Πολιτικές Ασφάλειας Πληροφοριών

1 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ο Όμιλος σε καθημερινή βάση συλλέγει, αποθηκεύει, επεξεργάζεται και διακινεί δεδομένα προσωπικού χαρακτήρα στα πλαίσια της εκτέλεσης των επιχειρησιακών του λειτουργιών. Η προστασία των δεδομένων προσωπικού χαρακτήρα και των συστημάτων επεξεργασίας τους, είναι στρατηγικής σημασίας για τον Όμιλο προκειμένου να επιτύχει τους βραχυχρόνιους και μακροχρόνιους στόχους του.

Ο Όμιλος, στο πλαίσιο της συμμόρφωσής του με τις βασικές αρχές επεξεργασίας δεδομένων προσωπικού χαρακτήρα, σέβεται τα δικαιώματα των φυσικών προσώπων και εξασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα τα οποία έχει στην κατοχή της:

- συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς, όπως αποτυπώνονται στο Αρχείο Δραστηριοτήτων Επεξεργασίας που τηρεί
- υφίστανται επεξεργασία μόνο για τους σκοπούς για τους οποίους έχουν συλλεχθεί, και εφόσον αυτό απαιτείται, για νομικούς και κανονιστικούς λόγους ή για το έννομο συμφέρον του Ομίλου και δεν υποβάλλονται σε περαιτέρω επεξεργασία,
- είναι κατάλληλα, συναφή και περιορίζονται στα ελάχιστα απαραίτητα για τους σκοπούς επεξεργασίας,
- υπόκεινται σε δίκαιη και νόμιμη επεξεργασία σύμφωνα με τα δικαιώματα των φυσικών προσώπων, είναι ακριβή και επικαιροποιούνται όταν απαιτείται, και ειδικά πριν τη λήψη κρίσιμων αποφάσεων για τα φυσικά πρόσωπα,
- δεν τηρούνται για χρονικό διάστημα μεγαλύτερο από αυτό που απαιτείται για το σκοπό της επεξεργασίας ή για τη συμμόρφωση με το νομικό και κανονιστικό πλαίσιο λειτουργίας
- διατηρούνται ασφαλή από μη εξουσιοδοτημένη πρόσβαση, απώλεια ή καταστροφή,
- μεταφέρονται σε φορείς εντός και εκτός του Ομίλου και της χώρας μόνο υπό την προϋπόθεση ότι εξασφαλίζεται επαρκές επίπεδο προστασίας από τους φορείς αυτούς.

  Τα ανωτέρω τηρούνται από το σύνολο των εργαζομένων του Ομίλου, καθώς και από τρίτα μέρη που εκτελούν εργασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων για λογαριασμό του Ομίλου.

Ο Όμιλος για να διασφαλίσει τα παραπάνω:

- έχει ορίσει Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer)
- εφαρμόζει Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών που καλύπτει το σύνολο των δραστηριοτήτων του για την παρακολούθηση και τον έλεγχο της ασφάλειας των δεδομένων προσωπικού χαρακτήρα ως προς την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητά τους, καθώς και την αξιολόγηση της αποτελεσματικότητας των διαδικασιών και Πολιτικών Ασφάλειας ως προς τη συμμόρφωση με το κανονιστικό πλαίσιο και τις βέλτιστες πρακτικές για την ασφάλεια πληροφοριών,

- εφαρμόζει διαδικασίες για την ικανοποίηση των δικαιωμάτων των φυσικών προσώπων
  - ενημερώνει με σαφήνεια τα φυσικά πρόσωπα σχετικά με την επεξεργασία δεδομένων, σύμφωνα με τις σχετικές νομοθετικές και κανονιστικές απαιτήσεις
  - ενσωματώνει τις απαιτήσεις διαχείρισης δεδομένων προσωπικού χαρακτήρα σε όλες τις λειτουργίες και διεργασίες του Ομίλου που σχετίζονται με την επεξεργασία τους
  - έχει καθορίσει ρόλους και υπευθυνότητες που σχετίζονται με τη διαχείριση των δεδομένων προσωπικού χαρακτήρα,
  - παρέχει σαφείς οδηγίες στο προσωπικό και τα τρίτα μέρη που εκτελούν εργασίες για λογαριασμό του Ομίλου για την ασφαλή χρήση και διαβίβαση των δεδομένων σύμφωνα με το Σύστημα Διαχειρίσεως Ασφάλειας Πληροφοριών,
  - διασφαλίζει ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτα μέρη και η επεξεργασία από άλλους Οργανισμούς για λογαριασμό του Ομίλου, υλοποιείται σε συμμόρφωση με το κανονιστικό πλαίσιο για την προστασία δεδομένων προσωπικού χαρακτήρα καθώς και την παρούσα Πολιτική,
  - σχεδιάζει, υιοθετεί και παρακολουθεί την εφαρμογή συστήματος δεικτών και στόχων για την ασφαλή και νόμιμη διαχείριση των δεδομένων
  - επενδύει στη συνεχή κατάρτιση, ευαισθητοποίηση και εκπαίδευση των εργαζομένων του σε θέματα προστασίας δεδομένων προσωπικού χαρακτήρα, καθώς και στη συνεχή βελτίωση της τεχνογνωσίας και τη διάχυσή της σε όλο το προσωπικό
  - κοινοποιεί την παρούσα Πολιτική σε όλο το προσωπικό και μεριμνά για τη συνεχή αναβάθμισή της, ώστε να επιτυγχάνεται η πλήρης συμμόρφωση με το ισχύον κανονιστικό πλαίσιο.

Ο Όμιλος δεσμεύεται στην αδιάλειπτη παρακολούθηση και τήρηση του κανονιστικού και νομοθετικού πλαισίου, καθώς και των κατευθυντήριων οδηγιών των αρμόδιων οργάνων της Ευρωπαϊκής Ένωσης, αναφορικά με τη διαχείριση της προστασίας των δεδομένων προσωπικού χαρακτήρα.

Το σύνολο του προσωπικού του Ομίλου και των συνεργατών, οι οποίοι έχουν πρόσβαση ή/ και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων για τα οποία είναι Υπεύθυνος Επεξεργασίας ο Όμιλος Ιατρικού Αθηνών, έχουν την ευθύνη της τήρησης των κανόνων της εφαρμοζόμενης Ομιλικής Πολιτικής Διαχείρισης Δεδομένων Προσωπικού Χαρακτήρα.

2 ΧΡΗΣΗΣ ΦΟΡΗΤΩΝ ΣΥΣΚΕΥΩΝ

Η προστασία των φορητών συσκευών είναι πρωταρχικής σημασίας για τον Όμιλο προκειμένου να διατηρείται η εμπιστευτικότητα των πληροφοριών που αποθηκεύονται σε αυτές.

Οι φορητές συσκευές που παραχωρούνται από τον Όμιλο, παραμένουν στην κυριότητά του όπως και κάθε πληροφορία που αποθηκεύεται σε αυτές.

Η Διεύθυνση Ασφάλειας Πληροφοριών σε συνεργασία με τη Διεύθυνση Πληροφορικής, διερευνούν και σχεδιάζουν τα απαραίτητα τεχνικά μέτρα προστασίας των πληροφοριών που αποθηκεύονται σε φορητές συσκευές.

Οι χρήστες φορητών συσκευών είναι υπεύθυνοι για την προστασία του εξοπλισμού που τους έχει παραχωρηθεί. Θα πρέπει να λαμβάνουν όλα τα απαραίτητα μέτρα που έχουν προδιαγραφεί από τη Διεύθυνση Ασφάλειας Πληροφοριών και τη Διεύθυνση Πληροφορικής, ώστε να προστατεύουν τις φορητές συσκευές και τις πληροφορίες που αυτές περιέχουν.

Οι φορητές συσκευές δεν θα πρέπει να μένουν ανεπιτήρητες σε δημόσιους χώρους.

Όταν χρησιμοποιούνται σε δημόσιους χώρους, ειδική μέριμνα θα πρέπει να λαμβάνεται ώστε να μην είναι εύκολη η ανάγνωση πληροφοριών από την οθόνη της συσκευής, από άτομα που βρίσκονται στον ίδιο χώρο.

Οι υπεύθυνοι των τμημάτων στους εργαζόμενους των οποίων έχουν παραχωρηθεί φορητές συσκευές, είναι υπεύθυνοι για τον έλεγχο της ορθής χρήσης τους. Σε περίπτωση εντοπισμού αποκλίσεων από την οριζόμενη ορθή χρήση τους, είναι υποχρεωμένοι να αναφέρουν τα περιστατικά στη Διεύθυνση Ασφάλειας Πληροφοριών.

Οι περιπτώσεις απώλειας ή κλοπής φορητής συσκευής θα πρέπει να αναφέρονται άμεσα στη Διεύθυνση Ασφάλειας Πληροφοριών.

Οι ευαίσθητες πληροφορίες που αποθηκεύονται σε φορητούς υπολογιστές πρέπει να είναι σε κρυπτογραφημένη μορφή.

Σε όλες τις φορητές συσκευές εφαρμόζονται δικλείδες ασφαλείας για την πρόσβαση των χρηστών, με τη χρήση κατάλληλων μηχανισμών ελέγχου (π.χ. κωδικός PIN, όνομα χρήστη/κωδικός προσβάσεως, βιομετρικά στοιχεία). Επιπλέον, εφαρμόζεται ένα δεύτερο στάδιο μηχανισμών ταυτοποιήσεως, που υποστηρίζει την ισχυρή ταυτοποίηση, πριν την πρόσβαση του χρήστη στο δίκτυο του Ομίλου και τις επιχειρηματικές εφαρμογές, που παρέχονται από ή μέσω της συσκευής. Η πρόσβαση στους πόρους του Ομίλου πραγματοποιείται μόνο μέσω ασφαλών κρυπτογραφημένων καναλιών.

