όλους τους κινδύνους και να εξασφαλίσει ότι είναι επαρκής οι έλεγχοι ασφάλειας και ότι συμμορφώνονται με την παρούσα πολιτική. Αυτή η ενότητα περιέχει ορισμένα από τα απαιτούμενα που πρέπει να ισχύουν πριν από τη μεταφορά των πληροφοριών.

10.7 Νομιμότητα και Αναγκαιότητα Διαβίβασης

Είναι επισφαλές να υποθέσουμε ότι επειδή κάποιος ζητά πληροφορίες είναι απαραίτητα και εξουσιοδοτημένος ή νομίμως δικαιούται να τις έχει. Αν υπάρχουν αμφιβολίες για τον

παραλήπτη τότε πρέπει να ενημερώνεται άμεσα η διοίκηση ή ο υπεύθυνος ασφάλειας πληροφοριών.

Μόλις επιβεβαιωθεί ότι η διαβίβαση είναι νόμιμη και απαραίτητη, τότε πρέπει να αποφασιστεί τι επιπέδου διαβάθμισης είναι η πληροφορία που θα αποσταλεί. Αυτό θα καθορίσει ποιο επίπεδο ασφάλειας είναι το κατάλληλο για το συγκεκριμένο τρόπο μεταφοράς.

Η διαβίβαση προσωπικών ή εμπιστευτικών πληροφοριών χωρίς ελέγχους ασφαλείας μπορεί να αφήσει το Πανεπιστήμιο έκθετο σε νομικά θέματα και να βλάψει τη φήμη του.

10.8 Προσωπικά Δεδομένα

Τα προσωπικά δεδομένα αφορούν ένα άτομο, εν ζωή, ταυτοποιήσιμο, άμεσα ή έμμεσα. Στα προσωπικά δεδομένα περιέχονται συχνά πληροφορίες σχετικές με τη φυλετική ή εθνοτική καταγωγή, τις πολιτικές απόψεις, τις θρησκευτικές πεποιθήσεις, την συνδικαλιστική συμμετοχή, δεδομένα σωματικής ή ψυχικής υγείας, τις σεξουαλικές προτιμήσεις, ή η τη διάπραξη αδικημάτων, οι οποίες χαρακτηρίζονται περαιτέρω ως ευαίσθητα προσωπικά δεδομένα (ειδικές κατηγορίες δεδομένων) και χρήζουν αυξημένης προστασίας.

Πριν την εκτέλεση οποιασδήποτε διαβίβασης δεδομένων θα πρέπει:

- Να υπάρχει τεκμηριωμένη η έγκριση του υπεύθυνου επεξεργασίας για τη συγκεκριμένη μεταφορά.
- Να επιβεβαιωθεί ότι η διαβίβαση είναι σύμφωνη με τις νομικές και κανονιστικές απαιτήσεις και ιδιαίτερα σύμφωνη με τον ΓΚΠΔ.
- Να επιβεβαιωθεί ότι η διαβίβαση είναι απαραίτητη.
- Να υπάρχει προηγούμενη σύμβαση με τον παραλήπτη, στην οποία θα πρέπει να αποτυπώνεται ότι κατανοεί τις ευθύνες του από τη στιγμή που θα λάβει στα συστήματά του πληροφορία που αφορά προσωπικά δεδομένα.

10.9 Εμπιστευτικά Δεδομένα

Οι εμπιστευτικές πληροφορίες είναι εκείνες τις οποίες το Πανεπιστήμιο είναι υπεύθυνο να τηρεί με διατυπώσεις αυξημένης ασφάλειας. Αυτές μπορεί να περιλαμβάνουν πληροφορίες που επηρεάζουν τα επιχειρηματικά συμφέροντα ενός τρίτου ή πληροφορίες για τις οποίες ο αποστολέας δεν κατέχει πνευματικά δικαιώματα π.χ. πληροφορίες μισθοδοσίας, συμβάσεις, συμφωνίες κλπ.

Τυχόν διαρροή τέτοιων πληροφοριών μπορεί να βλάψει τη φήμη του Πανεπιστημίου ή και να επιφέρει νομικές συνέπειες.

Πριν την εκτέλεση οποιασδήποτε διαβίβασης θα πρέπει:

- Να υπάρχει τεκμηριωμένη η έγκριση του υπεύθυνου επεξεργασίας για τη συγκεκριμένη διαβίβαση.
- Να επιβεβαιώσετε ότι δεν παραβιάζεται η ευθύνη τήρησης της πληροφορίας με ασφάλεια.
- Να επιβεβαιωθεί ότι η διαβίβαση είναι απαραίτητη.
- Να αφαιρείται οτιδήποτε δεν είναι απαραίτητο για το σκοπό του παραλήπτη.
- Να υπάρχει προηγούμενη σύμβαση με τον παραλήπτη, που να αποτυπώνεται ότι κατανοεί τις ευθύνες του από τη στιγμή που θα λάβει στα συστήματά του πληροφορία που αφορά προσωπικά δεδομένα.

10.10 Απαιτήσεις διαβίβασης προσωπικών δεδομένων

Αφού αποφασιστεί τι είδους πληροφορίες θα αποσταλούν και είναι έτοιμες για διαβίβαση, ο αποστολέας πρέπει να εξετάσει τις διάφορες διαθέσιμες μεθόδους διαβίβασης και κατά πόσον αυτές είναι κατάλληλες.

Αυτή η ενότητα περιλαμβάνει τις κύριες μεθόδους αποστολής και καθορίζει τους περιορισμούς και τις απαιτήσεις για ασφαλή μεταφορά δεδομένων προσωπικού χαρακτήρα.

Για όλες τις διαβιβάσεις προσωπικών δεδομένων, είναι απαραίτητο να έχει πιστοποιηθεί η ταυτότητα του παραλήπτη και να έχει πιστοποιηθεί κατάλληλα από τον αποστολέα.

10.11 Ηλεκτρονική Αλληλογραφία

Όπως αναφέρονται στην πολιτική ασφαλούς μετάδοσης μηνύματος ηλεκτρονικής αλληλογραφίας του οργανισμού (Π.11).

10.12 Δικτυακή Μεταφορά (FTP, SecureFTP , VPN)

Το τυπικό πρωτόκολλο μεταφοράς αρχείων (FTP) χωρίς κρυπτογράφηση είναι εγγενώς ανασφαλές και δεν πρέπει να χρησιμοποιείται για τη μετάδοση προσωπικών ή εμπιστευτικών δεδομένων.

Οι μεταφορές αρχείων μέσω ασφαλούς πρωτοκόλλου μεταφοράς αρχείων (SFTP) είναι αποδεκτές.

Για την περίπτωση της απομακρυσμένης σύνδεσης μέσω VPN, ακολουθείται η πολιτική τηλε-εργασίας (Π.02) του οργανισμού, ωστόσο η διασύνδεση με VPN δεν συνεπάγεται την πρόσβαση σε υπηρεσίες για τις οποίες πρέπει να προηγηθεί συνεννόηση με τον IT.

