ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η Διεύθυνση Ανθρώπινου Δυναμικού είναι υπεύθυνη να τηρεί ενημερωμένο αρχείο για όλο το δυναμικό της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ. Το αρχείο πρέπει να περιλαμβάνει ακριβείς και ενημερωμένες πληροφορίες αναφορικά με το ρόλο και τις αρμοδιότητες του εργαζόμενου μέσα στην Εταιρεία. Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ οφείλει να ακολουθεί επίσημες διαδικασίες για τον ασφαλή χειρισμό των προσωπικών δεδομένων των υπαλλήλων (π.χ. οικονομικά στοιχεία, ιατρικά στοιχεία).

Όλοι οι πόροι που παρέχονται στους υπαλλήλους / συνεργάτες για τη διεξαγωγή των εργασιακών τους καθηκόντων (π.χ. φορητοί υπολογιστές, κάρτες εισόδου κ.ά.) πρέπει να καταγράφονται. Οι χρήστες οφείλουν να υπογράφουν μια βεβαίωση παραλαβής των πόρων.

Γενικές Αρχές κατά τη Λήξη της Εργασίας / Συνεργασίας

Σε κάθε περίπτωση όπου τερματίζεται η συνεργασία του χρήστη με την Εταιρεία , η Διεύθυνση Ανθρωπίνου Δυναμικού σε συνεργασία με τους προϊσταμένους των χρηστών θα πρέπει να φροντίσουν άμεσα για τις παρακάτω ενέργειες:

- Την άμεση ανάκληση όλων των δικαιωμάτων φυσικής και λογικής πρόσβασης που τους είχαν παραχωρηθεί.
- Την επιστροφή κάθε πληροφορίας ή εξοπλισμού που ανήκει στην ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ.

Δεν επιτρέπεται στους υπαλλήλους / συνεργάτες να απομακρύνουν ή να διατηρούν πληροφορίες της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ μετά την λήξη της συνεργασίας με την Εταιρεία. Όλες οι πληροφορίες που τηρούνται από τον εργαζόμενο / συνεργάτη ή είναι στην κατοχή του κατά τη διάρκεια της απασχόλησής του, θα πρέπει να παραδίδονται στο προϊστάμενό του πριν την αποχώρησή του.

Εξαίρεση για τη μη εφαρμογή της παραπάνω πολιτικής αποτελούν προσωπικά αντίγραφα δημόσιων πληροφοριών, και προσωπικά αντίγραφα ηλεκτρονικής αλληλογραφίας. Όλοι οι χρήστες κατά τη λήξη της εργασιακής τους σχέσης με την Εταιρεία οφείλουν να επιστρέψουν όλα τα περιουσιακά στοιχεία της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ που τους παραχωρήθηκαν για την εκτέλεση της εργασίας τους, όπως φορητούς υπολογιστές, λογισμικό, κλειδιά, εγχειρίδια, κλπ.

21.1. ΠΟΛΙΤΙΚΗ ΔΙΑΒΑΘΜΙΣΕΩΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΠΟΡΩΝ

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ ορίζει τους κανόνες για την αποδεκτή χρήση των πληροφοριών και των πληροφοριακών της συστημάτων, σύμφωνα με το βαθμό κρισιμότητάς τους. Σκοπός είναι η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των συστημάτων και η αποτροπή επιβλαβών συμβάντων που μπορεί να προκύψουν από την κακή χρήση των παραπάνω. Όλοι οι χρήστες οφείλουν

να είναι σε συμμόρφωση με τους κανόνες αυτούς και απαγορεύεται να προβαίνουν σε μη επιτρεπόμενες ενέργειες.

Πεδίο Εφαρμογής

Η παρούσα πολιτική αφορά όλες τις εταιρικές πληροφορίες είτε σε έντυπη είτε σε ηλεκτρονική μορφή και όλα τα πληροφοριακά συστήματα που στηρίζουν τις επιχειρηματικές λειτουργίες της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ. Η πολιτική αυτή απευθύνεται σε όλα μέλη του προσωπικού και στους συνεργάτες της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ.