Για την παραχώρηση προσβάσεως σε πόρους του Ομίλου, υπάρχει υποδομή ασφαλείας, η οποία να εφαρμόζει τις απαραίτητες δικλείδες ασφαλείας. Οι ακόλουθοι έλεγχοι λαμβάνονται υπόψη για τον έλεγχο της προσβάσεως των συσκευών:

- Επαλήθευση ταυτότητας συσκευής (δηλ. η συσκευή συμπεριλαμβάνεται στο μητρώο των εγκεκριμένων συσκευών)
- Έλεγχος αλλοιώσεως της συσκευής (π.χ. jailbroken, rooted)
- Έλεγχος λειτουργικού συστήματος (δηλ. χρήση εγκεκριμένης εκδόσεως/επιπέδου ενημερώσεων ασφαλείας του λειτουργικού συστήματος)
- Επιβεβαίωση ρυθμίσεων ασφαλείας (π.χ. η πολιτική κωδικών προσβάσεως είναι σύμφωνη με την πολιτική ασφαλείας)
- Έλεγχος εφαρμογών (π.χ. επιτρεπτές εφαρμογές, ελάχιστες απαιτήσεις για τις εφαρμογών)
- Έλεγχος συσκευών (π.χ. απενεργοποίηση κάμερας, απενεργοποίηση WiFi)

Εφαρμόζονται αυτόματοι μηχανισμοί κλειδώματος της οθόνης σε όλες τις συσκευές, οι οποίοι να ενεργοποιούνται μετά την πάροδο μιας προκαθορισμένης περιόδου αδράνειας, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση στη συσκευή.

Οι πληροφορίες του Ομίλου πρέπει να διαχωρίζονται από τις προσωπικές πληροφορίες όταν αποθηκεύονται σε φορητές συσκευές, όπου αυτό είναι εφικτό. Οι εταιρικές πληροφορίες να προστατεύονται μέσω κατάλληλων μηχανισμών (π.χ. χρήση απομονωμένου περιβάλλοντος εκτελέσεως εργασιών - sandboxing, κρυπτογράφηση).

Σε περίπτωση απώλειας φορητών συσκευών διαγράφονται μέσω εξειδικευμένου μηχανισμού ασφαλείας οι πληροφορίες που είναι αποθηκευμένες σε αυτές.

3 ΑΠΟΔΕΚΤΗΣ ΧΡΗΣΗΣ

Οι υπάλληλοι του Ομίλου και οι συνεργάτες του ακολουθούν τους κάτωθι κανόνες ορθής και λελογισμένης χρήσης των πληροφοριακών υποδομών και πληροφοριών:

- Οι υπάλληλοι του Ομίλου δεν επιτρέπεται να εγκαθιστούν προγράμματα λογισμικού πέρα από αυτά που είναι προδιαγεγραμμένα να υπάρχουν σε κάθε υπολογιστική μονάδα ανάλογα με το ρόλο του χρήστη
- Υπεύθυνος για την εγκατάσταση προγραμμάτων λογισμικού είναι ο διαχειριστής των συστημάτων
- Δεν επιτρέπεται το «άνοιγμα» εκτελέσιμων αρχείων από εξωτερικά αποθηκευτικά μέσα που συνδέονται στις υπολογιστικές μονάδες των χρηστών
- Δεν επιτρέπεται το «άνοιγμα» εκτελέσιμων αρχείων που επισυνάπτονται σε email
- Δεν επιτρέπεται η χρήση εφαρμογών (ftp, p2p κ.α.) με τις οποίες δύναται ο χρήστης να μεταφέρει αρχεία από δικτυακούς τόπους στην υπολογιστική του μονάδα εκτός των περιπτώσεων που απαιτείται από τον χαρακτήρα της εργασίας του υπαλλήλου και έχει δοθεί σχετική άδεια από τον Υπεύθυνο Ασφάλειας Πληροφοριών
- Οι χρήστες οφείλουν να συνεργάζονται με τους διαχειριστές συστημάτων προκειμένου να διερευνάται η πηγή και ο τρόπος εγκατάστασης κακόβουλου λογισμικού σε περίπτωση ανίχνευσής του στις υπολογιστικές τους μονάδες
- Οι χρήστες δεν επιτρέπεται να χρησιμοποιούν το λογισμικό που τους παρέχεται για να επιχειρούν πρόσβαση σε πληροφορίες και συστήματα για τα οποία δεν έχουν λάβει την απαραίτητη εξουσιοδότηση
- Οι χρήστες δεν επιτρέπεται να χρησιμοποιούν το λογισμικό που τους παρέχεται για μεταφορά δεδομένων και γενικότερα στοιχείων που αποτελούν περιουσιακό στοιχείο του Ομίλου εκτός των ορίων του Ομίλου και εκτός των συστημάτων του, χωρίς την προηγούμενη έγκριση από τον Προϊστάμενο του τμήματος στο οποίο ανήκουν
- Δεν επιτρέπεται η χρήση των υπολογιστικών μονάδων για πρόσβαση, επεξεργασία και διακίνηση υλικού με ρατσιστικό, πορνογραφικό ή οποιουδήποτε άλλου παράνομου, μη αποδεκτού και επιβλαβούς περιεχομένου
- Οι προσφερόμενες υπηρεσίες και μέσα από τις υποδομές του Ομίλου όπως ηλεκτρονική αλληλογραφία (e-mail), πρόσβαση στο διαδίκτυο, φορητά υπολογιστικά μέσα, κ.λπ. διατίθενται για χρήση στα πλαίσια της εργασίας.
- Οι χρήστες δεν επιτρέπεται να προβαίνουν σε καμία ενέργεια παραβίασης των πολιτικών που καθορίζουν την πρόσβαση σε ιστοχώρους του διαδικτύου και εφαρμόζονται στα συστήματα ασφάλειας του Ομίλου

4 ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΧΡΗΣΤΩΝ

Η λειτουργία του Ομίλου βασίζεται σε πληροφοριακούς πόρους, για καθένα από τους οποίους έχει οριστεί ο Ιδιοκτήτης του, ο οποίος είναι υπεύθυνος για την έγκριση των προσβάσεων σε αυτόν.

Ο Όμιλος λαμβάνει μέτρα ελέγχου φυσικής και λογικής πρόσβασης προκειμένου να αποτρέψει κακόβουλες ή τυχαίες ενέργειες που μπορεί να επηρεάσουν τη διαθεσιμότητά ή να συντελέσουν στη διαρροή ή αλλοίωση ευαίσθητων πληροφοριών.

Η Διεύθυνση Πληροφορικής σχεδιάζει και αναπτύσσει τα απαραίτητα τεχνικά μέσα για τον έλεγχο των λογικών προσβάσεων σε συστήματα και εφαρμογές. Ο βαθμός προστασίας και τα είδη των μέσων ελέγχου πρόσβασης καθορίζονται με βάση την διαβάθμιση των πληροφοριών, σύμφωνα με την ***«Πολιτική Διακίνησης των Πληροφοριών».***

Η πρόσβαση σε συστήματα και εφαρμογές δίνεται με βάση τις αρχές της «Ελάχιστης απόδοσης δικαιωμάτων» και της «Ανάγκης γνώσης». Οι χρήστες έχουν δυνατότητα σύνδεσης μόνο σε συστήματα και εφαρμογές που είναι απαραίτητα για την εκπλήρωση των εργασιών που προβλέπει ο ρόλος τους. Τα δικαιώματα που τους εκχωρούνται επιτρέπουν την πρόσβαση μόνο στις πληροφορίες που λόγω της θέσης τους πρέπει να γνωρίζουν.

Η πρόσβαση σε συστήματα και εφαρμογές γίνεται με προσωπικούς λογαριασμούς. Σε περιπτώσεις συστημάτων που δεν είναι εφικτή η χρήση προσωπικών λογαριασμών, λαμβάνονται επιπρόσθετα τεχνικά μέτρα ώστε να εξασφαλίζεται η δυνατότητα εντοπισμού της ταυτότητας των χρηστών που συνδέονται σε αυτά.

Τα συστήματα και οι εφαρμογές του Ομίλου απαιτούν τη χρήση ισχυρών κωδικών πρόσβασης. Σε όσα δεν υπάρχει η δυνατότητα επιβολής ισχυρού κωδικού έχουν εκδοθεί οδηγίες για δημιουργία ισχυρών κωδικών πρόσβασης από τους ίδιους τους χρήστες.

Οι λογικές προσβάσεις εργαζομένων και συνεργατών στον Όμιλο και τα συστήματά του απενεργοποιούνται αμέσως μετά την λήξη της συνεργασίας. Σε περίπτωση μετακίνησης προσωπικού εντός του Ομίλου μεταβάλλονται άμεσα οι προσβάσεις με βάση τις αρχές που αναφέρονται παραπάνω. Σε τακτά χρονικά διαστήματα γίνεται έλεγχος και επιβεβαίωση όλων των προσβάσεων.

Τα μέτρα ελέγχου της λογικής πρόσβασης ισχύουν για το σύνολο των υπαλλήλων του

Ομίλου και των συνεργατών του. Ειδικότερα οι κανόνες που αφορούν λογικές συνδέσεις σε συστήματα και εφαρμογές ισχύουν είτε αυτές πραγματοποιούνται εντός του Ομίλου είτε από εξωτερικά δίκτυα.