10.13 Αφαιρούμενο Μέσο (CD, USB δίσκος, Κάρτα Μνήμης κλπ.)

Όπως αναφέρονται στην πολιτική χρήσης συσκευών και φορητών μέσων του οργανισμού (Π.04).

10.14 Μετάδοση FAX

Το FAX είναι εγγενώς ανασφαλές και δεν συνιστάται για τη διαβίβαση διαβαθμισμένων πληροφοριών. Ωστόσο, αναγνωρίζεται ότι ορισμένες περιστάσεις το απαιτούν. Σε αυτές τις περιπτώσεις θα πρέπει να ακολουθούνται τα παρακάτω:

- Ο αποστολέας πρέπει να ελέγξει ότι ο αριθμός φαξ είναι σωστός και ότι ο παραλήπτης περιμένει τη μετάδοση.
- Για πληροφορίες αυξημένης ευαισθησίας, ο αριθμός πρέπει να ελέγχεται και από έναν άλλο συνάδελφο και εκτός της μετάδοσης να υπάρχει και τηλεφωνική επαφή με τον παραλήπτη καθ' όλη τη διάρκεια της αποστολής, για επιβεβαίωση της λήψης .
- Τόσο ο αποστολέας όσο και ο παραλήπτης θα πρέπει να έχουν μια συμφωνημένη διαδικασία για να αποφευχθεί η παραμονή του αντιγράφου στη μνήμη του μηχανήματος FAX και μια σαφή απαίτηση για την ασφαλή καταστροφή του μηνύματος όταν αυτό δεν απαιτείται πλέον.
- Το μήνυμα πρέπει να περιέχει σαφείς οδηγίες σχετικά με τις ευθύνες του παραλήπτη, αν αυτός δεν είναι τελικά ο σωστός παραλήπτης.
- Κάθε αποστολή θα πρέπει να επιβεβαιώνεται ότι λήφθηκε από τον σωστό παραλήπτη.

10.15 Ταχυδρομική ή με courier Αποστολή

Είναι σημαντικό ότι ο φάκελος, είτε περιέχει ψηφιακό μέσο είτε χαρτί, πρέπει να διατηρείται ασφαλής κατά τη μεταφορά του και να παραδοθεί στο φυσικό πρόσωπο στο οποίο απευθύνεται ή στον νόμιμο εκπρόσωπο του νομικού προσώπου στο οποίο απευθύνεται. Αυτό μπορεί να επιτευχθεί ακολουθώντας τις παρακάτω οδηγίες:

- Πρέπει να χρησιμοποιείται ένας αξιόπιστος μεταφορέας για την παράδοση.
- Ο φάκελος/το πακέτο θα πρέπει να συσκευάζεται με ασφάλεια, να φέρει σαφή ετικέτα και να φέρει σφραγίδα, η οποία θα πρέπει να σπάσει για να ανοίξει η συσκευασία.

- Ο φάκελος/το πακέτο πρέπει να έχει διεύθυνση επιστροφής και στοιχεία επικοινωνίας.
- Η ετικέτα δεν πρέπει να αναφέρει τη φύση ή την αξία των περιεχομένων.
- Ο φάκελος/το πακέτο πρέπει να παραδοθεί μόνο στον παραλήπτη και να υπογράψει ο ίδιος για την παραλαβή του.
- Ο αποστολέας πρέπει να ελέγξει άμεσα ότι η παράδοση ήταν επιτυχής.

10.16 Τηλεφωνική Μετάδοση

Καθώς οι τηλεφωνικές κλήσεις μπορεί να παρακολουθούνται, να ακούγονται (ανοικτή ακρόαση), να καταγράφονται ή να παρεμποδίζονται είτε σκόπιμα είτε τυχαία, πρέπει να ληφθούν μέτρα ασφάλειας, όπως παρακάτω:

- Οι πληροφορίες που διαβιβάζονται πρέπει να περιορίζονται στο ελάχιστο.
- Τα προσωπικά δεδομένα δεν πρέπει να διαβιβάζονται μέσω τηλεφώνου παρά μόνο όταν η ταυτότητα και η έγκριση του παραλήπτη έχει επιβεβαιωθεί.

10.17 SMS, Μηνύματα Κοινωνικών Δικτύων, Εφαρμογές Άμεσων Μηνυμάτων (Instant Messaging)

Δεν επιτρέπεται η διαβίβαση προσωπικών πληροφοριών με κανένα από τα παραπάνω μέσα, καθώς και τα ομοειδή αυτών.

10.18 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Το Πανεπιστήμιο αναγνωρίζει την ευθύνη του να επεξεργάζεται τις πληροφορίες σύννομα, σύμφωνα με όλες τις νομικές και κανονιστικές απαιτήσεις και τις απαιτήσεις των εσωτερικών πολιτικών ασφαλείας του.

Είναι ευθύνη του αποστολέα να αξιολογεί τον κίνδυνο αναλόγως της διαβίβασης που σκοπεύει να πραγματοποιήσει και να εξασφαλίσει ότι όλοι οι σχετιζόμενοι κίνδυνοι γίνονται αντιληπτοί και αντιμετωπίζονται επαρκώς και ότι η διαβίβαση είναι κατάλληλα εγκεκριμένη βάσει των πολιτικών του Πανεπιστημίου. Οι απαιτήσεις ασφάλειας για τις διάφορες μεθόδους αποστολής έχουν παρατεθεί στην παράγραφο 11.5 της παρούσας πολιτικής.

Ο Προϊστάμενος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής είναι αρμόδιος για την εφαρμογή αυτής της πολιτικής.

10.19 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

α) Πολιτική χρήσης φορητών μέσων (Π.04)

β) Πολιτική τήλε-εργασίας (Π.02)

10.20 ΑΡΧΕΙΑ

Ουδέν

11 Πολιτική Ασφαλούς Αποστολής e-mail

11.1 ΣΚΟΠΟΣ

Σκοπός των παρόντων κανόνων ασφάλειας είναι να καθοριστεί, ο ασφαλής τρόπος χρήσης της υπηρεσίας μηνυμάτων ηλεκτρονικού ταχυδρομείου.

11.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Οι παρόντες κανόνες ασφάλειας εφαρμόζονται σε κάθε περίπτωση επικοινωνίας του Πανεπιστημίου, τόσο εσωτερικά όσο και εξωτερικά, με αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου.

11.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Ο Προϊστάμενος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- Το προσωπικό του Πανεπιστημίου (διοικητικό και εκπαιδευτικό)

11.4 ΠΕΡΙΓΡΑΦΗ

11.4.1 Παραδοχές

12.4.1.1 Λαμβάνεται ως δεδομένο ότι η επικοινωνία με τους εξυπηρετητές e-mail γίνεται με τη χρήση ασφαλών πρωτοκόλλων SSL/TLS.

11.5 ΚΑΝΟΝΕΣ ΑΠΟΣΤΟΛΗΣ

12.5.2.1 Ο χρήστης είναι υπεύθυνος για την ορθή συμπλήρωση της σωστής διεύθυνσης του/των παραλήπτη/ών.