Γενικές Αρχές Δικαιώματα και Υποχρεώσεις των Χρηστών

Όλοι οι χρήστες πρέπει να εφαρμόζουν και να τηρούν τη Πολιτική Ασφάλειας Πληροφοριών, τις υποστηρικτικές πολιτικές και διαδικασίες ασφάλειας και να εφαρμόζουν όλα τα ενδεικνυόμενα μέτρα, με σκοπό τη προστασία των πληροφοριών και πληροφοριακών συστημάτων της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ. Όλο το προσωπικό (εξωτερικοί συνεργάτες και υπάλληλοι) πρέπει να αποκτά πρόσβαση μόνο στους πληροφοριακούς πόρους που τους έχουν εκχωρηθεί για την διεξαγωγή των εργασιακών τους καθηκόντων. Οι χρήστες οφείλουν να χρησιμοποιούν τους πόρους που τους παρέχονται με ασφαλή και νόμιμο τρόπο. Οι χρήστες δεν επιτρέπεται να αποκαλύπτουν διαβαθμισμένες πληροφορίες, τις οποίες χρησιμοποιούν ή/και επεξεργάζονται κατά τη διεξαγωγή των εργασιακών τους καθηκόντων. Επιπρόσθετα, οι χρήστες πρέπει να είναι ενήμεροι ότι τα δεδομένα και οι πληροφορίες οι οποίες δημιουργούνται κατά τη διάρκεια της εργασίας τους στην Εταιρεία, είναι ιδιοκτησία της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ. Οι χρήστες δεν επιτρέπεται να υποκλέπτουν ή με οποιοδήποτε άλλο τρόπο να ανακαλύπτουν συνθηματικά, κρυπτογραφικά κλειδιά ή οποιοδήποτε άλλο μηχανισμό ελέγχου πρόσβασης ο οποίος θα μπορούσε να τους επιτρέψει μη εξουσιοδοτημένη πρόσβαση στα πληροφοριακά και δικτυακά συστήματα του Οργανισμού. Κάθε προσπάθεια μείωσης του επιπέδου ασφάλειας των πληροφοριακών συστημάτων απαγορεύεται αυστηρά. Απαγορεύεται κάθε είδους χρήση, εγκατάσταση και αντιγραφή παράνομου λογισμικού στα πληροφοριακά συστήματα της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ. Οι χρήστες δεν επιτρέπεται να εγκαθιστούν μη εξουσιοδοτημένο λογισμικό (οποιοδήποτε λογισμικό δεν έχει εγκατασταθεί από την ομάδα του IT Support), καθώς υπάρχει σοβαρός κίνδυνος το λογισμικό αυτό να είναι μολυσμένο με ιούς υπολογιστών, Trojan horses κλπ. το οποίο δύναται να βλάψει τις πληροφορίες και τα συστήματα του Οργανισμού.

Η χρήση των πληροφοριακών συστημάτων της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ παρέχεται στο προσωπικό της ως εργαλείο διεξαγωγής επιχειρηματικών δραστηριοτήτων. Η χρήση αυτών για προσωπικούς σκοπούς είναι επιτρεπτή μέσα σε ορισμένα πλαίσια, και επιτρέπεται όταν:

- Δε στοχεύει σε επίτευξη προσωπικού οφέλους του εργαζόμενου ή άλλης επιχειρηματικής οντότητας πλην της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ (εμπλοκή σε προσωπικές επιχειρηματικές δραστηριότητες του εργαζομένου, επιχειρήσεις με τις οποίες ο εργαζόμενος έχει οποιαδήποτε σχέση κερδοσκοπική ή μη κτλ),
- Δεν επηρεάζει την παραγωγικότητα των εργαζομένων,

- Δεν αντίκειται στην παρούσα και σε οποιαδήποτε άλλη πολιτική Δικαιώματα και Υποχρεώσεις της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ.

  Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ διατηρεί το δικαίωμα να διενεργεί τακτικούς ή έκτακτους ελέγχους στα πληροφοριακά συστήματα για την τήρηση των πολιτικών, των διαδικασιών και των μηχανισμών ασφάλειας. Τους ελέγχους τους πραγματοποιούν εξουσιοδοτημένα άτομα, και το προσωπικό οφείλει να συνεργαστεί για την ομαλή διεξαγωγή αυτών.

  <u>Προστασία Εταιρικών Πληροφοριών</u>

  Οι χρήστες κατά τη διαχείριση των συστημάτων και πληροφοριών της Εταιρείας πρέπει να συμμορφώνονται με το ισχύον νομοθετικό και κανονιστικό πλαίσιο και ειδικότερα με τις διατάξεις για την προστασία των προσωπικών δεδομένων.
  Όλοι οι υπάλληλοι της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ είναι υπεύθυνοι να «κλειδώνουν» τους σταθμούς εργασίας / φορητούς υπολογιστές όταν απομακρύνονται από αυτούς και να χρησιμοποιούν προστασία φύλαξης της οθόνης (screen saver).
  Οι υπάλληλοι απαγορεύεται να αποκαλύπτουν σε τρίτους ή να δημοσιοποιούν πληροφορίες και δεδομένα της Εταιρείας τα οποία δεν προορίζονται για δημόσια χρήση. Ενδεικτικά:
- Πληροφορίες χρηματοοικονομικού περιεχομένου που δεν έχουν δημοσίως κοινοποιηθεί,
- Επιχειρησιακά πλάνα και στρατηγικές,
- Ερευνητικές εργασίες που διεξάγονται στο πλαίσιο των δραστηριοτήτων της Εταιρείας,
- Πληροφορίες αναφορικά με τους εξωτερικούς συνεργάτες της Εταιρείας,
- Κάθε πληροφορία, η οποία δεν έχει χαρακτηριστεί ότι προορίζεται για δημόσια χρήση.

21.2. ΠΟΛΙΤΙΚΗ ΟΡΓΑΝΩΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η εταιρεία ανταποκρινόμενη στις απαιτήσεις της σύγχρονης επιχειρηματικής πραγματικότητας και στοχεύοντας στην προστασία των πληροφοριακών συστημάτων της, αποσκοπώντας πάντα στην απρόσκοπτη και υποδειγματική εξυπηρέτηση των Πελατών της, έχει εγκαταστήσει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.