5 ΔΙΑΒΑΘΜΙΣΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΠΟΡΩΝ

Ο Υπεύθυνος Ασφάλειας Πληροφοριών τηρεί κατάλογο ο οποίος περιέχει την καταγραφή των πληροφοριών, των πληροφοριακών και των ιατρικών συστημάτων του Ομίλου. Για κάθε πόρο καταγράφονται στοιχεία όπως:

- Όνομα
- Περιγραφή
- Τοποθεσία εγκατάστασης/αποθήκευσης
- Ιδιοκτήτης
- Διαβάθμιση
- Αξία

Για κάθε πόρο του Ομίλου η Διοίκηση ορίζει τον Ιδιοκτήτη του ο οποίος είναι υπεύθυνος για τη συντήρηση, χρήση και ασφάλεια του πόρου. Οι Ιδιοκτήτες των πόρων είναι υπεύθυνοι για τον καθορισμό του επιπέδου διαβάθμισής τους. Οι Ιδιοκτήτες των πόρων συνεργάζονται με τον Υπεύθυνο Ασφάλειας Πληροφοριών για τον καθορισμό των μέτρων που είναι απαραίτητα για την προστασία τους. Τα μέτρα προστασίας είναι ανάλογα του επιπέδου διαβάθμισης που αποδίδεται σε κάθε πόρο.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών συνεργάζεται με τους Ιδιοκτήτες των πληροφοριών που επεξεργάζεται ο Όμιλος προκειμένου να προσδιορίσει τον κύκλο ζωής τους. Τα στοιχεία τα οποία προσδιορίζονται είναι:

- Ο τρόπος εισαγωγής των πληροφοριών στον Όμιλο
- Ο τρόπος αποθήκευσης των πληροφοριών

- Ο τρόπος επεξεργασίας των πληροφοριών
- Ο τρόπος αποστολής των πληροφοριών εκτός του Ομίλου
- Ο τρόπος διαγραφής/καταστροφής των δεδομένων

Ο Υπεύθυνος Ασφάλειας Πληροφοριών σε συνεργασία με τους Ιδιοκτήτες των πληροφοριών προσδιορίζουν και εφαρμόζουν τα απαιτούμενα μέτρα ασφάλειας προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η διαθεσιμότητα και η ακεραιότητα των πληροφοριών που επεξεργάζεται ο Όμιλος.

Ο Όμιλος εφαρμόζει σύστημα διαβάθμισης των πληροφοριών και των πληροφοριακών πόρων προκειμένου να εφαρμόζει με αποτελεσματικό τρόπο μέτρα Ασφάλειας Πληροφοριών και να διασφαλίζει την ομαλή λειτουργία των επιχειρησιακών του δραστηριοτήτων. Η διαβάθμιση των πληροφοριακών πόρων γίνεται λαμβάνονται υπόψη κριτήρια όπως:

- Η αξία τους
- Η ευαισθησία των πληροφοριών που περιέχουν
- Η κρισιμότητά τους στην εκτέλεση των επιχειρησιακών δραστηριοτήτων του Ομίλου

Η διαβάθμιση των πόρων του Ομίλου γίνεται σε ένα από τα ακόλουθα επίπεδα:

- Δημόσιο
- Εσωτερικής Χρήσης
- Εμπιστευτικό
- Απόρρητο

Το προσωπικό του Ομίλου εφαρμόζει τα κατάλληλα μέτρα προστασίας των πόρων κατά τον χειρισμό τους ανάλογα με το επίπεδο διαβάθμισής του. Τα μέτρα προστασίας σκοπό έχουν τη διασφάλισης της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των πόρων κατά:

- Τη μεταφορά τους
- Την αποθήκευσή τους
- Την επεξεργασία τους
- Την καταστροφή τους

Το προσωπικό του Ομίλου, προβαίνει στη σήμανση των εντύπων και των ηλεκτρονικών μέσων αποθήκευσης τα οποία χρησιμοποιεί κατά την εκτέλεση των καθηκόντων του. Σε περίπτωση που ένα μέσο περιέχει πληροφορίες με διάφορα επίπεδα διαβάθμισης, η σήμανσή του αντιστοιχεί στο αυστηρότερο επίπεδο διαβάθμισης.

6 ΑΠΟΘΗΚΕΥΣΗΣ/ ΚΑΤΑΣΤΡΟΦΗΣ ΦΥΣΙΚΟΥ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΑΡΧΕΙΟΥ

Τα φυσικά και ηλεκτρονικά αρχεία του Ομίλου Ιατρικού Αθηνών αποτελούν αγαθό του Οργανισμού και μπορούν να χρησιμοποιούνται μόνο για την επίτευξη των επιχειρησιακών του στόχων. Η χρήση τους από τους εργαζόμενους του Ομίλου γίνεται σύμφωνα με τα οριζόμενα στις επιμέρους Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών και με τρόπο ώστε να διασφαλίζεται:

- Η συνέχεια των επιχειρησιακών δραστηριοτήτων του Ομίλου
- Η διάθεση υψηλού επιπέδου υπηρεσιών Υγείας
- Η ιδιωτικότητα των προσωπικών στοιχείων των ασθενών των κλινικών του Ομίλου

Ο χειρισμός ηλεκτρονικών πληροφοριών Υγείας γίνεται μέσω των κύριων εφαρμογών του Ομίλου. Η αποθήκευση αρχείων με ευαίσθητα προσωπικά στοιχεία ασθενών σε προσωπικούς υπολογιστές ή σε κοινόχρηστους φακέλους γίνεται μόνο για την εκτέλεση επιχειρησιακών δραστηριοτήτων που δεν μπορούν να υλοποιηθούν μέσω των κύριων εφαρμογών του Ομίλου και μόνο για το χρονικό διάστημα που απαιτείται για την ολοκλήρωση των εν λόγω δραστηριοτήτων.

Η αποθήκευση του φυσικού αρχείου γίνεται με τρόπο ώστε να διασφαλίζεται η πρόσβαση σε αυτό μόνο εξουσιοδοτημένου προσωπικού. Η πρόσβαση στους ειδικούς χώρους φύλαξης φακέλων ασθενών ελέγχεται μέσω κατάλληλων μηχανισμών οι οποίοι εξασφαλίζουν:

- Την πρόσβαση μόνο από εξουσιοδοτημένο προσωπικό
- Την καταγραφή των ενεργειών πρόσβασης
- Την ταυτοποίηση των ατόμων που εισέρχονται στον χώρο φύλαξης του αρχείου

Οι Ιδιοκτήτες πληροφοριών σε ηλεκτρονική ή φυσική μορφή είναι υπεύθυνοι για τον καθορισμό του μέγιστου χρόνου τήρησής τους. Ο χρόνος τήρησης προσδιορίζεται με βάση:

- Τις επιχειρησιακές ανάγκες του Ομίλου
- Την υποχρέωση παροχής κρίσιμων πληροφοριών Υγείας στους ασθενής των κλινικών του Ομίλου
- Την υποχρέωση τήρησης των νομικών και κανονιστικών απαιτήσεων σε σχέση με τη διαχείριση προσωπικών δεδομένων

Οι Ιδιοκτήτες πληροφοριών με βάση τις προκαθορισμένες απαιτήσεις τήρησης πληροφοριών είναι υπεύθυνοι για την δημιουργία αιτημάτων καταστροφής φυσικού αρχείου ή διαγραφής ηλεκτρονικών πληροφοριών από τις βάσεις δεδομένων του Ομίλου.

Αιτήματα καταστροφής φυσικού αρχείου ή διαγραφής ηλεκτρονικών πληροφοριών εξετάζονται από την Επιτροπή Ασφάλειας Πληροφοριών η οποία είναι υπεύθυνη για την έγκριση των αιτημάτων και τον ορισμό του προσφορότερου τρόπου για την υλοποίησή τους.

7 ΧΡΗΣΗΣ ΜΕΘΟΔΩΝ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Ο Όμιλος χρησιμοποιεί εργαλεία κρυπτογραφίας για την προστασία ευαίσθητων δεδομένων από ενέργειες κλοπής, αλλοίωσης ή μη εγκεκριμένης πρόσβασης.

Τα δεδομένα που κρυπτογραφούνται μπορούν να είναι αποθηκευμένα σε πληροφοριακά συστήματα του Ομίλου ή να μεταδίδονται μεταξύ του Ομίλου και συνεργατών του.

Οι Ιδιοκτήτες Πληροφοριών είναι υπεύθυνοι να προσδιορίζουν τη διαβάθμισή τους και να καθορίζουν αν είναι απαραίτητη η κρυπτογράφησή τους.

Η σύνδεση μεταξύ συστημάτων ή χρηστών και συστημάτων πάνω από δημόσια δίκτυα, γίνεται με χρήση συνδέσεων VPN στις οποίες τα δεδομένα κρυπτογραφούνται με τη χρήση ισχυρών μεθόδων κρυπτογράφησης.

Η διαχείριση των συστημάτων του Ομίλου μέσω Command Line Interface, γίνεται μέσω λογισμικού που δημιουργεί κρυπτογραφημένα κανάλια επικοινωνίας (Secure Shell).

Για τη διαχείριση των κωδικών πρόσβασης συστημάτων και εφαρμογών, χρησιμοποιείται εξειδικευμένο λογισμικό το οποίο παρέχει τη δυνατότητα ηλεκτρονικής αποθήκευσής τους σε κρυπτογραφημένη μορφή.

Το προσωπικό κρυπτογραφεί τα αρχεία με εμπιστευτικές πληροφορίες τα οποία διακινούνται με email μέσω του Ομίλου και των συνεργατών του. Εναλλακτικά, εμπιστευτικές πληροφορίες

μεταφέρονται μέσω κρυπτογραφημένων καναλιών επικοινωνίας (π.χ. HTTPS, SFTP, IPSEC VPN Tunnels).

Για τη διαχείριση των κρυπτογραφικών κλειδιών και των ψηφιακών πιστοποιητικών που χρησιμοποιούνται στον Όμιλο εφαρμόζονται οι ακόλουθες αρχές:

- Σε περίπτωση διανομής κρυπτογραφικών κλειδιών μέσω USB, διαγράφονται από το φορητό μέσο αποθήκευσης αμέσως μετά την εγκατάστασή τους.
- Τα αρχεία των κρυπτογραφικών κλειδιών κρυπτογραφούνται όταν διακινούνται μέσω email
- Σε περίπτωση αποχώρησης υπαλλήλων, αναιρούνται άμεσα τα κρυπτογραφικά κλειδιά που τους έχουν παραδοθεί κατά το διάστημα εργασίας τους

Όταν υπάρχει ανάγκη τήρησης αντιγράφων αρχείων κρυπτογραφικών κλειδιών, αυτά τηρούνται αποθηκευμένα σε κρυπτογραφημένη μορφή και σε χώρο προσβάσιμο μόνο από εξουσιοδοτημένο προσωπικό.

