Πολιτική Ορθής Χρήσης

Εταιρικών Ηλεκτρονικών Συσκευών, Δικτύου και Εφαρμογών

Έκδοση 1.0

20.01.2019

1. Γενικά

Η ΕΤΑΙΡΕΙΑ παρέχει στους εργαζόμενους κατάλληλο εξοπλισμό για την εκτέλεση της εργασίας τους (πχ σταθερό ηλεκτρονικό υπολογιστή και σταθερό τηλέφωνο) καθώς και υπηρεσίες ηλεκτρονικής αλληλογραφίας (e-mail), πρόσβαση στο διαδίκτυο και άλλες υποδομές, ενώ σε κάποιους εκ των εργαζομένων δίδεται και φορητός υπολογιστής και κινητό τηλέφωνο. Όλα τα ανωτέρω αποτελούν περιουσία της εταιρείας και δίδονται στους εργαζόμενους αποκλειστικά για την εκτέλεση των υπηρεσιών που ανέλαβαν κατά την πρόσληψη.

Η εταιρεία οφείλει να εξασφαλίζει ότι οι χρήστες της έχουν την κατάλληλη ενημέρωση για την σωστή και ασφαλή χρήση των συστημάτων στα οποία έχουν πρόσβαση.

2. Σκοπός

Η Πολιτική Ορθής Χρήσης καθορίζει τις υποχρεώσεις του οργανισμού αλλά και τις αρχές, τους κανόνες και τις συνέπειες για τους εργαζόμενους και συνεργάτες του, στους οποίους εκχωρείται το δικαίωμα πρόσβασης σε πληροφοριακά συστήματα και δεδομένα επικοινωνίας, και αποβλέπει στην αποτροπή καταχρηστικής άσκησης των δικαιωμάτων τους και της τέλεσης πράξεων που παραβιάζουν ή συνιστούν κίνδυνο παραβίασης των πληροφοριών που χρήζουν διαφύλαξης (προσωπικά, ευαίσθητα, άκρως ευαίσθητα - εμπιστευτικά δεδομένα του οργανισμού και των πελατών του)

3. Πεδίο Εφαρμογής

Η πολιτική εφαρμόζεται σε όλους τους εργαζομένους της ΕΤΑΙΡΕΙΑΣ.

4. Πολιτική

4.1 Γενικές Απαιτήσεις – Υποχρεώσεις

Οι εργαζόμενοι και συνεργάτες του οργανισμού οφείλουν να συμμορφώνονται με την Πολιτική Ορθής Χρήσης, συμπεριλαμβανομένων των σχετικών διαδικασιών, μέτρων ασφάλειας και οδηγιών.

Όλοι οι εργαζόμενοι και οι συνεργάτες του οργανισμού υπογράφουν σύμβαση συνεργασίας με την οποία εξασφαλίζεται ότι οι εργαζόμενοι και συνεργάτες του οργανισμού λαμβάνουν γνώση και έχουν αποδεχτεί την Πολιτική Ορθής Χρήσης ως προς την εργασία τους, προ της απόκτησης πρόσβασης σε πληροφοριακά αγαθά και σε δεδομένα επικοινωνίας.

Ο οργανισμός ενημερώνει με κάθε πρόσφορο μέσο και εκπαιδεύει τους εργαζόμενους και συνεργάτες του σχετικά με την εφαρμογή της Πολιτικής Ορθής Χρήσης για τη Διαχείριση των Πληροφοριών και τις τροποποιήσεις αυτής.

Οι εργαζόμενοι και συνεργάτες του οργανισμού, οι οποίοι αποκτούν πρόσβαση σε πληροφοριακά συστήματα και δεδομένα επικοινωνίας των πελατών δεν επιτρέπεται να αποκαλύπτουν οποιαδήποτε πληροφορία ή στοιχείο υποπίπτει στην αντίληψή τους ή την κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

Οι εργαζόμενοι και συνεργάτες του οργανισμού υποχρεούνται να ενημερώνουν άμεσα τον Υπεύθυνο Ασφαλείας των Πληροφοριών (Information Security Manager) σε περίπτωση που υποπέσει στην αντίληψή τους ένα κενό ασφάλειας ή σχετικό περιστατικό που θέτει σε κίνδυνο την εμπιστευτικότητα, την διαθεσιμότητα και την ακεραιότητα των πληροφοριών και των πληροφοριακών συστημάτων, όπου αυτή είναι αποθηκευμένη.