Οι βασικοί στόχοι, έτσι όπως αυτοί εκφράζονται μέσα στις διαδικασίες του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών της εταιρείας, είναι:

- Η δημιουργία βάσης για τη διαρκή βελτίωση της αποτελεσματικότητας των διεργασιών της, έχοντας ως γνώμονα τη συνεχή ικανοποίηση των αναγκών και των προσδοκιών των πελατών της στον μέγιστο δυνατό βαθμό.
- Η ελαχιστοποίηση του αριθμού των συμβάντων που μπορεί να επηρεάσουν τη συνέχεια των επιχειρησιακών διεργασιών, καθώς και την κατά το δυνατό μείωση των επιπτώσεών τους.
- Η Διοίκηση της εταιρίας θεωρεί ότι οι πληροφορίες που τηρούνται και διακινούνται με οποιονδήποτε τρόπο, μέσα από τα ηλεκτρονικά και μη συστήματα της, αποτελούν στοιχεία εξαιρετικής σημασίας για τη λειτουργία

και τη θέση της στην αγορά και δεσμεύεται να χειρίζεται τις πληροφορίες αυτές με τρόπο που προστατεύει την ασφάλειά τους, ενώ ταυτόχρονα συμμορφώνεται με τους νόμους και τις κανονιστικές διατάξεις στις οποίες υπόκειται.

Το σύστημα της εταιρίας ανασκοπείται σε τακτά χρονικά διαστήματα από τη Διοίκηση, προκειμένου να προσαρμόζεται στις νέες ανάγκες και εξελίξεις της αγοράς, στις νομοθετικές απαιτήσεις, αλλά και στην επίτευξη του στόχου για συνεχή βελτίωση των λειτουργιών της εταιρίας.

Η Διοίκηση δεσμεύεται στη διάθεση της υποδομής, των ανθρώπινων πόρων και του εξοπλισμού που κρίνεται απαραίτητη για την υλοποίηση των εργασιών της. Κάθε εργαζόμενος είναι υπεύθυνος να ανταποκρίνεται, να αφομοιώνει και να εφαρμόζει τις διαδικασίες που απαιτεί το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών μέσα από τις καθημερινές δραστηριότητες του.

21.3 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΦΑΡΜΟΓΩΝ

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ διατηρεί έναν ενημερωμένο κατάλογο με το πληροφοριακό και δικτυακό εξοπλισμό που στηρίζει την επιχειρηματική λειτουργία της Εταιρείας. Η διαδικασία της καταγραφής των πόρων του οργανισμού είναι σημαντικό τμήμα της διαδικασίας διαχείρισης κινδύνου. Ο κατάλογος πρέπει να είναι ανανεωμένος και να καταγράφονται σε αυτόν όλες οι αλλαγές που έχουν λάβει χώρα. Οι πόροι που καταγράφονται κατά ελάχιστο είναι οι ακόλουθοι:

- Πληροφοριακοί Πόροι (Software Assets): βάσεις δεδομένων, αρχεία δεδομένων, εφαρμογές, εργαλεία ανάπτυξης, servers κλπ.
- Φυσικοί Πόροι: υλικό υπολογιστών, εξοπλισμός τηλεπικοινωνιών, αποθηκευτικά μέσα κλπ.
- Δικτυακός Εξοπλισμός: μηχανισμοί προστασίας (firewalls,switches κλπ.

<u>Πεδίο Εφαρμογής</u>

Η παρούσα πολιτική αφορά όλες τις εταιρικές πληροφορίες είτε σε έντυπη είτε σε ηλεκτρονική μορφή και όλα τα πληροφοριακά συστήματα που στηρίζουν τις επιχειρηματικές λειτουργίες της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ. Η πολιτική αυτή απευθύνεται σε όλα μέλη του προσωπικού και στους συνεργάτες της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ.

21.4 ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

Πρόσβαση στους πόρους της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ (συστήματα, δίκτυο, πληροφορίες) πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα και μόνο στο πλαίσιο της διεκπεραίωσης των καθηκόντων τους. Το επίπεδο «λογικής πρόσβασης» πρέπει να είναι ανάλογο με τις απαιτήσεις ασφάλειας της πληροφορίας και του πληροφοριακού συστήματος και να προσδιορίζεται από την επιχειρηματική ανάγκη για τη διεκπεραίωση επαγγελματικών καθηκόντων. Τα θέματα αναφορικά με τη διαχείριση της λογικής πρόσβασης των χρηστών περιγράφονται παρακάτω.

Πεδίο Εφαρμογής

Η παρούσα πολιτική απευθύνεται σε όλους τους υπαλλήλους και τους εξωτερικούς συνεργάτες της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ, οι οποίοι χρειάζονται πρόσβαση στα πληροφοριακά συστήματα της Εταιρείας για την εκπλήρωση των εργασιακών καθηκόντων τους.

Γενικές Αρχές Δικαιώματα & Μηχανισμοί Πρόσβασης Χρηστών

Τα δικαιώματα πρόσβασης που δύναται να αποκτήσει ο κάθε χρήστης στα συστήματα της Εταιρείας, πρέπει να είναι επακριβώς ορισμένα και αυστηρά συνδεδεμένα με τις απαιτήσεις της εργασίας του, βάσει του ρόλου του στην ομάδα στην οποία ανήκει. Τα δικαιώματα πρόσβασης πρέπει να παραχωρούνται βάσει της ανάγκης γνώσης ("Need- to-know") για την αποφυγή θεμιτής ή αθέμιτης αποκάλυψης πληροφοριών. Συνεπώς, πρέπει να παρέχεται μόνο το ελάχιστο αποδεκτό επίπεδο προνομίων στους χρήστες έτσι ώστε να μπορούν να εκτελούν τις καθημερινές εργασίες τους. Κάθε χρήστης είναι συνδεδεμένος με ένα μοναδικό αναγνωριστικό (user id) και συνθηματικό, ως μέσο ταυτοποίησης και αυθεντικοποίησης στα συστήματα της Εταιρείας.