12.5.2.2 Απαγορεύεται να αναφέρονται στο πεδίο του τίτλου του μηνύματος ή/και στο σώμα του κειμένου του μηνύματος πληροφορίες που αφορούν σε δεδομένα της διεύθυνσης είτε σε προσωπικά δεδομένα.

12.5.2.3 Αν στο μήνυμα πρόκειται να αναφερθούν δεδομένα, αυτά θα πρέπει να εισάγονται πρώτα σε αρχείο (txt, xls, rtf, doc κλπ) και το αρχείο να μεταδίδεται σαν συνημμένο.

12.5.2.4 Τα δεδομένα που είναι χαρακτηρισμένα «εμπιστευτικά» ή «απόρρητα» δεν θα διαβιβάζονται αν το συνημμένο αρχείο δεν είναι προστατευμένο, τουλάχιστον με κωδικό πρόσβασης ή κρυπτογράφηση.

11.6 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Οποιοσδήποτε εργαζόμενος παραβιάσει την παρούσα Πολιτική Ασφάλειας μπορεί να υπόκειται σε πειθαρχικές κυρώσεις κατά την κρίση της Διοίκησης.

11.7 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

ΟΥΔΕΝ

11.8 ΑΡΧΕΙΑ

ΟΥΔΕΝ

12 Πολιτική Ασφάλειας B.Y.O.D. (Bring Your Own Device)

12.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφεί η μεθοδολογία διασύνδεσης προσωπικών υπολογιστών στο δίκτυο και στα υπολογιστικά συστήματα του οργανισμού όπως επίσης και οι ελάχιστες απαιτήσεις ασφαλείας που θα πρέπει να τηρούνται από τους ιδιοκτήτες των υπολογιστών αυτών .

12.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται για όλα τα μέσα που δύνανται να συνδέονται στο δίκτυο του Πανεπιστημίου, ήτοι φορητοί υπολογιστές (laptops), κινητά τηλέφωνα, tablets κλπ.

12.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Προστασίας Δεδομένων
- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- Προσωπικό Πανεπιστημίου (διοικητικό και εκπαιδευτικό)

12.4 ΠΕΡΙΓΡΑΦΗ

12.4.1 Χρήση Συσκευών

12.4.1.1. Γενικοί Κανόνες

Απαγορεύεται η χρήση μη εξουσιοδοτημένων/εγκεκριμένων φορητών υπολογιστών και/ή άλλων συσκευών όπως περιγράφονται παραπάνω. Η χρήση μπορεί να εκτελείται μόνο από εγκεκριμένες από το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής του Πανεπιστημίου συσκευές. Μετά την έγκριση χρήσης οποιασδήποτε συσκευής, δεν επιτρέπεται να γίνουν τροποποιήσεις και εγκαταστάσεις νέων προγραμμάτων χωρίς την προηγούμενη άδεια της Διεύθυνσης Πληροφορικής. Οι συσκευές θα πρέπει να ελέγχονται ανά τακτά χρονικά διαστήματα από την Διεύθυνση Πληροφορικής.

12.4.1.2.Εγγραφή στο Μητρώο

Οι συσκευές BYOD δεν εγγράφονται στο μητρώο συσκευών του οργανισμού αλλά στη λίστα συσκευών του Μέρους Γ'. Κατ' ελάχιστο θα πρέπει να αναφέρονται ο κάτοχος της συσκευής, ο σειριακός αριθμός της, το όνομα υπολογιστή, η Διεύθυνση του οργανισμού όπου χρησιμοποιείται και τα επιπλέον εγκεκριμένα προγράμματα που έχουν εγκατασταθεί.

12.4.1.3. Ευθύνη Τεχνικής Υποστήριξης

Το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής διατηρεί το δικαίωμα, χωρίς να είναι υποχρεωμένο να ενημερώσει πρώτα τον χρήστη, να διακόψει και/'η να απαγορεύσει τη σύνδεση συσκευής στο δίκτυο εάν επηρεάζονται θέματα ασφαλείας του δικτύου.

12.5 Ασφάλεια Συσκευής

12.5.1 Ρυθμίσεις συσκευής

Για να μπορεί να συνδεθεί μια συσκευή στο δίκτυο του Πανεπιστημίου, θα πρέπει ο ιδιοκτήτης της να έρθει σε συνεννόηση με το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής.

12.5.2 Ελάχιστα κριτήρια ασφάλειας

Σαν ελάχιστα κριτήρια ασφάλειας ορίζονται τα παρακάτω:

Α. Λειτουργικό σύστημα

Windows 10, έκδοση 1809 και νεότερη
Android έκδοση 6.0 (Marshmallow) ή iOS έκδοση 11 για κινητές συσκευές

Β. Ισχυρός κωδικός log-in χρήστη

Γ. Εγκατεστημένο πρόγραμμα antivirus

Δ. Ενεργό firewall (μόνο για υπολογιστές)

Ε. Προφίλ χρήστη (για χρήση μόνο για εργασία στο Πανεπιστήμιο)

12.5.3 Εγκεκριμένα Προγράμματα

12.5.3.1 Για την εξασφάλιση της σύνδεσης θα πρέπει η συσκευή να έχει εγκατεστημένα μόνο προγράμματα όπως αυτά αναφέρονται στο Μέρος Α’, (Λίστα Εγκεκριμένων Προγραμμάτων).

12.5.3.2. Εάν απαιτείται η εγκατάσταση και χρήση προγραμμάτων που δεν αναφέρονται στη λίστα εγκεκριμένων προγραμμάτων θα πρέπει να γίνεται αίτημα προς τη Διεύθυνση Πληροφορικής, ώστε να εξεταστεί κατά πόσο το πρόγραμμα πληρεί τους όρους ασφάλειας της πολιτικής ασφαλείας της διεύθυνσης όπου θα χρησιμοποιηθεί η συσκευή και σε περίπτωση θετικής έκβασης του ελέγχου, το συγκεκριμένο πρόγραμμα να συμπεριληφθεί στο Μέρος Β’ (Λίστα Πρόσθετων Εγκεκριμένων Προγραμμάτων).

12.5.3.3. Όλα τα προγράμματα των παραπάνω παραγράφων θα πρέπει να συνοδεύονται από πιστοποιητικό γνησιότητας, να υπάρχουν σε ισχύ οι απαιτούμενες άδειες χρήσης και να είναι ενημερωμένα στην τελευταία διαθέσιμη έκδοση.

12.6 Τεχνική Υποστήριξη

Η τεχνική υποστήριξη των συσκευών που εμπίπτουν στην παρούσα πολιτική από πλευράς Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής περιορίζεται μόνο σε επίλυση θεμάτων σύνδεσης με το δίκτυο. Κάθε άλλο τεχνικό πρόβλημα αποτελεί ευθύνη του ιδιοκτήτη της συσκευής.