4.2 Πρόσθετες Απαιτήσεις Αναφορικά με τους Συνεργάτες

Ο οργανισμός διατηρεί ενημερωμένο αρχείο στο οποίο καταγράφονται οι συνεργάτες του, φυσικά ή νομικά πρόσωπα, οι οποίοι προκειμένου να παράσχουν τις υπηρεσίες τους, αποκτούν ή δύνανται να αποκτήσουν πρόσβαση σε πληροφοριακά συστήματα και δεδομένα επικοινωνίας των πελατών. Ο οργανισμός συνάπτει με τους συνεργάτες του, συμβάσεις, των οποίων το ελάχιστο περιεχόμενο περιλαμβάνει:

- Όρους εμπιστευτικότητας, μη αποκάλυψης και τήρησης του απορρήτου.
- Απαιτήσεις και μέτρα ασφάλειας που λαμβάνονται για τη διαχείριση της ακεραιότητας και της διαθεσιμότητας των πληροφοριών κατά την επεξεργασία αυτών από τους συνεργάτες του οργανισμού, καθώς και την οριστική διαγραφή και καταστροφή αυτών μετά τη λήξη της συνεργασίας.

Για κάθε παραβίαση των συμβατικών όρων που αναφέρονται στις παραγράφους, ο οργανισμός ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας.

4.3 Κανόνες Ορθής Χρήσης Πληροφοριακών και Επικοινωνιακών Συστημάτων

Σε περίπτωση παραβίασης των αποδεκτών κανόνων χρήσης, αυτός που διαπράττει την πράξη είναι προσωπικά υπεύθυνος για την δράση του ή την δράση που αναλαμβάνεται από άλλον, λόγω της παραβίασης των κανόνων αυτών.

Η έλλειψη γνώσης ή η εξοικείωση με τους κανόνες δεν απαλλάσσει τους εμπλεκόμενους από την ευθύνη αυτή και κάθε παραβίαση υπόκειται σε πειθαρχικό έλεγχο και κυρώσεις.

Οι ηλεκτρονικές πληροφορίες που χρησιμοποιούνται από το προσωπικό της εταιρείας στο πλαίσιο της επιχειρησιακής δραστηριότητας είναι ιδιοκτησία της εταιρείας αλλά και του υποκειμένου της επεξεργασίας και υπόκειται σε όλες τις πολιτικές, τις διαδικασίες, τους κανόνες προστασίας και τις αποδεκτές κατευθυντήριες γραμμές που διέπουν την λειτουργία της επιχείρησης και την Εθνική Νομοθεσία.

Απαγορεύεται κάθε δραστηριότητα ή πράξη η οποία στρέφεται κατά της επιχείρησης ή παραβιάζει την ασφάλεια ή την εμπιστευτικότητα των πληροφοριών που διαχειρίζεται. Παραδείγματα απαγορευμένων πράξεων περιλαμβάνουν:

- Εγκατάσταση (installation) νέων υπολογιστών ή αναβάθμιση (upgrading) χωρίς την προηγούμενη έγκριση του Υπεύθυνου Ασφάλειας των Πληροφοριών Συστημάτων και του Τεχνικού τμήματος