Κάθε χρήστης φέρει αποκλειστική ευθύνη για οποιαδήποτε ενέργεια λαμβάνει χώρα μέσω του προσωπικού του λογαριασμού (user id/ password). Η χρήση ομαδικών λογαριασμών (Group accounts) πρέπει να αποφεύγεται, εκτός εάν υπάρχει συγκεκριμένη επιχειρησιακή ανάγκη. Σε μια τέτοια περίπτωση πρέπει να υπάρχει έγκριση από Υπεύθυνο Ασφαλείας. Στη περίπτωση που η πρόσβαση σε δυο ή περισσότερες υπηρεσίες απαιτεί τη δημιουργία περαιτέρω λογαριασμών για ένα χρήστη, τότε οι λογαριασμοί αυτοί θα πρέπει να έχουν μεταξύ τους διαφορετικά συνθηματικά. Η χορήγηση προνομιακών δικαιωμάτων πρόσβασης (privileged accounts) είναι επιτρεπτή μόνο όταν απαιτείται από το ρόλο του χρήστη (π.χ. διαχειριστής δικτύου). Για τη χορήγηση προνομιακών δικαιωμάτων είναι απαραίτητη η έγκριση του Υπεύθυνου Ασφαλείας.

Τροποποίηση και Κατάργηση Δικαιωμάτων Πρόσβασης

Σε περίπτωση που κάποιος υπάλληλος αλλάξει ρόλο και αρμοδιότητες, αλλάζουν και τα δικαιώματα πρόσβασης που αντιστοιχούν στα νέα του καθήκοντα. Κατά συνέπεια, τα δικαιώματα πρόσβασης που δεν χρειάζονται στη νέα θέση εργασίας του χρήστη, πρέπει να καταργούνται αμέσως. Τα δικαιώματα πρόσβασης των χρηστών και των εξωτερικών συνεργατών της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ πρέπει να καταργούνται άμεσα μετά την αποχώρηση του χρήστη από την Εταιρεία και τη λήξη του έργου αντίστοιχα. Σε περίπτωση που ο υπάλληλος που αποχωρεί γνωρίζει συνθηματικά λογαριασμών που χρειάζεται να παραμείνουν ενεργοί, τότε τα συνθηματικά των λογαριασμών πρέπει να αλλάζουν κατά τη λήξη της απασχόλησης του χρήστη.

21.5 ΠΟΛΙΤΙΚΗ ΑΝΑΠΤΥΞΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΕΦΑΡΜΟΓΩΝ

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ διαθέτει πλήρη περιγραφή του computer room ή του χώρου εγκατάστασης (φυσική πρόσβαση, προστασία χώρου, ασφάλεια συστημάτων, ρεύματα, εναλλακτική παροχή ηλ. ρεύματος, κλιματισμός κ.λπ.).
Πλήρες και αναλυτικό Διάγραμμα Αρχιτεκτονικής Δικτύου που να περιλαμβάνει:

- Δικτυακές συσκευές, servers, σταθμούς εργασίας. Για κάθε δικτυακή συσκευή εμφανίζεται ο αριθμός των Interfaces που διαθέτει, VLANs, Συνδέσεις με Internet, τρόπος με τον οποίο επιτυγχάνεται η σύνδεση στο Internet (π.χ. adsl,

- Πλήρη περιγραφή του τοπικού δικτύου των σταθμών εργασίας.
- Λίστα εξοπλισμού, η οποία να περιέχει για την κάθε συσκευή:
- Κατασκευαστή, μοντέλο, serial numbers, κύρια χαρακτηριστικά,
- Εγγύηση, συντήρηση/υποστήριξη, αντίστοιχο συμβόλαιο.
- Λίστα λογισμικού (λειτουργικών συστημάτων, έτοιμων πακέτων λογισμικού, εφαρμογών) που για κάθε πακέτο να περιέχει: Κατασκευαστή, έκδοση, serial numbers, κωδικούς προϊόντος (software keys),
- Εγγύηση, συντήρηση/υποστήριξη, αντίστοιχο συμβόλαιο.
- Λίστα προμηθευτών, κατασκευαστών, συνεργατών (που υποστηρίζουν το ΠΣ) για το hardware και το software, με στοιχεία επικοινωνίας (για περίπτωση προβλήματος).
- Κατηγοριοποίηση πόρων Πληροφοριακού Συστήματος (ΠΣ) ως προς τη σπουδαιότητά τους για την εύρυθμη λειτουργία της εταιρίας
- Κατηγοριοποίηση περιβαλλόντων Πληροφοριακού Συστήματος ως προς το είδος λειτουργίας τους (παραγωγικό περιβάλλον, περιβάλλον ανάπτυξης, test περιβάλλον).
- Πλήρη Τεκμηρίωση Λειτουργικών Συστημάτων Microsoft Windows, λαμβάνοντας σοβαρά υπόψιν τον επίσημο κύκλο ζωής υποστήριξης της κάθε έκδοσης.

21.6 ΠΟΛΙΤΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ έχει λάβει όλα τα απαραίτητα οργανωτικά και τεχνολογικά μέτρα για την πρόληψη και την αντιμετώπιση των περιστατικών ασφάλειας, με σκοπό να είναι δυνατός ο έγκαιρος χειρισμός τους πριν πραγματοποιηθεί σημαντική ζημιά. Όλα τα ύποπτα περιστατικά διερευνώνται από το αρμόδιο προσωπικό, σύμφωνα με τις καταγεγραμμένες διαδικασίες.