12.7 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

- Παράρτημα ΙΙ.1 – Λίστα Εγκεκριμένων Προγραμμάτων
- Παράρτημα ΙΙ.2 – Λίστα Πρόσθετων Εγκεκριμένων Προγραμμάτων
- Μέρος Γ’ – Μητρώο Συσκευών BYOD

12.8 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
1. ΕΠ.05.02, Μητρώο συσκευών BYOD	Αρχείο excel		
2. Μέρος Α’ παρούσης	Φυσικό Αρχείο		

Μέρος Α’

ΛΙΣΤΑ ΣΥΣΚΕΥΩΝ (BYOD)

Α/Α	Όνομα Κατόχου	Σειριακός Συσκευής	Όνομα Υπολογιστή	Γραφείο Υπαλλήλου	Επιπλέον Προγράμματα

13 ΠΟΛΙΤΙΚΗ ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ

13.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να καθοριστούν οι κατηγορίες στις οποίες κατατάσσονται τα πληροφοριακά περιουσιακά στοιχεία του οργανισμού, ανάλογα με τη σημασία τους και να περιγραφεί ο τρόπος διαχείρισης για την κάθε κατηγορία.

13.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται για όλα τα πληροφοριακά περιουσιακά στοιχεία του οργανισμού, τα οποία εμπίπτουν στο πεδίο εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας της Πληροφορίας.

13.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Προστασίας Δεδομένων
- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- Προσωπικό Πανεπιστημίου (διοικητικό και εκπαιδευτικό)

13.4 ΠΕΡΙΓΡΑΦΗ

13.4.1. Κατηγοριοποίηση εγγράφων και λοιπών πληροφοριακών περιουσιακών στοιχείων

Τα προσωπικά δεδομένα που υφίστανται επεξεργασία μέσω των συστημάτων του Πανεπιστημίου, πρέπει να προστατεύονται σύμφωνα με την ταξινόμηση που λαμβάνουν καθ 'όλη τη διάρκεια του κύκλου ζωής τους, από τη συλλογή ή δημιουργία έως την καταστροφή.

Τα έγγραφα που εντάσσονται στο Σύστημα Διαχείρισης Προστασίας Προσωπικών Δεδομένων κατηγοριοποιούνται και λαμβάνουν τους παρακάτω χαρακτηρισμούς:

α) Αδιαβάθμητα – Δεν περιέχουν Προσωπικά Δεδομένα

β) Εμπιστευτικά (confidential) – Περιέχουν Προσωπικά Δεδομένα

γ) Απόρρητα (secret) – Περιέχουν Ευαίσθητα Προσωπικά Δεδομένα

Αρμόδιοι για την κατάταξη των εγγράφων στις παραπάνω κατηγορίες είναι οι υπεύθυνοι των εμπλεκόμενων οργανωτικών μονάδων.

Τα δεδομένα προσωπικού χαρακτήρα ή αλλιώς προσωπικά δεδομένα χαρακτηρίζονται ως εμπιστευτικά, ενώ τα ευαίσθητα προσωπικά δεδομένα ως απόρρητα. Στην παράγραφο 13.4.2 ορίζεται τι είναι προσωπικά δεδομένα και καταγράφονται στο Μητρώο.

Τα πληροφοριακά περιουσιακά στοιχεία που εντάσσονται στο Σύστημα Διαχείρισης Προστασίας Προσωπικών Δεδομένων Πληροφορίας κατατάσσονται στις ακόλουθες βασικές κατηγορίες:

α) Μικρής κρισιμότητας - Δεν περιέχουν Προσωπικά Δεδομένα

β) Μεσαίας κρισιμότητας – Περιέχουν Προσωπικά Δεδομένα

γ) Μεγάλης κρισιμότητας – Περιέχουν Ευαίσθητα Προσωπικά Δεδομένα

Αρμόδιοι για την κατάταξη των λοιπών πληροφοριακών περιουσιακών στοιχείων στις παραπάνω κατηγορίες είναι ο Υπεύθυνος Προστασίας Δεδομένων, σε συνεργασία με τα κατά περίπτωση αρμόδια στελέχη.

Στο έντυπο «ΕΠ.01.02 Κατάλογος Περιουσιακών Στοιχείων Πληροφορίας» καταγράφονται τα βασικά στοιχεία του εξοπλισμού και των πληροφοριακών συστημάτων του οργανισμού.

Η σχετική καταγραφή της κατάταξης περιγράφεται στη Διαδικασία «Εκτίμηση Επικινδυνότητας & Αντιμετώπιση Κινδύνων Ασφάλειας Πληροφοριών».

13.4.2. Ορισμός προσωπικών δεδομένων

‘Δεδομένα προσωπικού χαρακτήρα’ (‘personal data’): Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (‘υποκείμενο των δεδομένων’). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε αναγνωριστικό ταυτότητας ή σε έναν ή

περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

'Ευαίσθητα Δεδομένα': Ορισμένοι τύποι των προσωπικών δεδομένων θεωρούνται ευαίσθητα, και απαιτούν ένα υψηλότερο επίπεδο φροντίδας και προστασίας και περιλαμβάνουν:

- Πολιτικές απόψεις,
- Στοιχεία φυλετικής καταγωγής,
- Δεδομένα που αφορούν τη σεξουαλική ζωή του ατόμου,
- Θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
- Συμμετοχή σε συνδικαλιστική οργάνωση,
- Πληροφορίες για την σωματική ή ψυχική υγεία,
- Στοιχεία για ποινικές διώξεις ή καταδίκες,
- Βιομετρικά στοιχεία,
- Γενετικά δεδομένα,
- Πληροφορίες που αφορούν τα παιδιά

'Επεξεργασία' ('processing'): Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

'Υπεύθυνος επεξεργασίας' ('controller'): Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

'Εκτελών την επεξεργασία' ('processor'): Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

'Παραβίαση δεδομένων προσωπικού χαρακτήρα' ('personal data breach'): η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

13.4.3. Διαχείριση πληροφοριακών στοιχείων ανάλογα με την κατηγορία στην οποία εντάσσονται

Η διαχείρισή των εγγράφων ανά κατηγορία γίνεται όπως περιγράφεται στη συνέχεια:

Τα απόρρητα αρχεία περιέχουν εξαιρετικά εμπιστευτικές πληροφορίες και πρόσβαση σε αυτά έχει η Διοίκηση και εξουσιοδοτημένα από αυτήν υπάλληλοι. Τα απόρρητα αρχεία πρέπει να φέρουν σχετική σήμανση και είναι σφραγισμένα όταν είναι σε έντυπη μορφή, ενώ όταν είναι σε ηλεκτρονική μορφή η πρόσβαση αλλά και η επεξεργασία τους πρέπει να προστατεύεται με κωδικό.

Τέτοια έγγραφα είναι:

- Τα οικονομικά στοιχεία του Πανεπιστημίου
- Ευαίσθητα προσωπικά δεδομένα (ενδεικτικά, στοιχεία φοιτητών με αναπηρίες)

Τα εμπιστευτικά έγγραφα περιέχουν πληροφορίες, η μη εξουσιοδοτημένη χρήση των οποίων μπορεί να επηρεάσει την αποτελεσματικότητα των λειτουργιών, να προκαλέσει οικονομικές απώλειες ή μείωση της αξιοπιστίας του Πανεπιστημίου. Η πρόσβαση σε αυτά γίνεται από κατάλληλα εξουσιοδοτημένους υπαλλήλους και η δημοσιοποίησή των πληροφοριών που εμπεριέχουν δεν επιτρέπεται.