8 ΠΟΛΙΤΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Σε περίπτωση περιστατικού Ασφάλειας Πληροφοριών, ο Υπεύθυνος Ασφάλειας Πληροφοριών είναι αρμόδιος για τον συντονισμό όλων των απαραίτητων ενεργειών για την αντιμετώπισή του. Περαιτέρω, σε περίπτωση όπου ένα περιστατικό Ασφάλειας Πληροφοριών αποτελεί ταυτόχρονα και περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα, ο Υπεύθυνος Ασφάλειας Πληροφοριών συνεργάζεται με τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων (Data Protection Officer – DPO). Σε κάθε περίπτωση εξασφαλίζεται η ανεύρεση των απαραίτητων πόρων για τον περιορισμό των ζημιών και τον προσδιορισμό των αιτιών του περιστατικού Ασφάλειας Πληροφοριών. Εφαρμόζεται διαδικασία αντιμετώπισης (***Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας Πληροφοριών***) ώστε να διασφαλίζεται ότι τα συμβάντα και τα περιστατικά Ασφάλειας Πληροφοριών ανιχνεύονται, καταγράφονται, επιλύονται και αναφέρονται στη Διοίκηση και στις αρμόδιες αρχές.

Στα πλαίσια της διαδικασίας Αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριών εκτελούνται ενέργειες:

- Προσδιορισμού των αιτιών εμφάνισης του περιστατικού Ασφάλειας Πληροφοριών
- Σχεδιασμού και εφαρμογής μέτρων προστασίας προκειμένου να αποτραπεί η επανάληψη του περιστατικού ασφάλειας
- Συλλογής αποδεικτικών στοιχείων
- Επικοινωνίας με όσους έχουν επηρεασθεί από το περιστατικό ασφάλειας ή με όσους έχουν εμπλακεί στην αποκατάσταση της κανονικής λειτουργίας του Ομίλου
- Υποβολής εκθέσεων στις αρμόδιες αρχές σχετικά με τις ενέργειες που πραγματοποιήθηκαν ή/ και άλλες απαιτούμενες πληροφορίες

Τα στοιχεία που συλλέγονται κατά τη διερεύνηση περιστατικών Ασφάλειας Πληροφοριών χρησιμοποιούνται για:

- Την ανάλυση / επίλυση προβλημάτων που εμφανίζονται εσωτερικά στον Όμιλο
- Την βελτίωση της παραμετροποίησης των συστημάτων Ασφάλειας για την ανίχνευση εισβολών
- Αποδεικτικά στοιχεία στις περιπτώσεις εκδίκασης υπόθεσης που σχετίζεται με την εμφάνιση του περιστατικού Ασφάλειας Πληροφοριών

9 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΟΥΣ ΑΝΑΠΤΥΞΗΣ ΣΥΣΤΗΜΑΤΩΝ

Κατά το στάδιο σχεδιασμού νέων συστημάτων ή εφαρμογών προδιαγράφονται οι απαιτήσεις Ασφάλειας Πληροφοριακών Συστημάτων. Η Διεύθυνση Ασφάλειας Πληροφοριών σε συνεργασία με αρμόδια τμήματα της Διεύθυνσης Πληροφορικής προσδιορίζουν και καταγράφουν τις απαιτήσεις ασφάλειας των νέων συστημάτων και εφαρμογών.

Η ανάπτυξη και οι δοκιμές συστημάτων και εφαρμογών υλοποιούνται σε ξεχωριστό περιβάλλον το οποίο είναι απομονωμένο από το περιβάλλον παραγωγής, εξασφαλίζοντας με αυτό τον τρόπο την προστασία των επιχειρησιακών λειτουργιών του Ομίλου.

Κατά την ανάπτυξη νέων συστημάτων ακολουθούνται οι κάτωθι ενέργειες:

- Προσδιορίζονται οι πληροφορίες που το σύστημα θα διαχειρίζεται και καθορίζονται οι απαιτήσεις ασφάλειας κατά την αποθήκευση ή τη μετάδοσή τους
- Προσδιορίζονται οι ανάγκες πρόσβασης και καθορίζονται οι μηχανισμοί αυθεντικοποίησης των χρηστών
- Ορίζεται ο χώρος φυσικής εγκατάστασης του συστήματος και προσδιορίζονται τα απαραίτητα μέτρα προστασίας του
- Καθορίζεται η λογική συνδεσμολογία του συστήματος. Προσδιορίζεται αν απαιτείται η υλοποίηση πρόσθετων μηχανισμών περιορισμού και ελέγχου της λογικής πρόσβασης
- Αναλύονται οι καταγραφές που παράγει και προσδιορίζεται ο τρόπος ασφαλούς αποθήκευσής τους
- Προσδιορίζονται οι ανάγκες λήψης αντιγράφων ασφαλείας.

Κατά την ανάπτυξη νέων συστημάτων στο δίκτυο του Ομίλου ακολουθούνται ενέργειες που σκοπό έχουν τον περιορισμό του κινδύνου εμφάνισης περιστατικών Ασφάλειας Πληροφοριών. Για το λόγο αυτό τροποποιούνται οι αρχικές ρυθμίσεις τους πριν εγκατασταθούν στο παραγωγικό περιβάλλον.

10 ΠΟΛΙΤΙΚΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΕΦΑΡΜΟΓΩΝ

Για τη διασφάλιση των επιχειρησιακών λειτουργιών του Ομίλου Ιατρικού χρησιμοποιούνται εξειδικευμένα προγράμματα λογισμικού για την παρακολούθηση της λειτουργίας των πληροφοριακών συστημάτων και εφαρμογών. Ο έγκαιρος εντοπισμός γεγονότων που μπορεί να οδηγήσουν σε εμφάνιση δυσλειτουργιών ή περιστατικών Ασφάλειας Πληροφοριών, έχει αποφασιστική σημασία για την αποτελεσματική αντιμετώπισή τους και τη διασφάλιση της συνέχειας των υπηρεσιών Υγείας που προσφέρουν οι κλινικές του Ομίλου.

Η παρακολούθηση των συστημάτων και εφαρμογών βασίζεται στους εξής άξονες:

- Παρακολούθηση της χωρητικότητας των συστημάτων
- Έλεγχος των καταγραφών που παράγουν πληροφοριακά και δικτυακά συστήματα
- Έλεγχος των καταγραφών που παράγουν εξειδικευμένα συστήματα Ασφάλειας Πληροφοριών

Το επίπεδο χρήσης των πληροφοριακών συστημάτων προσδιορίζεται μέσω της παρακολούθησης παραμέτρων όπως:

- Χρήση της CPU
- Χρήση της μνήμης
- Διαθέσιμος χώρος σε μέσα αποθήκευσης δεδομένων

- Χρήση των γραμμών επικοινωνίας

Μέσω των παρατηρούμενων τιμών είναι δυνατός ο προσδιορισμός:

- Ασυνήθιστων τιμών που πιθανόν σχετίζονται με δυσλειτουργίες συστημάτων
- Αναγκών αναβάθμισης των συστημάτων

Μέσω των συστημάτων παρακολούθησης παράγονται ενημερώσεις σε περιπτώσεις υπέρβασης των προκαθορισμένων ορίων, έτσι ώστε να είναι δυνατή η έγκαιρη απόκριση του εξουσιοδοτημένου προσωπικού.

Τα πληροφοριακά συστήματα, οι εφαρμογές και οι δικτυακές συσκευές είναι παραμετροποιημένες ώστε να παράγουν καταγραφές οι οποίες χρησιμοποιούνται από τη Διεύθυνση Ασφάλειας Πληροφοριών κατά την αντιμετώπιση περιστατικών Ασφάλειας και από τους διαχειριστές των συστημάτων κατά τη διερεύνηση θεμάτων απόδοσης και επίλυσης προβλημάτων λειτουργίας. Οι συγκεκριμένες καταγραφές αφορούν:

- Προσπάθειες συνδέσεων χρηστών
- Ενέργειες παραμετροποίησης
- Ενέργειες διαχείρισης πληροφοριών

Οι παραγόμενες καταγραφές αφορούν ενέργειες απλών χρηστών αλλά και των διαχειριστών των συστημάτων.

Τα εξειδικευμένα συστήματα Ασφάλειας Πληροφοριών παράγουν καταγραφές μέσω των οποίων είναι δυνατόν:

- Να εντοπίζονται απόπειρες μη εξουσιοδοτημένων προσβάσεων
- Να ανιχνεύονται ύποπτες δραστηριότητες που πιθανόν σχετίζονται με προσπάθειες παραβίασης της Ασφάλειας Πληροφοριών
- Να ταυτοποιούνται ενέργειες σύνδεσης χρηστών σε συστήματα ή εφαρμογές

Η Διεύθυνση Ασφάλειας Πληροφοριών πραγματοποιεί σε τακτική βάση ελέγχους στις καταγραφές των πληροφοριακών συστημάτων και των συστημάτων Ασφάλειας προκειμένου να ανιχνεύει ενέργειες που πιθανόν σχετίζονται με συμβάντα Ασφάλειας Πληροφοριών.

Προκειμένου να είναι εφικτή η διερεύνηση ιστορικών στοιχείων κατά την διαχείριση περιστατικών Ασφάλειας Πληροφοριών λαμβάνονται αντίγραφα των αρχείων καταγραφής τα οποία είναι προσβάσιμα μόνο από εξουσιοδοτημένο προσωπικό.

11 ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Προκειμένου να διασφαλίζεται η απρόσκοπτη λειτουργία των πληροφοριακών συστημάτων του Ομίλου λαμβάνονται οργανωτικά και τεχνικά μέτρα που σκοπό έχουν την προστασία τους από κακόβουλα προγράμματα λογισμικού που είναι δυνατόν να επηρεάσουν τη λειτουργίας τους.