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ έχει αναπτύξει τους κατάλληλους διαύλους επικοινωνίας για την αναφορά των περιστατικών ασφάλειας και να τους γνωστοποιήσει σε όλο το προσωπικό του. Τα θέματα διαχείρισης περιστατικών ασφάλειας περιγράφονται παρακάτω.

<u>Πεδίο Εφαρμογής</u>

Η παρούσα πολιτική ασφάλειας αφορά σε όλα τα πληροφοριακά συστήματα που στηρίζουν τη λειτουργία της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ. Επίσης, αφορά όλους τους χρήστες και τους εξωτερικούς συνεργάτες που αποκτούν πρόσβαση σε αυτά και στις πληροφορίες της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ κατά τη διάρκεια της συνεργασίας τους με την Εταιρεία.

Γενικές Αρχές Διαχείρισης Περιστατικών Ασφάλειας

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ εφαρμόζει όλους τους απαραίτητους μηχανισμούς ασφαλείας για την προστασία των πληροφοριακών συστημάτων από ενδεχόμενα περιστατικά ασφάλειας. Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ έχει ορίσει με σαφήνεια τους απαραίτητους ρόλους και τις αντίστοιχες αρμοδιότητες για την άμεση και ορθή αντιμετώπιση των ενδεχόμενων περιστατικών ασφάλειας. Οι ρόλοι έχουν ανατεθεί σε κατάλληλα καταρτισμένους υπαλλήλους της Εταιρείας ή εξωτερικούς συνεργάτες. Οι χρήστες δεν επιτρέπεται να αποκαλύπτουν πληροφορίες που σχετίζονται με τα περιστατικά ασφάλειας. Οι πληροφορίες αυτές συζητούνται μόνο με το υπεύθυνο και εξουσιοδοτημένο προσωπικό της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ.

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ έχει ορίσει τον Υπεύθυνο Ασφάλειας ως το σημείο επικοινωνίας και αναφοράς των περιστατικών ασφάλειας. Κάθε μορφή παρεμπόδισης του προσωπικού να εκτελέσει το έργο του κατά το στάδιο της αναφοράς, της έρευνας και της αντιμετώπισης των περιστατικών ασφάλειας, θεωρείται μη συμμόρφωση με τη Πολιτική Ασφάλειας Πληροφοριών και ενδέχεται να υπάρξουν πειθαρχικές κυρώσεις. Ο Υπεύθυνος Ασφάλειας είναι υπεύθυνος να αξιολογήσει εάν το περιστατικό ασφάλειας οφείλεται σε κακόβουλες ενέργειες που προέρχονται από τους εσωτερικούς χρήστες της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ είτε από εξωτερικούς παράγοντες και ανάλογα να ενημερώσει άμεσα τη Διοίκηση, ώστε να καθοριστούν οι ενέργειες για την αντιμετώπισή του.

Κάθε περιστατικό ασφάλειας που επιβεβαιώνεται πρέπει να αξιολογείται ως προς τη κρισιμότητά του βάσει των δεδομένων ή πιθανών επιπτώσεων στην Εταιρεία. Ενδεικτικά:

- Υψηλή Προτεραιότητα: όταν έχουν διακυβευτεί ή είναι πολύ πιθανό να διακυβευτούν κρίσιμα πληροφοριακά συστήματα της Εταιρείας, με αποτέλεσμα να επηρεαστεί η ομαλή συνέχεια της λειτουργίας του και να υπάρξουν μεγάλες οικονομικές απώλειες.
- Μεσαία Προτεραιότητα: όταν υπάρχουν βάσιμες ενδείξεις ότι κρίσιμα ή/και υποστηρικτικά συστήματα της Εταιρείας είναι στόχος επίθεσης (π.χ. επιθέσεις τύπου denial of service, σημαντικός αριθμός scans σε πληροφοριακά συστήματα της Εταιρείας, διαρροή συνθηματικών προνομιούχων χρηστών)
- Χαμηλή Προτεραιότητα: όταν δεν υπάρχει άμεσος κίνδυνος, αλλά έχουν εντοπιστεί σημάδια επιθέσεων και παραβίασης στα πληροφοριακά συστήματα (π.χ. μικρός αριθμός αποτυχημένων προσπαθειών μη εξουσιοδοτημένης πρόσβασης σε πληροφοριακά συστήματα).

Μετά την αντιμετώπιση του περιστατικού διεξάγεται ανάλογη έρευνα με στόχο την ανακάλυψη των αιτιών της πραγματοποίησης του περιστατικού ασφάλειας και τις άμεσες και έμμεσες επιπτώσεις του περιστατικού ασφάλειας. Επιπρόσθετα, γίνεται αξιολόγηση των ενεργειών που έλαβαν χώρα. Ο Υπεύθυνος Ασφάλειας πρέπει να τηρεί ενημερωμένο αρχείο που θα περιέχει τις παραπάνω πληροφορίες καθώς μπορεί να χρησιμοποιηθούν κατά τη διεξαγωγή αποτίμησης κινδύνου και κατά την αξιολόγηση των υπαρχόντων μηχανισμών ασφάλειας των πληροφοριακών συστημάτων. Ο απώτερος σκοπός είναι η απόκτηση εμπειρίας από το περιστατικό ασφάλειας. Μετά την αντιμετώπιση του περιστατικού ασφάλειας, πρέπει να διεξάγεται έλεγχος των

μηχανισμών ασφάλειας στα πληροφοριακά συστήματα που είχαν επηρεαστεί. Ο έλεγχος μπορεί να πραγματοποιείται είτε από το προσωπικό, είτε από εξωτερικούς συνεργάτες, εάν αυτό κρίνεται απαραίτητο.