Τέτοια έγγραφα είναι ενδεικτικά:

- Στοιχεία φοιτητών/υπαλλήλων Α.Μ.Ε.Α.
- Στοιχεία φοιτητών δικαιούχων δωρεάν στέγασης/φοίτησης
- Προσωπικά δεδομένα υγείας εξεταζόμενων από την Ιατρό Εργασίας
- Πληροφορίες αναρρωτικών αδειών υπαλλήλων
- Λίστες στοιχείων των ερευνητών πεδίου
- Λίστες με στοιχεία ατόμων που συμμετέχουν σε προσωπικές συνεντεύξεις και το περιεχόμενο αυτών
- Τα στοιχεία της κάθε έρευνας

Τα αδιαβάθμητα έγγραφα περιέχουν πληροφορίες οι οποίες δεν είναι εμπιστευτικές και μπορούν να δημοσιοποιηθούν μετά από έγκριση του αρμόδιου προϊσταμένου με την προϋπόθεση ότι η δημοσιοποίησή τους δεν αντιβαίνει σε οποιαδήποτε σχετική νομική διάταξη ή/και κώδικα δεοντολογίας και ηθικής και σε κάθε περίπτωση χωρίς να υπάρχει επίπτωση για το Πανεπιστήμιο, το προσωπικό του Πανεπιστημίου, την ακαδημαϊκή κοινότητα και τους συνεργάτες του Πανεπιστημίου .

13.4.4. Διαχείριση πληροφοριακών στοιχείων ανάλογα με την κρισιμότητα

Για ότι αφορά την κρισιμότητα των περιουσιακών στοιχείων ακολουθούμε τα εξής:

Για τα μικρής κρισιμότητας λοιπά πληροφοριακά περιουσιακά στοιχεία δεν απαιτείται να ληφθούν μέτρα προστασίας τους.

Για τα μεσαίας κρισιμότητας λοιπά πληροφοριακά περιουσιακά στοιχεία απαιτείται η λήψη μέτρων προστασίας τους.

Για τα μεγάλης κρισιμότητας λοιπά πληροφοριακά περιουσιακά στοιχεία, τα οποία ορίζεται ότι είναι ζωτικής σημασίας για τον οργανισμό λαμβάνονται επιπλέον μέτρα προστασίας σε σύγκριση με τα μεσαίας κρισιμότητας.

13.5 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Οποιοσδήποτε εργαζόμενος παραβιάσει την παρούσα Πολιτική Ασφάλειας ενδέχεται να υποστεί πειθαρχικές κυρώσεις.

13.6 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

- ΕΠ.01.01 Πίνακας Καταγραφής Προσωπικών Δεδομένων
- ΕΠ.01.02 Κατάλογος Περιουσιακών Στοιχείων Πληροφορίας
  (Από την Δ.01 ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΩΝ)

13.7 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
ΕΠ.05.01 ΜΗΤΡΩΟ ΣΥΣΚΕΥΩΝ	Ηλεκτρονική	Επ’ αόριστον	Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ	Ηλεκτρονική	Επ’ αόριστον	Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

14 Πολιτική Τηλε-εργασίας

14.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να περιγραφεί η μεθοδολογία διασύνδεσης από απομακρυσμένους υπολογιστές στο εσωτερικό δίκτυο και στα υπολογιστικά συστήματα του Πανεπιστημίου για σκοπούς τηλε-εργασίας και να περιγράψει τις μεθόδους και τις εφαρμογές οι οποίες μπορούν να χρησιμοποιηθούν για την εκτέλεση τηλεδιασκέψεων με το προσωπικό ή/και εξωτερικούς συνεργάτες ή/και πελάτες του οργανισμού.

14.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε όλο το προσωπικό για όλα τα μέσα που χρησιμοποιούνται για τηλε-εργασία και δύνανται να συνδέονται στο εσωτερικό δίκτυο ή / και δύνανται να χρησιμοποιούνται για την εκτέλεση μίας τηλεδιάσκεψης, ήτοι σταθεροί υπολογιστές (desktops), φορητοί υπολογιστές (laptops), κινητά τηλέφωνα, tablets κλπ.

14.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Προστασίας Δεδομένων
- Προϊστάμενος Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής
- Προσωπικό Πανεπιστημίου (διοικητικό και εκπαιδευτικό)

14.4 ΠΕΡΙΓΡΑΦΗ

14.4.1 Τηλε-εργασία – Χρήση Συσκευών

Η εκτέλεση τηλε-εργασίας μπορεί να γίνεται μόνο με πρόσβαση στις εσωτερικές συσκευές που προμηθεύει το Πανεπιστήμιο από εξωτερικές συσκευές των χρηστών με VPN σύνδεση.

Απαγορεύεται η χρήση μη εξουσιοδοτημένων / εγκεκριμένων υπολογιστών και / ή άλλων συσκευών. Μετά την έγκριση χρήσης οποιασδήποτε συσκευής, δεν επιτρέπεται να γίνουν τροποποιήσεις και εγκαταστάσεις νέων προγραμμάτων χωρίς την προηγούμενη άδεια του Τμήματος Πληροφορικής. Οι εξουσιοδοτημένες συσκευές μπορεί να ελέγχονται ανά τακτά χρονικά διαστήματα από το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής.

14.4.2 Ρυθμίσεις Ασφάλειας Συσκευής

Για να μπορεί να συνδεθεί μια συσκευή απομακρυσμένα στο εσωτερικό δίκτυο με την υλοποίηση της τεχνολογίας VPN (Virtual Private Network), θα πρέπει η συσκευή να ελεγχθεί από το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής, ότι καλύπτει ορισμένα ελάχιστα κριτήρια ασφάλειας.

Σαν ελάχιστα κριτήρια ασφάλειας ορίζονται τα παρακάτω:

Α. Λειτουργικό σύστημα:

Windows 10, έκδοση 1809 και νεότερη
Android έκδοση 6.0 (Marshmallow) ή iOS έκδοση 11 για κινητές συσκευές

Β. Ισχυρός κωδικός log-in χρήστη, όπως προβλέπεται από την Πολιτική Απορρήτου Κωδικών Χρηστών.

Γ. Εγκατεστημένο και ενημερωμένο πρόγραμμα antivirus

Δ. Ενεργό firewall (μόνο για υπολογιστές)

14.4.3 Ρυθμίσεις Ασφαλείας Σύνδεσης

Η απομακρυσμένη σύνδεση πρέπει να είναι καλύπτει όλες τις προδιαγραφές ασφαλείας. Για την εξασφάλιση της σύνδεσης θα πρέπει να ρυθμιστεί η επίτευξη της να υλοποιείται με την χρήση του ασφαλούς πρωτοκόλλου (π.χ. IPSec, SSLVPN). Επίσης, όπου είναι εφικτό, γίνεται χρήση ιδιωτικού / δημόσιου κλειδιού.