Το σύνολο των υπολογιστικών μονάδων των χρηστών και των διακομιστών του Ομίλου προστατεύονται από αντιϊκό λογισμικό. Η πρόσβαση στο διαδίκτυο ελέγχεται μέσω εξειδικευμένου εξοπλισμού Firewall. Σε αυτόν εφαρμόζονται πολιτικές ελέγχου και περιορισμού της πρόσβασης σε ιστοχώρους που ενέχουν υψηλό κίνδυνο μόλυνσης με κακόβουλο λογισμικό.

Το λογισμικό που επιτρέπεται να εγκαθίσταται σε υπολογιστικές μονάδες χρηστών και στους διακομιστές του Ομίλου είναι καταγεγραμμένο και παρακολουθείται μέσω εξειδικευμένων προγραμμάτων. Ανά τακτά χρονικά διαστήματα δημιουργούνται αναφορές εγκατεστημένου λογισμικού οι οποίες ελέγχονται αν περιέχουν μη επιτρεπτά προγράμματα.

Στις υπολογιστικές μονάδες οι χρήστες δεν έχουν δικαιώματα διαχειριστή και η εγκατάσταση λογισμικού γίνεται μόνο από εργαζόμενους της Διεύθυνσης Πληροφορικής.

12 ΛΗΨΗΣ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ

Η λήψη αντιγράφων ασφαλείας είναι πρωταρχικής σημασίας για τη λειτουργία του Ομίλου γιατί διασφαλίζει τη διαθεσιμότητα και ακεραιότητα κρίσιμων πληροφοριών και εξασφαλίζει την ταχεία επαναφορά των επιχειρησιακών λειτουργιών του σε περίπτωση καταστροφής. Για τη λήψη των αντιγράφων ασφαλείας χρησιμοποιείται εξειδικευμένο πληροφοριακό σύστημα.

Οι Ιδιοκτήτες των πληροφοριών και των πληροφοριακών συστημάτων καθορίζουν τις ανάγκες λήψης αντιγράφων ασφαλείας. Η συχνότητα λήψης αντιγράφων ασφαλείας καθορίζεται με βάση τις απαιτήσεις του σημείου ανάκαμψης των υποστηριζόμενων επιχειρησιακών λειτουργιών.

Η φύλαξη των αντιγράφων ασφαλείας γίνεται τοπικά στον ίδιο χώρο που φιλοξενείται το πληροφοριακό σύστημα από το οποίο λαμβάνεται το αντίγραφο και σε απομακρυσμένη τοποθεσία. Στην πρώτη περίπτωση, τα αντίγραφα ασφαλείας χρησιμοποιούνται για την άμεση αποκατάσταση της λειτουργίας συστημάτων σε περίπτωση εμφάνισης δυσλειτουργιών σε αυτά. Η φύλαξη αντιγράφων ασφαλείας σε απομακρυσμένα σημεία εγγυάται την αποκατάσταση των επιχειρησιακών λειτουργειών του Ομίλου σε περίπτωση εμφάνισης σοβαρού καταστροφικού γεγονότος σε χώρους φιλοξενίας πληροφοριακών συστημάτων.

Ιδιαίτερα μέτρα λαμβάνονται για την προστασία των αντιγράφων ασφαλείας που φιλοξενούνται σε χώρους οι οποίοι δεν βρίσκονται υπό την εποπτεία του Ομίλου, όπως:

- Κρυπτογράφηση των αντιγράφων ασφαλείας που αποθηκεύονται σε φορητά μέσα αποθήκευσης (σκληροί δίσκοι, tapes)
- Φύλαξη φορητών μέσων αποθήκευσης σε χώρους που ασφαλίζουν και προσφέρουν προστασία από πυρκαγιά
- Κρυπτογράφηση του σκληρού δίσκου ή της βάσης δεδομένων των πληροφοριακών συστημάτων που χρησιμοποιούνται για τη λήψη και φύλαξη αντιγράφων ασφαλείας

Προκειμένου να διαπιστώνεται η ορθή λειτουργία των μηχανισμών λήψης αντιγράφων ασφαλείας, πραγματοποιούνται σε τακτική βάση δοκιμές επαναφοράς δεδομένων. Κατά την πραγματοποίηση των δοκιμών ελέγχονται τα ακόλουθα σημεία:

- Η ακεραιότητα των πληροφοριών που περιέχονται στα αντίγραφα ασφαλείας
- Ο χρόνος που απαιτείται για την επαναφορά τους

Η επαναφορά δεδομένων υλοποιείται σε συστήματα τα οποία προστατεύονται με τους ίδιους μηχανισμούς Ασφάλειας που προστατεύουν τα παραγωγικά συστήματα προκειμένου να ελαχιστοποιείται ο κίνδυνος εμφάνισης περιστατικών διαρροής πληροφοριών. Επιπρόσθετα, μετά το πέρας των δοκιμών τα δεδομένα διαγράφονται ασφαλώς από τα συστήματα δοκιμών.

13 ΕΝΤΟΠΙΣΜΟΥ ΑΔΥΝΑΜΙΩΝ ΚΑΙ ΔΙΕΞΑΓΩΓΗΣ ΕΛΕΓΧΩΝ ΑΣΦΑΛΕΙΑΣ

Η ανάγκη ελαχιστοποίησης του κινδύνου εμφάνισης περιστατικών μη εξουσιοδοτημένων προσβάσεων ή μόλυνσης με κακόβουλο λογισμικό καθιστά επιτακτική την ανάγκη συστηματικής εγκατάστασης των ενημερώσεων λογισμικού που εκδίδουν οι κατασκευαστές πληροφοριακών συστημάτων και υποδομών. Με τον τρόπο αυτό αντιμετωπίζονται οι ευπάθειες που μπορούν να εκμεταλλευτούν κακόβουλοι χρήστες για να αποκτήσουν πρόσβαση στις υποδομές του Ομίλου και να προκαλέσουν προβλήματα στην ομαλή επιχειρησιακή του λειτουργία.

Τα αρμόδια τμήματα της Διεύθυνσης Πληροφορικής τηρούν κατάλογο με τα πληροφοριακά συστήματα και εφαρμογές του Ομίλου στον οποίο καταγράφονται μεταξύ άλλων πληροφορίες σε σχέση με τους κατασκευαστές τους και τις τρέχουσες εγκατεστημένες εκδόσεις λογισμικού. Ο εντοπισμός ευπαθειών επιτυγχάνεται μέσω:

- Των ενημερώσεων που ανακοινώνουν οι κατασκευαστές συστημάτων και λογισμικού
- Των τεχνικών ελέγχων που διενεργούνται σε συστήματα και προγράμματα λογισμικού

Η εγκατάσταση των ενημερώσεων σε συστήματα διακομιστών υλοποιείται ακολουθώντας

τις εξής αρχές:

- Οι ενημερώσεις ασφάλειας εγκαθίστανται με προτεραιότητα το συντομότερο δυνατό μετά την ανακοίνωσή τους από τους κατασκευαστές των συστημάτων
- Οι ενημερώσεις λογισμικού εγκαθίστανται σε παραγωγικό περιβάλλον αφού πρώτα αξιολογηθούν σε δοκιμαστικό περιβάλλον και διαπιστωθεί ότι δεν προκαλούν την εμφάνιση δυσλειτουργιών σε συστήματα και εφαρμογές
- Για την εγκατάσταση των ενημερώσεων σε παραγωγικό περιβάλλον ακολουθείται διαδικασία υλοποίησης αλλαγών

Η διαχείριση των ενημερώσεων υπολογιστικών μονάδων χρηστών υλοποιείται μέσω κεντρικού συστήματος το οποίο εγκαθιστά με αυτοματοποιημένο τρόπο τις τελευταίες ενημερώσεις που εκδίδει ο κατασκευαστής του λειτουργικού συστήματος.

Σε περίπτωση αδυναμίας εγκαταστάσεων ενημερώσεων λογισμικού λαμβάνονται πρόσθετα μέτρα Ασφάλειας προκειμένου να περιοριστεί ο κίνδυνος εκμετάλλευσης των ευπαθειών, όπως:

- Απομόνωση του συστήματος σε ξεχωριστή δικτυακή ζώνη και έλεγχος των προσβάσεων σε αυτό
- Απενεργοποίηση υπηρεσιών που σχετίζονται με τις ευπάθειες
- Αύξηση του επιπέδου παρακολούθησης του συστήματος προκειμένου να εντοπίζονται έγκαιρα προσπάθειες εκμετάλλευσης των ευπαθειών

Για τον εντοπισμό ευπαθειών και αδυναμιών σε συστήματα και εφαρμογές του Ομίλου διεξάγονται έλεγχοι:

- Ύπαρξης ευπαθειών (vulnerability scans)
- Παρείσδυσης (penetration test)

Οι τεχνικοί έλεγχοι διεξάγονται σε περιοδική βάση και όποτε:

- Υπάρχει σημαντική αλλαγή στην αρχιτεκτονική του δικτύου
- Εγκαθίσταται νέα εφαρμογή στο παραγωγικό περιβάλλον

Τα αποτελέσματα των τεχνικών ελέγχων αξιολογούνται και αντιμετωπίζονται κατά προτεραιότητα οι ευπάθειες και αδυναμίες που ενέχουν αυξημένο κίνδυνο να οδηγήσουν στην εμφάνιση περιστατικών:

- Διακοπής των επιχειρησιακών λειτουργιών του Ομίλου
- Παραβίασης της πρόσβασης σε δεδομένα Υγείας ή σε άλλες εμπιστευτικές ή απόρρητες πληροφορίες

14 ΦΥΣΙΚΗΣ ΚΑΙ ΠΕΡΙΒΑΛΛΟΝΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Ο Όμιλος Ιατρικού Αθηνών εφαρμόζει μέτρα Φυσικής και Περιβαλλοντικής Ασφάλειας προκειμένου να διασφαλίζει ότι:

- Προστατεύονται οι κτηριακές εγκαταστάσεις και το προσωπικό που στεγάζεται σε αυτές από κινδύνους που μπορούν να προέλθουν από ακραία φυσική φαινόμενα ή επιθέσεις εγκληματικών στοιχείων
- Μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε χώρους που στεγάζει πληροφοριακά συστήματα και φυσικό αρχείο με ευαίσθητα δεδομένα υγείας
- Μόνο εξουσιοδοτημένο Ιατρικό προσωπικό έχει πρόσβαση σε χώρους παροχής υπηρεσιών υγείας για τους οποίους απαιτούνται αυξημένα μέτρα φύλαξης
- Παρακολουθούνται οι περιβαλλοντικές συνθήκες λειτουργίας των πληροφοριακών συστημάτων και αντιμετωπίζονται άμεσα και αποτελεσματικά γεγονότα που ενδέχεται να οδηγήσουν σε αποσταθεροποίησή τους
- Διακινείται με ασφαλή μέθοδο ο πληροφοριακός και ιατρικός εξοπλισμός από και προς τις εγκαταστάσεις του Ομίλου

Προκειμένου να προστατεύονται επαρκώς οι κρίσιμοι πόροι του Ομίλου, εφαρμόζονται μέτρα σε πολλαπλά επίπεδα (Άμυνα σε Βάθος) μέσω των οποίων επιτυγχάνεται ο έλεγχος της:

- Περιμέτρου των εγκαταστάσεων
- Πρόσβασης της εισόδου σε αυτές
- Πρόσβασης σε Ασφαλείς Περιοχές

Ως Ασφαλείς περιοχές ορίζονται οι χώροι:

- Φιλοξενίας πληροφοριακών συστημάτων
- Τήρησης φυσικού αρχείου με Ιατρικούς φακέλους
- Παροχής ιατρικών υπηρεσιών για τους οποίους απαιτούνται αυξημένα μέτρα φύλαξης
- Φιλοξενίας των γραφείων της Διοίκησης του Ομίλου

Η διασφάλιση της ομαλής λειτουργίας των πληροφοριακών συστημάτων εξαρτάται σε μεγάλο βαθμό από τα υποστηρικτικά δίκτυα στα οποία βασίζονται. Εξειδικευμένα συστήματα παρακολουθούν σε συνεχή βάση τη λειτουργία των υποστηρικτικών συστημάτων και παράγουν αναφορές όταν υπάρχουν αποκλίσεις από τις προκαθορισμένες τιμές που προσδιορίζουν τις βέλτιστες συνθήκες λειτουργίας. Τα επιμέρους συστήματα του υποστηρικτικού εξοπλισμού συντηρούνται σύμφωνα με το πρόγραμμα των κατασκευαστών τους, ενώ πραγματοποιούνται τακτικοί έλεγχοι για την εξακρίβωση της ορθής λειτουργίας τους.

15 ΚΑΘΑΡΟΥ ΓΡΑΦΕΙΟΥ – ΚΑΘΑΡΗΣ ΟΘΟΝΗΣ

Οι εργαζόμενοι εφαρμόζουν πολιτική καθαρού γραφείου – καθαρής οθόνης σύμφωνα με την οποία:

- Οι οθόνες των χρηστών δεν είναι ορατές από τρίτους και οι χρήστες δεν πρέπει να εισάγουν συνθηματικά ενώ παρακολουθούνται από τρίτους
- Οι υπολογιστές κλειδώνουν αυτόματα μετά τη παρέλευση 15 λεπτών
- Οι χρήστες αποσυνδέονται από τα συστήματα και να τακτοποιούν τα γραφεία τους όποτε απομακρύνονται από το χώρο εργασίας τους
- Οι χρήστες δεν καταγράφουν ευαίσθητη πληροφορία σε χαρτιά ή άλλα μέσα αποθήκευσης τα οποία βρίσκονται εκτεθειμένα πάνω στο γραφεία τους. Μετά τη λήξη της εργασίας, όλα τα έντυπα τακτοποιούνται και κλειδώνονται ασφαλώς, σύμφωνα με την κατηγορία διαβάθμισής τους
- Όλα τα έντυπα απομακρύνονται από τους εκτυπωτές, τα φαξ και τα φωτοαντιγραφικά μηχανήματα.

16 ΔΙΑΣΥΝΔΕΣΗΣ ΜΕ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥΣ ΣΥΝΕΡΓΑΤΕΣ

Ο Όμιλος Ιατρικού Αθηνών στα πλαίσια της λειτουργίας του συνδέεται με δίκτυα συνεργατών του για λόγους που μπορεί να σχετίζονται με:

- Τις επιχειρηματικές δραστηριότητες του Ομίλου
- Την ανάγκη υποστήριξης πληροφοριακών συστημάτων
- Την ανάγκη υποστήριξης Ιατρικών συστημάτων

Μέσω των διασυνδέσεων ανταλλάσσονται πληροφορίες που σχετίζονται με:

- Τις υπηρεσίες που προσφέρει ο Όμιλος
- Τη λειτουργία πληροφοριακών συστημάτων ή Ιατρικού εξοπλισμού

Η διασύνδεση του Ομίλου με τους συνεργάτες του υλοποιείται μέσω μόνιμων συνδέσεων ή προσωρινών συνδέσεων κατά τις οποίες αυθεντικοποιούνται οι χρήστες και παραμένουν ενεργές για όσο χρόνο απαιτείται για την ολοκλήρωση συγκεκριμένων ενεργειών. Οι μόνιμες συνδέσεις υλοποιούνται μέσω μισθωμένων γραμμών ή μέσω του Διαδικτύου. Σε όλες τις περιπτώσεις η επικοινωνία γίνεται μέσω κρυπτογραφημένων καναλιών ώστε να διασφαλίζεται η εμπιστευτικότητα των διακινούμενων πληροφοριών. Τα κανάλια επικοινωνίας (μόνιμα ή προσωρινά) καταλήγουν σε εξειδικευμένο εξοπλισμό μέσω του οποίου εφαρμόζονται πολιτικές περιορισμού της πρόσβασης σε συστήματα για τα οποία έχουν τη σχετική εξουσιοδότηση οι συνεργάτες.

Κάθε αίτημα διασύνδεσης με συνεργάτη αξιολογείται από τη Διεύθυνση Ασφάλειας Πληροφοριών η οποία καθορίζει αν απαιτούνται πρόσθετοι μηχανισμοί Ασφάλειας. Σε περιπτώσεις σύνδεσης συνεργατών σε συστήματα με ευαίσθητα στοιχεία είναι δυνατόν να εφαρμόζονται τεχνικά μέτρα μέσω των οποίων καταγράφονται επακριβώς οι ενέργειές τους.

Στις συμβάσεις με τους συνεργάτες του Ομίλου περιγράφεται ο τρόπος διασύνδεσης των δύο μερών, τα συστήματα στα οποία έχουν δικαίωμα πρόσβασης καθώς και το είδος και η μορφή των πληροφοριών που διακινούνται. Επιπρόσθετα, προσδιορίζονται τα μέτρα Ασφάλειας που λαμβάνει κάθε μέρος κατά την αποθήκευση των πληροφοριών στις εγκαταστάσεις του καθώς οι υποχρεώσεις του ως προς τη διαγραφή τους.

Ο Όμιλος Ιατρικού Αθηνών γνωστοποιεί την Πολιτική Ασφάλειας Πληροφοριών στους συνεργάτες του και τους ενημερώνει για τη διαδικασία που θα πρέπει να ακολουθούν σε περίπτωση εντοπισμού γεγονότων που ενδέχεται να οδηγήσουν σε παραβίαση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των πληροφοριών που διακινείται μεταξύ των δύο μερών.

17 ΕΠΙΛΟΓΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΣΥΝΕΡΓΑΣΙΩΝ ΜΕ ΤΡΙΤΟΥΣ

Ο Όμιλος στα πλαίσια της συνεργασίας του με προμηθευτές ή εξωτερικούς συνεργάτες είναι δυνατόν να επιτρέπει την πρόσβαση στις υποδομές του. Ο Όμιλος υλοποιεί τα αναγκαία μέτρα ελέγχου πρόσβασης και αποτροπής ενεργειών που μπορεί να επηρεάσουν τη λειτουργία της πληροφοριακής του υποδομής ή να συντελέσουν στη διαρροή ή αλλοίωση πληροφοριών.

Κατά τη σύναψη νέων συνεργασιών, καθορίζονται τα κριτήρια ή άλλες απαιτήσεις ασφάλειας πληροφοριών που πρέπει να ληφθούν υπόψη κατά την αξιολόγηση των υποψήφιων προμηθευτών/ συνεργατών. Ενδεικτικά κριτήρια/ απαιτήσεις αφορούν τα ακόλουθα:

- Εφαρμογή πιστοποιημένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών που καλύπτει τις σχετικές με το αντικείμενο των υπηρεσιών δραστηριότητες. Εναλλακτικά, ύπαρξη διαδικασιών και πολιτικών ασφάλειας οι οποίες εφαρμόζονται από τον προμηθευτή, καθώς και αποδεικτικά στοιχεία εφαρμογής τους. Σε κάθε περίπτωση θα πρέπει να καλύπτονται θέματα διαχείρισης των περιστατικών ασφάλειας (information security incident management).
- Χρήση από τον προμηθευτή όρων εμπιστευτικότητας/ εχεμύθειας στις συμβάσεις εργασίας με το προσωπικό του ή υπογραφή ξεχωριστού Non-disclosure agreement (NDA).
- Σε περίπτωση που ο προμηθευτής κάνει χρήση υπηρεσιών cloud, έχει επιλέξει πιστοποιημένο πάροχο ως προς την ασφάλεια των πληροφοριών
- Χρήση κρυπτογραφημένων καναλιών για την επικοινωνία ευαίσθητων πληροφοριών (όπου απαιτείται)
- Προσωπικό πιστοποιημένο σε τεχνολογίες και πρακτικές ασφάλειας πληροφοριών
- Ειδικότερες τεχνικές απαιτήσεις για προμηθευτές/ συνεργάτες που αναπτύσσουν λογισμικό για λογαριασμό του Ομίλου, όπως:
  - Χρήση διαφορετικών περιβαλλόντων για την ανάπτυξη και τον έλεγχο λογισμικού
  - Εφαρμογή μηχανισμών ελέγχου των εκδόσεων λογισμικού (version control)
  - Ενσωμάτωση ελέγχων ασφάλειας στον κύκλο ζωής της ανάπτυξης λογισμικού (source code review, vulnerability assessments, web application penetration testing κ.λπ.) ο Χρήση εναλλακτικών υποδομών για τις εφαρμογές και τα δεδομένα σε περίπτωση καταστροφικού συμβάντος (Disaster Recovery Site)