Υποχρεώσεις Προσωπικού

Όλοι οι υπάλληλοι της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ οφείλουν να είναι ενήμεροι με την παρούσα πολιτική ασφάλειας και να τις εφαρμόζουν όταν παραστεί ανάγκη. Όλοι οι υπάλληλοι της ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ είναι υπεύθυνοι να παρατηρούν και να αναφέρουν κάθε ύποπτο περιστατικό ασφάλειας και κάθε πιθανή αδυναμία των πληροφοριακών συστημάτων στον Υπεύθυνο Ασφάλειας. Ιδιαίτερα οι διαχειριστές συστημάτων είναι υπεύθυνοι να παρατηρούν και να αναφέρουν οποιαδήποτε αδυναμία του πληροφοριακού συστήματος που θα υποπέσει στην αντίληψή τους κατά τη διεξαγωγή των εργασιακών τους καθηκόντων. Οι χρήστες δεν πρέπει να αποκαλύπτουν τις αντίστοιχες πληροφορίες σε μη εξουσιοδοτημένα άτομα, σε καμία περίπτωση. Οι χρήστες δεν πρέπει σε καμία περίπτωση να επιχειρούν αυτόβουλη παρέμβαση στα πληροφοριακά συστήματα, εκτός εάν είναι εξουσιοδοτημένοι. Μόνο το εξειδικευμένα προσωπικό συμμετέχει στην ανάκαμψη των συστημάτων στη κανονική τους λειτουργία.

Προστασία από Κακόβουλο Λογισμικό

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ οφείλει να λαμβάνει όλα τα απαραίτητα οργανωτικά και τεχνικά μέτρα ασφάλειας, τα οποία αποσκοπούν στην αποτροπή, ανίχνευση και αντιμετώπιση του κακόβουλου λογισμικού. Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ οφείλει να ενημερώνει τους εργαζόμενους αναφορικά με τους κινδύνους από το κακόβουλο λογισμικό καθώς και για τις υποχρεώσεις τους σε σχέση με τα μέτρα προστασίας έναντι του κακόβουλου λογισμικού. Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΣΕ οφείλει, να πραγματοποιεί έλεγχο της ακεραιότητας του λογισμικού των ΠΕΣ. Ο έλεγχος αυτός έχει ως σκοπό τη διαπίστωση της μη ύπαρξης λογισμικού στα ΠΕΣ πέραν αυτού που έχει επισήμως προμηθευτεί.

21.7 ΠΟΛΙΤΙΚΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ

Η διοίκηση της ΙΚΤΙΝΟΣ ΕΛΛΑΣ αναγνωρίζει τους κινδύνους που ενδέχεται να απειλήσουν την απρόσκοπτη λειτουργία των δραστηριοτήτων της και διαθέτει όλους τους απαιτούμενους πόρους για την εφαρμογή Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας ώστε:

- Να διασφαλίσει την Επιχειρησιακή Συνέχεια κρίσιμων δραστηριοτήτων σε περίπτωση εκδήλωσης περιστατικού που οδηγεί σε μη διαθεσιμότητα ή αδυναμία πρόσβασης των εγκαταστάσεων της εταιρίας
- Να είναι σε θέση να επιστρέψει σε αποδεκτά επίπεδα λειτουργίας στο συντομότερο δυνατό χρόνο
- Να ελαχιστοποιήσει τις επιπτώσεις που ενδέχεται να προκαλέσουν περιστατικά διακοπής στην αξιοπιστία και φήμη της εταιρίας ενώπιον των πελατών της.

21.8 ΠΟΛΙΤΙΚΗ ΔΙΑΓΡΑΦΗΣ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Όλες οι διαβαθμισμένες πληροφορίες είτε σε έντυπη είτε σε ηλεκτρονική μορφή, πρέπει να καταστρέφονται με ασφάλεια όταν πλέον δεν είναι χρήσιμες για τη λειτουργία της Εταιρείας, με σκοπό να αποφευχθεί η διαρροή τους.

21.9 ΠΟΛΙΤΙΚΗ ΑΡΧΕΙΟΘΕΤΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η Εταιρεία δεσμεύεται, για την νόμιμη και δίκαιη διαχείριση και αρχειοθέτηση όλων των Προσωπικών Δεδομένων, σεβόμενη τα νόμιμα δικαιώματα, την ιδιωτικότητα και την εμπιστοσύνη όλων όσων με τους οποίους συναλλάσσεται.

Αρχές Προστασίας Δεδομένων

Η παρούσα Πολιτική αποσκοπεί στον καθορισμό της βέλτιστης πρακτικής της Εταιρείας για την εξασφάλιση της προστασίας των Προσωπικών Δεδομένων. Όλα τα Προσωπικά Δεδομένα πρέπει να:

- υποβάλλονται σε νόμιμη, δίκαιη και διαφανή επεξεργασία,
- συλλέγονται για συγκεκριμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία με τρόπο ασυμβίβαστο προς τους σκοπούς αυτούς,
- είναι ακριβή και, εφόσον απαιτείται, να διατηρούνται ενημερωμένα.