- Κατέβασμα (downloading) ή εγκατάσταση (installation) προγραμμάτων χωρίς την προηγούμενη έγκριση του Υπεύθυνου Ασφάλειας των Πληροφοριών Συστημάτων και του Τεχνικού τμήματος
- Χρήση σπασμένου ή χωρίς άδεια χρήσης, λογισμικού (unlicensed software)
- Χρήση προγραμμάτων ή ιστοσελίδων του διαδικτύου οι οποίες παραβιάζουν την ιδιωτικότητα των πελατών ή του προσωπικού.
- Απεγκατάσταση ή απενεργοποίηση ή παραβίαση του λογισμικού προστασίας (antivirus) ή των λοιπών εγκατεστημένων από την εταιρεία προγραμμάτων.
- Αυθαίρετη προσπάθεια για το σπάσιμο των κωδικών πρόσβασης.
- Μη εξουσιοδοτημένη πρόσβαση σε αρχεία, προγράμματα, βάσεις δεδομένων, εμπιστευτική πληροφορία ή δεδομένα προσωπικού χαρακτήρα (βασικά και ευαίσθητα).
- Η παρακώληση ή η άρνηση της συνεργασίας με τον Υπεύθυνο Ασφάλειας των Πληροφοριών Συστημάτων
- Η δημοσιοποίηση – καταγραφή σε οποιοδήποτε σημείο γύρω από την θέση εργασίας ή η κοινοποίηση των κωδικών χρήσης, σε άλλους. Οι χρήστες πρέπει να ασφαλίζουν τους κωδικούς χρήσης έτσι ώστε να μην είναι προσβάσιμοι σε οποιονδήποτε.
- Ο εταιρικός κωδικός πρόσβασης να είναι διαφορετικός από οποιονδήποτε άλλο χρησιμοποιείται για άλλες περιπτώσεις εκτός εταιρείας
- Χρήση εταιρικού εξοπλισμού ή εταιρικής υπηρεσίας (π.χ email) για μη επιχειρησιακές χρήσεις ή για προσωπικό όφελος.
- Η φυσική και η λογική πρόσβαση σε διαγνωστικές και configuration θύρες χωρίς προηγούμενη έγκριση υπευθύνου.
- Η αποστολή ευαίσθητης πληροφορίας μέσω ταχυδρομείου ή courier χωρίς προηγούμενη έγκριση υπευθύνου.
- Η τηλεφωνική συνομιλία σχετικά με ευαίσθητη ή άκρως ευαίσθητη πληροφορία, εάν υπάρχει στο χώρο κάποιος μη εξουσιοδοτημένος.
- Η αποστολή e-mail ή fax που περιλαμβάνει ευαίσθητη ή άκρως ευαίσθητη πληροφορία χωρίς προηγούμενη έγκριση υπευθύνου.
- Η αποστολή e-mail ή fax σε λάθος διεύθυνση.
- Η επίδοση φωτοτυπίας ή άλλου τύπου διαβαθμισμένης πληροφορίας σε μη εξουσιοδοτημένο πρόσωπο.
- Η εισαγωγή στον υπολογιστή συσκευών σε USB θύρες αν δεν έχουν λάβει έγκριση από τον υπεύθυνο του IT Υποδομών
- Η χρήση του εταιρικού Η/Υ από τρίτο πρόσωπο. Οι χρήστες προτείνεται να τον κλειδώνουν κάθε φορά που απομακρύνονται από αυτόν
- Η ανάρτηση περιεχομένου στο εταιρικό portal διαφορετικό από αυτό που συμφωνήθηκε με τον υπεύθυνο περιεχόμενου καθώς επίσης και κάθε μορφή αλλοίωσης περιεχομένου ή διαγραφής χωρίς προηγούμενη έγκριση από τον υπεύθυνο

4.4 Χρήση δικτύου διαβίβασης δεδομένων (LAN, WAN, Internet / Intranet / Extranet)

Οι ηλεκτρονικές υπηρεσίες που παρέχονται στοχεύουν στη διευκόλυνση και υποστήριξη των υπηρεσιών της ΕΤΑΙΡΕΙΑΣ και λαμβάνουν χώρα εντός της περιμέτρου της εταιρείας. Χρήστες των ηλεκτρονικών υπηρεσιών είναι μόνον όσοι λαμβάνουν άδεια πρόσβασης σε αυτές.