Επιπλέον, στο πλαίσιο της σύναψης μιας νέας συνεργασίας με προμηθευτή/ συνεργάτη, προσδιορίζονται οι ανάγκες πρόσβασης σε πληροφορίες και υποδομές του Ομίλου. Η Διεύθυνση Ασφάλειας Πληροφοριών, σε συνεργασία με τη Διεύθυνση Πληροφορικής, σχεδιάζουν και υλοποιούν τα κατάλληλα μέτρα ελέγχου της πρόσβασης και των ενεργειών που επιτρέπεται να εκτελεί ο συνεργάτης. Οι συνεργάτες του Ομίλου υπογράφουν συμφωνίες εμπιστευτικότητας και μη αποκάλυψης ευαίσθητων ή/ και κρίσιμων δεδομένων. Στα συμβόλαια συνεργασίας, μεταξύ άλλων, αναγνωρίζονται και καταγράφονται οι επιτρεπτές προσβάσεις των συνεργατών σε υποδομές και πληροφορίες του Ομίλου.

Το προσωπικό των προμηθευτών, αλλά και οι συνεργάτες/ υπεργολάβοι αυτών, είναι υποχρεωμένοι να τηρούν τους κανόνες Ασφάλειας Πληροφοριών του Ομίλου.

Ο Όμιλος ενημερώνει και εκπαιδεύει τους συνεργάτες του σε θέματα της Πολιτικής Ασφάλειας Πληροφοριών, καθώς και στη χρήση των μηχανισμών πρόσβασης στις υποδομές του. Οι συνεργάτες του Ομίλου οφείλουν να ενημερώνουν άμεσα τη Διεύθυνση Ασφάλειας Πληροφοριών,

σε περίπτωση που εργαζόμενός τους προβεί σε ενέργειες που αντιβαίνουν στην Πολιτική Ασφάλειας του Ομίλου ή στους όρους Ασφάλειας Πληροφοριών που περιγράφονται στη σύμβαση συνεργασίας.

Οι συμβάσεις με τους συνεργάτες του Ομίλου αναθεωρούνται είτε μετά από απόφαση της Διοίκησης του Ομίλου με βάση την αξιολόγηση ενός συνεργάτη, είτε σε κάποια από τις ακόλουθες περιπτώσεις:

- Ανάγκη επαναπροσδιορισμού των εμπορικών όρων
- Αλλαγές στις υποδομές και στην οργάνωση του Ομίλου ή των προμηθευτών
- Τροποποιημένες απαιτήσεις ασφάλειας λόγω αλλαγών στους κινδύνους (εμφάνιση νέων, αύξηση κρισιμότητας υφιστάμενων κ.λπ.)
- Εμφάνιση κρίσιμων περιστατικών ασφάλειας που επηρεάζουν σημαντικά τις λειτουργίες του προμηθευτή
- Αλλαγές στις προσφερόμενες υπηρεσίες από τους προμηθευτές.

18 ΔΙΑΚΙΝΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Οι πληροφορίες που μεταφέρονται προς και από τον Όμιλο προστατεύονται με κατάλληλα μέτρα που διασφαλίζουν την εμπιστευτικότητα, ακεραιότητα και αυθεντικότητά τους.

Τα μέτρα που λαμβάνονται για την προστασία των πληροφοριών εξαρτώνται από τη διαβάθμισή τους. Οι «Ιδιοκτήτες Πληροφοριών» είναι υπεύθυνοι κατά τον προσδιορισμό του κύκλου ζωής τους, να ορίσουν τις συνθήκες κάτω από τις οποίες απαιτείται η μεταφορά τους, να καθορίσουν τον τρόπο και τα μέσα που θα χρησιμοποιούνται για την μεταφορά τους και να προδιαγράψουν τα απαραίτητα μέτρα προστασίας τους.

Η μεταφορά πληροφοριών μεταξύ συστημάτων ή μεταξύ χρηστών και συστημάτων, πάνω από δημόσια δίκτυα, γίνεται μέσω προστατευμένων καναλιών επικοινωνίας.

Στις συμφωνίες συνεργασίας με άλλες εταιρείες οι οποίες περιλαμβάνουν ενέργειες μεταφοράς πληροφοριών, ορίζονται και περιγράφονται όροι σχετικοί με την ασφάλεια των μεταφερόμενων πληροφοριών. Πιο συγκεκριμένα:

- Δίνεται περιγραφή των μεταφερόμενων πληροφοριών
- Περιγράφεται ο τρόπος μεταφοράς των δεδομένων και των μέτρων προστασίας που λαμβάνονται
- Προδιαγράφονται στοιχεία σχετικά με την επεξεργασία των δεδομένων (τρόπος αποθήκευσης, χρόνος τήρησης, τρόπος διαγραφής τους)

Ο Όμιλος, προκειμένου να προστατέψει την εμπιστευτικότητα των πληροφοριών που επεξεργάζεται, συνάπτει συμβάσεις με τους υπαλλήλους και τους συνεργάτες του οι οποίες περιλαμβάνουν όρους εμπιστευτικότητας και μη αποκάλυψης. Οι συγκεκριμένοι όροι προσδιορίζουν:

- Τις πληροφορίες που θα πρέπει να προστατεύονται
- Τις απαιτούμενες ενέργειες όταν τερματίζεται η συνεργασία
- Τις απαιτούμενες ενέργειες για να αποφευχθεί η αποκάλυψη εμπιστευτικών πληροφοριών
- Τα δικαιώματα χρήσης των εμπιστευτικών πληροφοριών.

19 ΠΟΛΙΤΙΚΗ ΧΡΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Η χρήση του διαδικτύου (internet) και του ηλεκτρονικού ταχυδρομείου (e-mail) από το προσωπικό του Ομίλου ή/ και τους συνεργάτες του γίνεται αποκλειστικά για επαγγελματικούς σκοπούς και μόνο για την εκτέλεση των συμφωνηθέντων εργασιών στο πλαίσιο καθορισμένων αρμοδιοτήτων ή στο πλαίσιο συνεργασίας με τον Όμιλο. Ο Όμιλος εφαρμόζει μέτρα ελέγχου της ασφάλειας κατά τη χρήση των υπηρεσιών internet και e-mail, σύμφωνα με τα οριζόμενα στην ***«Πολιτική Προστασίας από Κακόβουλο Λογισμικό»***. Επιπλέον, καθένας που χρησιμοποιεί υπηρεσίες internet και e-mail μέσω εξοπλισμού του Ομίλου, έχει την υποχρέωση συμμόρφωσης με τα οριζόμενα στην ***«Πολιτική Αποδεκτής Χρήσης»***.

Παρακάτω αναφέρονται κανόνες για την αποτελεσματική χρήση του ηλεκτρονικού ταχυδρομείου:

- Οι χρήστες δεν ανοίγουν αρχεία που είναι συνημμένα σε e-mails όταν δεν είναι απολύτως σίγουροι για την ταυτότητα του αποστολέα, γιατί υπάρχει ο κίνδυνος εγκατάστασης κακόβουλου λογισμικού (virus, Trojan horse, worms, spyware, toolkits) στους υπολογιστές τους και κατά συνέπεια τη μεταφορά του μέσω του δικτύου σε όλα τα συστήματα του Ομίλου. Σε περίπτωση που υπάρχει οποιαδήποτε αμφιβολία ή το e-mail φαίνεται ύποπτο (αρκετά ορθογραφικά ή/ και συντακτικά λάθη, κείμενο εκφοβισμού κ.λπ.), οι χρήστες επικοινωνούν με τον Υπεύθυνο Ασφάλειας Πληροφοριών.
- Διαγράφονται άμεσα e-mail από δήθεν παρόχους οικονομικών υπηρεσιών (π.χ. Τράπεζες) όπου ζητούνται τα συνθηματικά χρηστών ή οποιοδήποτε άλλο προσωπικό στοιχείο.
- Οι χρήστες δεν θα πρέπει να απαντάνε και να προωθούν e-mail που λαμβάνουν με θέμα την ενημέρωση για ιούς ή κενά ασφαλείας. Ο μόνος υπεύθυνος για την αποστολή τέτοιων μηνυμάτων είναι η Διεύθυνση Ασφάλειας Πληροφοριών.
- Δεν θα πρέπει να αποκαλύπτεται σε καμία περίπτωση κανένα αναγνωριστικό (username – password) ηλεκτρονικών λογαριασμών.
- Δεν πρέπει να αποστέλλονται video ή εικόνες και γενικότερα μεγάλου μεγέθους αρχεία μέσω του ηλεκτρονικού ταχυδρομείου, καθώς δημιουργείται συμφόρηση και καθυστέρηση στο δίκτυο.
- Σε περίπτωση που υπάρχει υποψία ότι ένα e-mail περιέχει ιό, θα πρέπει να ενημερώνεται άμεσα η Διεύθυνση Ασφάλειας Πληροφοριών.
- Δεν θα πρέπει να γνωστοποιείται την ομιλική διεύθυνση ηλεκτρονικού ταχυδρομείου σε εξωτερικούς παρόχους ηλεκτρονικών υπηρεσιών ή σελίδες κοινωνικής δικτύωσης.
- Υπενθυμίζεται ότι το email (mailbox) <u>δεν είναι αποθηκευτικός χώρος</u>. Κάθε εργαζόμενος θα πρέπει να διενεργεί τακτική εκκαθάριση του ηλεκτρονικού ταχυδρομείου.