Επιτρέπεται η σύνδεση σε υπολογιστικά συστήματα του Πανεπιστημίου μέσω υπηρεσίας «απομακρυσμένης επιφάνειας εργασίας» (Remote Desktop Protocol), μόνο όταν αυτή γίνεται μέσω ασφαλούς εικονικού ιδιωτικού δικτύου (VPN).

Με τη χρήση της VPN τεχνολογίας σε προσωπικό εξοπλισμό, οι χρήστες θα πρέπει να κατανοήσουν ότι τα μηχανήματα που χρησιμοποιούν για την πραγματοποίηση της σύνδεσης τους, καθίστανται προέκταση του δικτύου του οργανισμού. Συνέπεια τούτου είναι ότι πρέπει να ακολουθούν τις πολιτικές ασφαλείας του οργανισμού και ο ιδιωτικός εξοπλισμός τους υπόκειται στους ίδιους κανόνες που εφαρμόζονται για τον εξοπλισμό του οργανισμού.

14.5 Τηλε-εργασία – Ευθύνες

Για την εκτέλεση τηλε-εργασίας θα πρέπει να εξασφαλίζεται ότι ακολουθούνται οι παρακάτω όροι και κανόνες τόσο από το Τμήμα Πληροφορικής του οργανισμού, όσο και από τους χρήστες.

14.5.1 Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής

- Παρέχει κάθε δυνατή βοήθεια και εκπαίδευση στους χρήστες σε θέματα απομακρυσμένης σύνδεσης στο εσωτερικό δίκτυο του οργανισμού.
- Εξασφαλίζει ότι οι χρήστες που εκτελούν τηλε-εργασία περιορίζονται στους ελάχιστους απαραίτητους με βάση τα καθήκοντά τους και οι προσβάσεις τους είναι οι ελάχιστες απαραίτητες, για την εκτέλεση των καθηκόντων τους, σύμφωνα με την υφιστάμενη Πολιτική Προσβάσεων του οργανισμού.
- Αξιολογεί και όπου είναι τεχνικά εφικτό, παρέχει στους ασκούντες τηλε-εργασία τη δυνατότητα χρήσης της επαγγελματικού ταχυδρομείου (email) για αποστολή ή λήψη μηνυμάτων για σκοπούς τηλεργασίας από εξωτερικό δίκτυο.
- Φροντίζει για τη λήψη αντιγράφων ασφαλείας για αρχεία με προσωπικά δεδομένα, τα οποία υφίστανται επεξεργασία στο πλαίσιο δραστηριοτήτων τηλεργασίας με βάση την Πολιτική Αντιγράφων Ασφαλείας.

14.5.2 Χρήστες Τηλε-εργασίας

Με την βοήθεια και τις συμβουλές του Τμήματος Στατιστικής, Μηχανοργάνωσης και Πληροφορικής του οργανισμού, οι χρήστες θα πρέπει να εξασφαλίζουν και να μεριμνούν για τα παρακάτω:

- Την εγκατάσταση αντιϊκού προγράμματος και την καθημερινή του ενημέρωση, όπως και την ενεργοποίηση και λειτουργία του firewall της συσκευής τους.
- Τη σύνδεση του σταθμού εργασίας στον εξοπλισμό του παρόχου internet, που διαθέτει ο χώρος, μέσω καλωδίου δικτύου. Εάν αυτό δεν είναι εφικτό, και πρέπει να συνδέεται στο διαδίκτυο μέσω ασύρματου δικτύου, θα πρέπει να ρυθμιστεί κατάλληλα ο εξοπλισμός του παρόχου, ώστε να χρησιμοποιεί το πρωτόκολλο ασφαλείας WPA2 και ισχυρό κωδικό πρόσβασης.
- Την εγκατάσταση των τελευταίων διαθέσιμων ενημερώσεων του λειτουργικού συστήματος και των εφαρμογών του υπολογιστή τους.

- Τη χρήση προγραμμάτων πλοήγησης στο διαδίκτυο (π.χ. Microsoft Edge, Google Chrome, Mozilla Firefox κλπ) με ανώνυμη περιήγηση ή τη διαγραφή από το ιστορικό των συνδέσμων που σχετίζονται με την τηλε-εργασία τους.
- Την αποφυγή χρήσης προσωπικού ηλεκτρονικού ταχυδρομείου (π.χ. gmail, yahoo, hotmail) για αποστολή ή λήψη μηνυμάτων για σκοπούς τηλεργασίας. Αντ' αυτού, θα πρέπει να χρησιμοποιείται η επαγγελματική ηλεκτρονική διεύθυνση την οποία παρέχει ο Οργανισμός. Εάν αυτό δεν είναι τεχνικά εφικτό, τότε το περιεχόμενο των μηνυμάτων που αφορά προσωπικά δεδομένα πρέπει να κρυπτογραφείται κατάλληλα (π.χ. είτε ολόκληρο το μήνυμα είτε μόνο τα συνημμένα αρχεία).
- Την αποφυγή χρήσης εφαρμογών ανταλλαγής μηνυμάτων (κείμενο ή/και βίντεο) για τους σκοπούς της τηλεργασίας από υπηρεσίες των οποίων τα χαρακτηριστικά ασφάλειας (κρυπτογράφηση, ρυθμίσεις προστασίας δεδομένων) αξιολογούνται ως μη ισχυρά.
- Την αποφυγή αποθήκευσης αρχείων σε τοπικό υπολογιστή ή υπηρεσία διαδικτυακής αποθήκευσης (π.χ. Dropbox, One Drive, Google Drive, κλπ). Αν αυτό δεν είναι εφικτό, προστασία τουλάχιστον με κωδικό πρόσβασης των αποθηκευμένων αρχείων της εργασίας τους ή την κρυπτογράφησή τους, ιδιαίτερα αν τα αρχεία αυτά περιέχουν προσωπικά δεδομένα.
- Την αποθήκευση των αρχείων που χρησιμοποιούν για την τηλε-εργασία, σε διακριτούς φακέλους, διαφορετικούς από αυτούς που χρησιμοποιούν για τα προσωπικά τους αρχεία.
- Τη λήψη αντίγραφου ασφαλείας των αρχείων με προσωπικά δεδομένα, σύμφωνα με τις οδηγίες του τμήματος πληροφορικής του Πανεπιστημίου.
- Εφαρμογή της Πολιτικής Καθαρής Οθόνης στις συσκευές που χρησιμοποιούνται για τηλε-εργασία με κλείδωμά τους (π.χ. προφύλαξη οθόνης, με κωδικό απενεργοποίησης) αν μείνουν ανενεργές.

14.6 Τηλεδιασκέψεις – Ασφάλεια Σύνδεσης

Ο χρήστης, από την απομακρυσμένη του θέση, καταβάλλει κάθε προσπάθεια ώστε ο σταθμός εργασίας του να συνδέεται στον εξοπλισμό του παρόχου internet, που διαθέτει ο χώρος, μέσω καλωδίου δικτύου. Εάν αυτό δεν είναι εφικτό, και πρέπει να συνδέεται στο διαδίκτυο μέσω ασύρματου δικτύου, θα πρέπει να ρυθμιστεί κατάλληλα ο εξοπλισμός του παρόχου, ώστε να χρησιμοποιεί το πρωτόκολλο ασφαλείας WPA2 και ισχυρό κωδικό πρόσβασης.