Τα προνόμια / πλαίσιο παραχώρησης του δικαιώματος χρήσης των ηλεκτρονικών υπηρεσιών παρέχεται από τη Γενική Διεύθυνση Οργάνωσης και Πληροφορικής. Η πρόσβαση των χρηστών στις ηλεκτρονικές υπηρεσίες διέπεται από τους ακόλουθους όρους και προϋποθέσεις:

- Κάθε μορφής πρόσβαση στο δίκτυο παρέχεται και ενεργοποιείται μετά από δηλωμένη συμφωνία του χρήστη με τους παρόντες κανόνες αποδεκτής χρήσης και οφείλει να ακολουθεί την "πολιτική ορθής χρήσης" όπως αυτή υιοθετήθηκε από το τμήμα IT

- Κάθε χρήστης είναι υπεύθυνος για τις δραστηριότητες κάθε μορφής πρόσβασης αυτού στο δίκτυο και οφείλει να λαμβάνει όλα τα ενδεικνυόμενα μέτρα για τη διασφάλιση του απορρήτου των επικοινωνιών του και της εμπιστευτικότητας των προσωπικών δεδομένων. Γενικά οφείλει να διασφαλίζει ότι οι υπηρεσίες χρησιμοποιούνται σύμφωνα με το νόμο, την καλή πίστη και τα χρηστά ήθη.

- Ο χρήστης δεν μεταδίδει ποτέ προσωπικές πληροφορίες χωρίς την επίσημη άδεια του υποκειμένου της πληροφορίας. Το επίθετο, όνομα ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου, οι ιατρικές εξετάσεις, κ.λπ.) περιλαμβάνονται σε αυτή την πληροφορία.

- Ο χρήστης υποχρεούται να μην προβεί σε ενέργειες που παραβιάζουν (με παραγωγή, δημοσίευση ή διακίνηση υλικού) τα προσωπικά δεδομένα (individual personal data) και τα πνευματικά δικαιώματα (copyrights) των δικαιούχων.

- Κάθε χρήστης είναι υπεύθυνος για τη σωστή σύνδεση του εξοπλισμού του με το δίκτυο σε συνεργασία με το Τεχνικό τμήμα το οποίο παρέχει τεχνικές συμβουλές και υποστήριξη για την αποκατάσταση συναφών δυσλειτουργιών.

- Είναι υποχρέωση του χρήστη να χειρίζεται και να χρησιμοποιεί τον κάθε είδους εξοπλισμό συστημάτων ή δικτύου που ανήκει στην εταιρεία με αυξημένη προσοχή ώστε να μην προκαλούνται ζημιές ή φθορές. Τυχόν ατυχήματα θα πρέπει να αναφέρονται άμεσα στο Τεχνικό τμήμα ώστε να αποκαθίστανται το συντομότερο δυνατό.

- Ο χρήστης οφείλει να χρησιμοποιεί το δίκτυο με τρόπο ώστε εν γνώσει του να μη δημιουργεί συνθήκες που σπαταλούν άσκοπα δικτυακούς πόρους ή εν γένει προκαλούν οποιαδήποτε δυσλειτουργία στο δίκτυο, ούτε και να προβαίνει σε παράνομες πράξεις.

- Υποχρεούται να ενημερώνει το Τεχνικό τμήμα για οποιαδήποτε αλλαγή στα δεδομένα των δικτυακών συνδέσεών του.

- Όσοι δικαιούνται πρόσβασης στο διαδίκτυο, δεν μπορούν να χρησιμοποιούν αυτό το δικαίωμα για την εκτέλεση κάθε παράνομης δραστηριότητας, όπως προσπάθεια να κερδίσουν την αναρμόδια πρόσβαση σε απαγορευμένες διευθύνσεις (hacking, cracking).

- Υποχρεούται να λαμβάνουν όλα τα ενδεικνυόμενα μέτρα για τη διασφάλιση του ιδιωτικού απορρήτου, όπως η απόκρυψη passwords, certificates και να αναφέρουν στον Υπεύθυνο

Ασφάλειας των Πληροφοριών Συστημάτων οποιαδήποτε απόπειρα υποκλοπής του συνθηματικού τους πέσει στην αντίληψή τους.