21.10 ΠΟΛΙΤΙΚΗ ΚΑΤΑΣΤΡΟΦΗΣ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΜΕΣΩΝ ΠΛΗΡΟΦΟΡΙΚΩΝ

Καταστροφή Αποθηκευτικών Μέσων και Εγγράφων

Σε περίπτωση που κάποιο επαναχρησιμοποιούμενο αποθηκευτικό μέσο πρόκειται να αλλάξει χρήση ή δεν απαιτείται πλέον η διατήρηση των αποθηκευμένων πληροφοριών του, τότε πρέπει να διαγράφονται με ασφαλή τρόπο όλα τα περιεχόμενά του. Όλα τα έγγραφα τα οποία βρίσκονται σε έντυπη μορφή, πρέπει να καταστρέφονται ασφαλώς με τη χρήση κατάλληλων μηχανημάτων (π.χ. shredder). Οι Ιδιοκτήτες Συστημάτων πρέπει να εξασφαλίζουν ότι πριν τη καταστροφή των αποθηκευτικών μέσων, τα δεδομένα και το λογισμικό που βρίσκονται αποθηκευμένα σε αυτά έχουν αφαιρεθεί. (A_05 - Αρχείο Καταστροφής Διαβαθμισμένων Εγγράφων & Αποθηκευτικών Μέσων)

21.11 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΜΕΣΩ EMAIL

Όταν κάποιος επικοινωνεί μέσω email με την Εταιρία, τότε ανάλογα με τη φύση του αιτήματος/ερωτήματος, το είδος και το εύρος των πληροφοριών που ζητάει, ο αρμόδιος εκπρόσωπος της Εταιρίας θα ελέγξει πρώτα αν η email διεύθυνση του αποστολέα είναι εξουσιοδοτημένη για επικοινωνία (για να

λάβει απαντήσεις ή πληροφορίες ή να ζητήσει την εκτέλεση μιας εργασίας από την Εταιρία).

Η Εταιρία δεν παρέχει πληροφορίες (και ειδικά προσωπικά δεδομένα) μέσω email, τηλεφώνου και live chat, ενώ ακόμα και αν έχει προηγηθεί ταυτοποίηση του πελάτη.

Η Εταιρία θεωρεί απόρρητα τα αιτήματα που συμπληρώνουν οι πελάτες της και την ηλεκτρονική αλληλογραφία που στέλνουν διαμέσω των υπηρεσιών της και δε μεταβιβάζει το περιεχόμενο αυτών παρά μόνο στον άμεσα ενδιαφερόμενο αποδέκτη και στον νόμο, εφόσον αυτό της ζητηθεί ή στην περίπτωση που το περιεχόμενο του μηνύματος θεωρηθεί ότι την θίγει ή συνδέεται με παράνομες ενέργειες.

Αν κάποιος Πελάτης ή χρήστης δηλώσει ψευδή ηλεκτρονική διεύθυνση ή προσπαθήσει να πάρει τη θέση κάποιου άλλου όταν στέλνει πληροφορίες online, όλες οι πληροφορίες -καθώς επίσης και η διεύθυνση IP του χρήστη- θα αποτελούν μέρος οποιασδήποτε νόμιμης έρευνας τυχόν διαταχθεί.

Οι εργαζόμενοι της Εταιρείας μπορεί να χρειαστεί να επεξεργαστούν κάθε ηλεκτρονικό μήνυμα σε συνεργασία με το τεχνικό της τμήμα.

Η διακίνηση της ηλεκτρονικής αλληλογραφίας γίνεται μέσω του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol) και κανένα από τα δεδομένα που παρέχετε δεν θα μεταβιβαστεί ή θα υποβληθεί σε επεξεργασία από οποιονδήποτε τρίτο φορέα επεξεργασίας δεδομένων. Οι SMTP διακομιστές προστατεύονται από πρωτόκολλο ασφαλείας TLS, που σημαίνει ότι το περιεχόμενο ηλεκτρονικού ταχυδρομείου κρυπτογραφείται πριν αποσταλεί μέσω του διαδικτύου. Το περιεχόμενο του ηλεκτρονικού ταχυδρομείου αποκρυπτογραφείται από τους τοπικούς μας υπολογιστές και συσκευές. Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου που χρησιμοποιούνται πραγματοποιούνται μέσω των διακομιστών των παρόχων της Microsoft οι οποίοι συμμορφώνονται με τον κανονισμό GDPR. Η υπηρεσία Newsletter πραγματοποιείται μέσω των διακομιστών του πάροχου MAILCHIMP ο οποίος συμμορφώνεται με τον κανονισμό GDPR.

Microsoft (Πολιτική απορρήτου)
Mailchimp (Πολιτική απορρήτου)

Η ιστοσελίδα, οι email servers και ο newsletter server λειτουργούν σε περιβάλλον HTTPS:// με την κάλυψη ειδικού πιστοποιητικού SSL που αποδεικνύει ότι κρυπτογραφούνται όλα τα δεδομένα που διακινούνται μέσω της φόρμας επικοινωνίας.

Τηρείται η τακτική εφαρμογή των πιο πρόσφατων (και σταθερών) ενημερώσεων λογισμικού και ιδιαίτερα τα security updates, service packs και ασφαλείας όλου του συστήματος IT μας (η/υ γραφείων και servers).