Η αποθήκευση αρχείων στον τοπικό υπολογιστή του χρήστη θα πρέπει να αποφεύγεται. Όλα τα αρχεία, τα οποία θα χρειαστεί να αποθηκευτούν τοπικά, θα πρέπει να προστατεύονται με κωδικό πρόσβασης ή να κρυπτογραφούνται στο λειτουργικό σύστημα του χρήστη.

14.7 Ασφάλεια Εφαρμογών Τηλεδιάσκεψης

Για τη επιλογή χρήσης συγκεκριμένης εφαρμογής εξετάζονται και εφαρμόζονται οι παρακάτω κανόνες για την προστασία των προσωπικών δεδομένων αλλά και των ευαίσθητων πληροφοριών του οργανισμού.

- Θα πρέπει η επιλεγμένη εφαρμογή να υποστηρίζει κρυπτογράφηση από άκρη σε άκρη (end-to-end encryption).
- Οι όροι χρήσης της επιλεγμένης εφαρμογής να καλύπτουν τις απαιτήσεις ασφαλείας του οργανισμού, όπως αυτές έχουν αποτυπωθεί στη γενική πολιτική ασφαλείας του οργανισμού.
- Ο σύνδεσμος μιας προγραμματισμένης τηλεδιάσκεψης δεν θα πρέπει να δημοσιοποιείται πουθενά, παρά μόνο να κοινοποιείται στους συμμετέχοντες και συνιστάται η χρήση κωδικού ή εναλλακτικά δωματίου αναμονής.
- Κατά τη διάρκεια της τηλεδιάσκεψης, απαγορεύεται η καταγραφή της σε video, το οποίο μπορεί να αναπαραχθεί αργότερα, όπως απαγορεύεται και η λήψη στιγμιότυπων των συμμετεχόντων, χωρίς την έγκριση όλων των συμμετεχόντων.

14.8 Εφαρμογές Τηλεδιάσκεψης

Το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής είναι αρμόδιο για την επιλογή και έγκριση των κατάλληλων εφαρμογών τηλεδιάσκεψης που καλύπτουν τις ανωτέρω προδιαγραφές. Δεν επιτρέπεται η χρήση μη εξουσιοδοτημένων/εγκεκριμένων εφαρμογών τηλεδιασκέψεων. Δεν επιτρέπεται η εγκατάσταση οποιασδήποτε εφαρμογής τηλεδιάσκεψης από τους χρήστες στους τοπικούς σταθμούς εργασίας τους χωρίς την προηγούμενη γραπτή έγκριση του τμήματος πληροφορικής. Οι τηλεδιασκέψεις διοργανώνονται μέσω της πλατφόρμας zoom κατόπιν ειδικής άδειας και μέσω του google meet από τον ιδρυματικό λογαριασμό.

14.9 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Οποιοσδήποτε εργαζόμενος παραβιάσει την παρούσα Πολιτική Ασφάλειας ενδέχεται να υποστεί πειθαρχικές κυρώσεις.

14.10 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

- Ουδέν

14.11 ΑΡΧΕΙΑ

Ουδέν

ΠΑΡΑΤΗΜΑ ΙΙ

Λίστα Προγραμμάτων

1 Εγκεκριμένα

Windows 10 Pro και ανώτερο
Office 2016 Pro και ανώτερο
Acrobat reader
7zip
Eset Antivirus
Skype
CDBurnXP
WinRar
Putty
CCleaner
Vmware Player
Chrome
Firefox
Vlc
Java
Teamviewer
Anydesk
GoogleEarth
MPC Home Cinema
Adobe Air
Adobe Flash
Adblock Plus

2 Πρόσθετα

Όλα τα λογισμικά των οποίων δεν απαιτείται αγορά και η άδεια χρήσης τους επιτρέπεται σε εργασιακό περιβάλλον, εφόσον εγκριθούν από το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής επιτρέπονται.

15 Πολιτική Επικοινωνίας με τις Αρχές

15.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να καθοριστούν οι αρμοδιότητες για την επικοινωνία του Πανεπιστημίου σχετικά με θέματα ασφάλειας της πληροφορίας με τις αρμόδιες Αρχές.

15.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε κάθε περίπτωση επικοινωνίας σχετικά με θέματα ασφάλειας της πληροφορίας με τις αρμόδιες Αρχές.

15.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Πρύτανης
- Υπεύθυνος Προστασίας Δεδομένων

15.4 ΠΕΡΙΓΡΑΦΗ

15.4.1 Επικοινωνία με Αρμόδιες Αρχές

α) Υπεύθυνος Επικοινωνίας με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) είναι ο Υπεύθυνος Προστασίας Δεδομένων.

β) Ο Πρύτανης εκπροσωπεί το Πανεπιστήμιο ενώπιον της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

γ) Σε περιπτώσεις περιστατικών παραβίασης της ασφάλειας Προσωπικών Δεδομένων και εφόσον συντρέχει λόγος να εμπλακούν αρμόδιες Αρχές (π.χ. ΑΠΔΠΧ, Αστυνομία, Πυροσβεστική, κλπ) αρμόδιος επικοινωνίας είναι ο Πρύτανης και ο Υπεύθυνος Προστασίας Δεδομένων.

Όταν απαιτείται να δοθεί κάποια απάντηση ή στοιχεία στις αρμόδιες Αρχές, ο Υπεύθυνος Προστασίας Δεδομένων σε συνεργασία με τη Νομική Υπηρεσία και τον Πρύτανη προετοιμάζει τα σχετικά έγγραφα..

15.4.2 Επικοινωνία στο Πλαίσιο Εφαρμογής Σχεδίων Έκτακτης Ανάγκης

Σε περιπτώσεις επικοινωνίας στα πλαίσια εφαρμογής σχεδίων έκτακτης ανάγκης (βλ. σχετική Διαδικασία), οι αρμοδιότητες για την επικοινωνία καθορίζονται στα πλαίσια των σχεδίων αντιμετώπισης έκτακτης ανάγκης που καταρτίζονται.

15.5 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Οποιοσδήποτε εργαζόμενος παραβιάσει την παρούσα Πολιτική Ασφάλειας ενδέχεται να υποστεί πειθαρχικές κυρώσεις.

15.6 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

- Ουδέν

15.7 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Αλληλογραφία σχετική με την Ασφάλεια Δεδομένων	Έντυπη / ηλεκτρονική	Επ’ αόριστον	Υπεύθυνος Προστασίας Δεδομένων

16 Πολιτική Διαχείρισης Ασφάλειας σε Συμφωνίες με Τρίτους

16.1 ΣΚΟΠΟΣ

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι να καθοριστούν οι απαιτήσεις για τους όρους που θα πρέπει να συμφωνούνται αναφορικά με την ασφάλεια των προσωπικών δεδομένων κατά την κατάρτιση σχετικών συμφωνιών με τρίτους (παρόχους υπηρεσιών, προμηθευτές κλπ.).