Όλες οι πληροφορίες που διακινούνται μέσω διαδικτύου (από τερματικά του Ομίλου) θα πρέπει να είναι αποκλειστικά επαγγελματικού περιεχομένου. Παρακάτω αναφέρονται μερικοί κανόνες για την αποτελεσματική / ασφαλή χρήση του διαδικτύου:

Το διαδίκτυο (internet) **ΔΕΝ** πρέπει να χρησιμοποιείται για:

- Αντιγραφή, αποκάλυψη, μεταφορά, αλλαγή ονομασίας, ανάγνωση ή διαγραφή πληροφοριών ή προγραμμάτων που ανήκουν σε άλλον χρήστη, χωρίς την έγκρισή του.
- Αντιγραφή, αποκάλυψη, μεταφορά, αλλαγή ονομασίας, ανάγνωση ή διαγραφή πληροφοριών ή προγραμμάτων που ανήκουν στον Όμιλο, χωρίς προηγούμενη έγκριση από τα αρμόδια στελέχη του Ομίλου.
- Παραβίαση ή παράκαμψη των μηχανισμών ασφαλείας που εφαρμόζει ο Όμιλος για προστασία από τους κινδύνους του Internet.
- Χρήση της δυνατότητας πρόσβασης στο Internet για απόκτηση παράνομης πρόσβασης σε άλλο υπολογιστικό σύστημα ή υπηρεσία.

- Κοινοποίηση λογαριασμών (accounts) ή κωδικών (passwords) άλλων χρηστών.
- Άνοιγμα κάθε είδους αρχείου προερχόμενου από το Internet χωρίς να έχει προηγηθεί σάρωση από λογισμικό antivirus.
- Δημιουργία λογαριασμών σε Online υπηρεσίες ή/ και κοινωνικά μέσα δικτύωσης (social media) όπως gmail, facebook κ.λπ. με ίδιο user name ή / και password που χρησιμοποιείται για πρόσβασή σε πληροφοριακούς πόρους του Ομίλου
    - (υπολογιστές, laptops, servers κ.α.).
- Αντιγραφή αρχείων μη επαγγελματικού περιεχομένου (downloading).

Το διαδίκτυο (Internet) μπορεί να χρησιμοποιηθεί για τη σύνδεση σε οποιοδήποτε ιστότοπο (Web site) απαιτείται για επαγγελματικούς λόγους, στο πλαίσιο εκτέλεσης των καθηκόντων βάσει αρμοδιοτήτων του ρόλου ή ρόλων που έχει αναλάβει κάθε εργαζόμενος.

Υπενθυμίζεται ότι η σύνδεση και χρήση των υπηρεσιών του Internet γίνεται μόνο με το εγκεκριμένο από τη Διεύθυνση Πληροφορικής λογισμικό και υλικό.

Οι χρήστες των υπηρεσιών πρόσβασης στο Διαδίκτυο και χρήσης ηλεκτρονικού ταχυδρομείου θα πρέπει να είναι ενήμεροι ότι το προσωπικό των διαχειριστών των πληροφοριακών συστημάτων είναι δυνατόν, στα πλαίσια των καθηκόντων του, να λάβει γνώση των ιστοχώρων που επισκέπτονται ή των πληροφοριών που διακινούν μέσω email.

20 ΠΟΛΙΤΙΚΗ ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΠΡΟΣΒΑΣΗΣ

Ο Όμιλος Ιατρικού Αθηνών εφαρμόζει μέτρα για τον έλεγχο της εξ αποστάσεως πρόσβασης (remote access) στις πληροφοριακές υποδομές του, είτε από το προσωπικό είτε από προσωπικό προμηθευτών ή συνεργάτες του Ομίλου. Ειδικότερα εφαρμόζονται τα εξής:

- Χρήση κρυπτογραφημένων καναλιών επικοινωνίας για την πρόσβαση σε υπολογιστικούς πόρους του Ομίλου. Το προσωπικό του Ομίλου μπορεί να έχει πρόσβαση μόνο μέσω ασφαλών εικονικών δικτύων (Virtual Private Networks – VPN), χρησιμοποιώντας τα κατάλληλα διαπιστευτήρια (username/ password, onetime password κ.λπ.).
- Κάθε VPN τερματίζει σε δικτυακή συσκευή firewall, όπου εφαρμόζονται κανόνες ελέγχου που επιτρέπουν ή απορρίπτουν την επικοινωνία.
- Η εξ αποστάσεως πρόσβαση των προμηθευτών ή συνεργατών του Ομίλου στα πληροφοριακά συστήματα για τα οποία έχουν εξουσιοδοτηθεί είναι ελεγχόμενη, διενεργείται για συγκεκριμένους σκοπούς, οι οποίοι είναι εκ των προτέρων γνωστοί στον Όμιλο και έχουν εγκριθεί από τη Διεύθυνση Ασφάλειας Πληροφοριών και οποιονδήποτε άλλο ρόλο απαιτείται ανά περίπτωση (π.χ. Ιδιοκτήτης Πληροφοριών).
- Σε κάθε περίπτωση, για την απομακρυσμένη σύνδεση σε πληροφοριακές υποδομές και πόρους του Ομίλου, χρησιμοποιούνται μόνο εγκεκριμένες από τον Όμιλο εφαρμογές.
- Καθένας ο οποίος συνδέεται απομακρυσμένα στις πληροφοριακές υποδομές του Ομίλου (εργαζόμενος, συνεργάτης, προμηθευτής κ.λπ.) έχει την υποχρέωση να συμμορφώνεται με τα οριζόμενα στην ***«Πολιτική Αποδεκτής Χρήσης»*** του Ομίλου.
- Αποτελεί υποχρέωση των εξουσιοδοτημένων για εξ αποστάσεως πρόσβαση χρηστών, να τηρούν αυστηρά προσωπικά τα διαπιστευτήρια πρόσβασης, να μην τα μοιράζονται με τρίτους και να διασφαλίζουν ότι μόνο αυτοί θα συνδέονται απομακρυσμένα σε πληροφοριακές υποδομές και πόρους του Ομίλου.
- Οι ενέργειες που εκτελούν οι χρήστες οι οποίοι συνδέονται εξ αποστάσεως στις πληροφοριακές υποδομές του Ομίλου καταγράφονται.

Η διαχείριση των λογαριασμών των χρηστών διενεργείται βάσει των κανόνων που ορίζονται στην ***«Πολιτική Ελέγχου Πρόσβασης & Διαχείρισης Χρηστών»***.

21 ΠΟΛΙΤΙΚΗ ΔΙΚΤΥΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Ο Όμιλος Ιατρικού Αθηνών εφαρμόζει μέτρα ελέγχου σε όλες τις δικτυακές επικοινωνίες, ανάλογα με το σκοπό κάθε επικοινωνίας και τα δεδομένα που χρησιμοποιούνται, ώστε να διασφαλίζεται η εμπιστευτικότητα, ακεραιότητα ή/ και διαθεσιμότητα των δεδομένων και συστημάτων του Ομίλου. Για τον έλεγχο της πρόσβασης σε πληροφοριακούς πόρους μέσω δικτυακών επικοινωνιών, εφαρμόζονται τα οριζόμενα στην ***«Πολιτική Ελέγχου Πρόσβασης & Διαχείρισης Χρηστών»*** και στην ***«Πολιτική Εξ Αποστάσεως Πρόσβασης»***.

Συστήματα και εφαρμογές τα οποία απαιτείται να είναι προσβάσιμα από το διαδίκτυο, τοποθετούνται σε ειδική ζώνη (DMZ) και η επικοινωνία τους με τις εσωτερικές πληροφοριακές υποδομές του Ομίλου αποκόπτεται μέσω συσκευής firewall.

Εφαρμόζονται, όπου απαιτείται, τεχνικές διαχωρισμού δικτύων (network segregation), με σκοπό τον περιορισμό της εξάπλωσης μιας επιτυχημένης διαδικτυακής επίθεσης στο σύνολο των πληροφοριακών υποδομών του Ομίλου.

Τα αρχεία καταγραφών των δικτυακών συσκευών ελέγχονται σε τακτά διαστήματα, σύμφωνα με τα οριζόμενα στην ***«Πολιτική Παρακολούθησης Ασφάλειας Συστημάτων και Εφαρμογών»***.

Η σύνδεση σε ασύρματα δίκτυα (Wireless networks) του Ομίλου γίνεται μετά από κατάλληλη εξουσιοδότηση. Στα ασύρματα δίκτυα εφαρμόζονται τεχνικές κρυπτογράφησης, σύμφωνα με τα οριζόμενα στην ***«Πολιτική Χρήσης Μεθόδων Κρυπτογραφίας»***.

Οποιαδήποτε αλλαγή απαιτείται σε δικτυακές υποδομές ή σε ρυθμίσεις δικτυακών συσκευών, υλοποιείται μέσω καθορισμένης διαδικασίας διαχείρισης αλλαγών. Δικτυακές συνδέσεις οι οποίες χαρακτηρίζονται ως μη απαραίτητες, απενεργοποιούνται εντός σύντομου χρονικού διαστήματος, μετά την οριστικοποίηση της μη αναγκαιότητας από όλους τους εμπλεκομένους (π.χ. αρμόδιοι Διευθυντές, Ιδιοκτήτες Πληροφοριών, Υπεύθυνοι Πόρων κ.α.).

ΟΜΙΛΟΣ ΙΑΤΡΙΚΟΥ ΑΘΗΝΩΝ

Ημερομηνία Έκδοσης / αναθεώρησης	Αριθμός	Λεπτομέρειες	Έγκριση Ημερομηνία Έκδοσης Αλλαγών	
21.09.2023	1η	ΕΚΔΟΣΗ	ΔΣ	21.09.2023