Η παρακολούθηση (monitoring) της λειτουργίας των υπηρεσιών μας και η ανίχνευση κακόβουλων ενεργειών σε πραγματικό χρόνο (real-time), είναι

καταλυτική για την αποτροπή και την ανταπόκρισή μας σε περιστατικά ασφάλειας στους servers που φιλοξενούνται στο δίκτυό μας.

Ο διακομιστής της ιστοσελίδας και το δίκτυο του πάροχου προστατεύονται με τα παρακάτω μέτρα ασφαλείας:

- προστασία από DDOS επιθέσεις,
- προστασία από hackers, bots που προσπαθούν να αποκτήσουν πρόσβαση σε ιστότοπους
- προστασία από διασπορά spam, ιών & παραπλανητικών (phishing) email
- αυτόματη αποκατάσταση ευπαθειών σε εγκατεστημένα λογισμικά (πχ

Στο server της ιστοσελίδας, γίνεται συνεχής (σε 24ωρη βάση) αυτόματη εκτέλεση διεργασιών, που ελέγχουν για αποτυχίες ελέγχου ταυτότητας σύνδεσης (failed logins) και αποκλείονται προσωρινά ή μόνιμα οι IP διευθύνσεις από τις οποίες γίνονται οι απόπειρες σύνδεσης.

Στο server της ιστοσελίδας, εφαρμόζεται προγραμματισμένη και συστηματική λήψη αντιγράφων ασφαλείας (backup) για την επαναφορά τους μετά από τυχόν ξαφνική βλάβη. Εκτός από τις προγραμματισμένες και τακτικές λήψεις αντιγράφων ασφαλείας, γίνεται έκτακτη λήψη αντιγράφου δεδομένων.

21.12 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΕΞ'ΑΠΟΣΤΑΣΕΩΣ ΕΡΓΑΣΙΑΣ

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ λαμβάνοντας υπόψιν τις ιδιαίτερες συνθήκες λόγω COVID19 ορίζει και υποστηρίζει συγκεκριμένες διαδικασίες για την τηλεργασία. Οι διαδικασίες αυτές πρέπει να λαμβάνουν υπόψη, για την κάθε περίπτωση, τη φύση και τη σοβαρότητα των κινδύνων ως προς την προστασία προσωπικών δεδομένων, οι οποίοι απορρέουν από την εξ αποστάσεως εργασία. Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ ενημερώνει επαρκώς, εκπαιδεύει και συνδράμει τους εργαζομένους του στην εφαρμογή των διαδικασιών αυτών, λαμβάνοντας υπόψη ότι πολλοί χρήστες δεν είναι εξοικειωμένοι με τις τεχνολογίες που υποστηρίζουν την τηλεργασία και τους σχετικούς κινδύνους. Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ ΑΕ αναγνωρίζει ότι οι υποχρεώσεις των φορέων αναφορικά με την προστασία των προσωπικών δεδομένων των εργαζομένων τους αποκτούν ιδιάζουσα βαρύτητα στην περίπτωση της τηλεργασίας. Και τούτο, διότι ο εργαζόμενος, λόγω του γεγονότος ότι βρίσκεται στο σπίτι του, έχει μεγαλύτερη προσδοκία για την προστασία της ιδιωτικής του ζωής.

21.13 ΠΟΛΙΤΙΚΗ ΚΩΔΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Η ΙΚΤΙΝΟΣ ΕΛΛΑΣ έχει διασφαλίσει ότι υπάρχουν κατάλληλοι έλεγχοι κωδικού πρόσβασης για την προστασία εμπιστευτικών πληροφοριών.

<u>Πολιτική</u>

- Ισχυροί κωδικοί πρόσβασης απαιτούνται για οποιαδήποτε συστήματα που παρέχουν πρόσβαση σε περιορισμένα δεδομένα.

- Ισχυροί κωδικοί πρόσβασης συνιστώνται για οποιαδήποτε συστήματα που παρέχουν πρόσβαση σε εσωτερικά δεδομένα.

- Οι χρήστες δεν πρέπει να μοιράζονται κωδικούς πρόσβασης με κανέναν, συμπεριλαμβανομένων Διευθυντών και μελών του IT Τμήματος.

- Εάν ένας Χρήστης γνωρίζει ή έχει λόγο να πιστεύει ότι ένας κωδικός πρόσβασης έχει αποκαλυφθεί ή έχει αλλοιωθεί, ο κωδικός πρόσβασης πρέπει να αλλάξει ή να απενεργοποιηθεί αμέσως.

- Εάν οι κωδικοί πρόσβασης τεκμηριώνονται σε χαρτί, το χαρτί αυτό πρέπει να αποθηκεύεται σε ασφαλή κλειδωμένη θέση. Οι κωδικοί που αποθηκεύονται ηλεκτρονικά με κωδικό πρόσβασης ή κρυπτογραφημένα.

21.14 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ

Λαμβάνονται τακτικά αντίγραφα ασφαλείας των βασικών επιχειρησιακών πληροφοριών

Χρησιμοποιείται κατάλληλος κύκλος δημιουργίας αντιγράφων ασφαλείας, ο οποίος είναι επαρκώς τεκμηριωμένος (Πολιτική Αντιγράφων Ασφάλειας και Ανάκτησης Δεδομένων και Διαδικασία Λήψης Αντιγράφων Ασφάλειας).