16.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται σε κάθε περίπτωση σύναψης συμφωνίας με τρίτο μέρος, στα πλαίσια της οποίας γίνεται επεξεργασία προσωπικών δεδομένων, εκ μέρους οιουδήποτε εκ των αντισυμβαλλομένων.

16.3 ΥΠΕΥΘΥΝΟΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

- Υπεύθυνος Προστασίας Δεδομένων
- Υπηρεσίες Πανεπιστημίου που καταρτίζουν συμβάσεις (πχ ΕΛΚΕ)

16.4 ΠΕΡΙΓΡΑΦΗ

Όταν συνάπτονται έγγραφες συμφωνίες με τρίτους, το αντικείμενο των οποίων μπορεί να έχει επίπτωση στην Ασφάλεια των προσωπικών δεδομένων που διαχειρίζεται τόσο το Πανεπιστήμιο, όσο και το αντισυμβαλλόμενο μέρος, θα πρέπει κατά την κατάρτιση της συμφωνίας να εξετάζεται μια σειρά θεμάτων και, αν κρίνεται απαραίτητο, να καθορίζονται στο πλαίσιο της συμφωνίας οι σχετικές λεπτομέρειες.

Τα θέματα που θα εξετάζονται είναι κατ' ελάχιστον τα ακόλουθα:

1. Η τήρηση της εμπιστευτικότητας της πληροφορίας και ιδιαίτερα των προσωπικών δεδομένων και από τις δύο πλευρές, σύμφωνα με το νομικό κανονιστικό πλαίσιο, καθώς και τα τυχόν πνευματικά δικαιώματα.
2. Η διαδικασία που θα ακολουθείται σε περίπτωση διαρροής (ή υποψίας διαρροής) δεδομένων·
3. Περιπτώσεις κατά τις οποίες συμφωνείται ότι παύουν να ισχύουν οι όροι της συμφωνίας (όλοι ή μέρος τους), όπως π.χ. ανωτέρα βία·

4. Σε περιπτώσεις σύνδεσης του αντισυμβαλλόμενου στο δίκτυο του Πανεπιστημίου ή/και σύνδεσης του Πανεπιστημίου στο δίκτυο του αντισυμβαλλόμενου, το είδος της σύνδεσης και ο σκοπός αυτής, καθώς και τα άτομα που είναι εξουσιοδοτημένα να κάνουν σύνδεση στο δίκτυο από πλευράς κάθε αντισυμβαλλομένου·
5. Σε περιπτώσεις χρήσης δανειζόμενου εξοπλισμού ή λογισμικού από έναν εκ των αντισυμβαλλομένων, ο σκοπός της χρήσης αυτής, καθώς και οι σχετικές λεπτομέρειες, όπως για παράδειγμα, η δυνατότητα αλλαγής configuration. Επίσης, τα άτομα που είναι εξουσιοδοτημένα να κάνουν χρήση δανειζόμενου εξοπλισμού/λογισμικού από πλευράς κάθε αντισυμβαλλομένου·
6. Η χρήση από έναν εκ των αντισυμβαλλομένων κωδικών, ποιος τους καθορίζει και πώς αυτοί γνωστοποιούνται ή/και αλλάζουν·
7. Η κατάργηση κωδικών/προσβάσεων, καθώς και η επιστροφή τυχόν πληροφοριακών στοιχείων από τον έναν εκ των αντισυμβαλλομένων στον άλλο·
8. Οι πληροφορίες που παρέχονται από έναν εκ των αντισυμβαλλομένων στον άλλον σχετικά με τα άτομα τα οποία εξουσιοδοτούνται·
9. Η διαδικασία που θα ακολουθείται σε περιπτώσεις αποχώρησης εξουσιοδοτημένου προσωπικού·
10. Οποιεσδήποτε περιπτώσεις για τις οποίες απαιτείται γραπτή ενημέρωση του ενός εκ των αντισυμβαλλομένων από τον άλλο·
11. Η διαδικασία που θα ακολουθηθεί με την ολοκλήρωση της σύμβασης, καθώς και τυχόν πληροφοριακά περιουσιακά στοιχεία που θα πρέπει να επιστραφούν ή να καταστραφούν ή να διακοπεί η χρήση ή και/η πρόσβαση σε αυτά, από τον ένα εκ των αντισυμβαλλομένων στον άλλο, εφόσον κρίνεται απαραίτητο·
12. Οι διαδικασίες/μέθοδοι που χρησιμοποιούνται για τη διασφάλιση της πληροφορίας από πλευράς καθενός εκ των αντισυμβαλλομένων.
13. Πολιτικές ασφαλείας που θα πρέπει να υιοθετηθούν από τους αντισυμβαλλόμενους·
14. Θέματα σύνδεσης τρίτων στο εσωτερικό δίκτυο ενός εκ των αντισυμβαλλομένων, όπου ως τρίτοι ορίζονται συνεργάτες, προμηθευτές κλπ. Συγκεκριμένα, αν η σύνδεση τρίτων θα γίνεται μετά από αίτημα, οι πληροφορίες που θα περιέχονται στο αίτημα, τα άτομα που θα εγκρίνουν το αίτημα, το μέσο με το οποίο θα γίνεται η σύνδεση, τα είδη υπηρεσιών στις οποίες θα έχουν πρόσβαση τρίτοι, ο τρόπος ελέγχου πρόσβασης τρίτου (authentication) κ.λπ.

15. Τυχόν φόρμες ή στοιχεία που συμφωνούνται να χρησιμοποιούνται για αιτήματα παροχής υπηρεσιών, για αιτήματα πρόσβασης, για δήλωση προβλημάτων, κλπ.

Εκτός από τα προαναφερθέντα θέματα, ανάλογα με τις ιδιαιτερότητες της εκάστοτε συμφωνίας, είναι δυνατόν να εξετάζονται και να καθορίζονται και επιπλέον όροι στην κάθε σύμβαση.

Η εξέταση και ο καθορισμός των όρων των συμφωνιών γίνεται από τη Διοίκηση του Πανεπιστημίου, σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων εφόσον η Διοίκηση το κρίνει απαραίτητο.

16.5 ΕΠΙΒΟΛΗ ΠΟΛΙΤΙΚΗΣ

Οποιοσδήποτε εργαζόμενος παραβιάσει την παρούσα Πολιτική Ασφάλειας ενδέχεται να υποστεί πειθαρχικές κυρώσεις.

16.6 ΣΧΕΤΙΚΑ ΕΝΤΥΠΑ

- Ουδέν

16.7 ΑΡΧΕΙΑ

ΠΕΡΙΓΡΑΦΗ	ΜΟΡΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ ΤΗΡΗΣΗΣ
Αρχείο Συμφωνιών / Συμβάσεων με Τρίτους	Έντυπη / ηλεκτρονική	Επ’ αόριστον	Η εκάστοτε υπηρεσία που συνάπτει συμβάσεις με τρίτους