- Να επιλέγουν και να διαφυλάττουν ασφαλές συνθηματικό (strong password) για πρόσβαση στις δικτυακές υπηρεσίες σύμφωνα με την «διαδικασία δημιουργίας και διαχείρισης κωδικών πρόσβασης». Τα συνθηματικά χρήστη δεν πρέπει ποτέ να γράφονται σε χαρτί ή να αποθηκεύονται σε ηλεκτρονική μορφή, ούτε να δίνονται σε τρίτους. Εάν είναι δύσκολο ο χρήστης να θυμάται το κωδικό του και αναγκαστεί να τον γράψει, τότε να βεβαιωθεί ότι δεν τον έχει επισημάνει ως κωδικό πρόσβασης και να τον διατηρεί σε ασφαλές μέρος. Οι κωδικοί των χρηστών είναι αυστηρά προσωπικοί και απαγορεύεται η μεταβίβαση ή πώληση των δικαιωμάτων των χρηστών. Απαγορεύεται η χρήση πρόσφατων κωδικών στη διαδικασία αλλαγής τους.

- Ο χρήστης υποχρεούται να μην επιχειρεί να εκμεταλλευθεί πιθανά κενά ασφάλειας του δικτύου, να μην διαταράσσει την ομαλή λειτουργία αυτού, να μην εκτελεί οποιοδήποτε κακόβουλο λογισμικό και γενικά να αποφεύγει οποιαδήποτε ενέργεια που δύναται να θέσει σε κίνδυνο ή να υποβαθμίσει το επίπεδο ασφάλειας των πληροφοριακών συστημάτων και την εύρυθμη λειτουργία του.

- Ενθαρρύνεται η άμεση ενημέρωση του Τεχνικού τμήματος σχετικά με οποιαδήποτε μη φυσιολογική συμπεριφορά του υπολογιστικού του συστήματος ή του λογισμικού προστασίας.

- Απαγορεύεται ρητά η εγκατάσταση οποιουδήποτε συστήματος λογισμικού χωρίς την έγκριση του Τεχνικού τμήματος.

- Απαγορεύεται ρητά η οποιαδήποτε μεταβολή του τρόπου και των παραμέτρων λειτουργίας, χωρίς την πρωθύστερη σχετική έγκριση από το Τεχνικού τμήμα.

- Απαγορεύεται ρητά η κατοχή, χρήση και ανάπτυξη ιών ή άλλων επιβλαβών εφαρμογών.

- Η χρήση του δικτύου πρέπει να περιορίζεται μόνο σε ενέργειες και πράξεις που είναι αναγκαίες για την διεκπεραίωση των δραστηριοτήτων της επιχείρησης. Χρήση σε περιπτώσεις έκτακτης ανάγκης ή για τον έλεγχο των καιρικών συνθηκών μπορεί να θεωρηθεί αποδεκτή.

- Η αποδεκτή χρήση του δικτύου δεν περιλαμβάνει το παίξιμο παιχνιδιών στο προσωπικό υπολογιστή είτε στο internet και το registration σε chat rooms ή ιστοσελίδες χωρίς την έγγραφη άδεια του Υπεύθυνου Ασφάλειας Πληροφοριακών Συστημάτων.

- Απαγορεύεται η παρενόχληση με οποιαδήποτε μορφή, η δημιουργία χώρων παράνομου Intranet ή σελίδων, η ανταλλαγή (copyrighted) υλικού ή η παραγωγή οποιουδήποτε υλικού που μπορεί να κριθεί επιθετικό.

- Απαγορεύεται αυστηρά η χρήση του δικτύου για σκόπιμη εξάπλωση ιών λογισμικού οποιουδήποτε είδους και εφόσον διαπιστωθεί μπορεί να αυτό προκαλέσει πειθαρχικές κυρώσεις έως και τον τερματισμό της απασχόλησης.

- Το προσωπικό και οι συνεργάτες φέρουν την ευθύνη για την χρήση οποιουδήποτε πόρου χρησιμοποιούν και δεν μπορούν να χρησιμοποιήσουν πόρους της εταιρείας που ενδεχόμενα τους διατεθούν, για οποιαδήποτε παράνομη ανταλλαγή αρχείων.

- Λήψη κάθε μουσικής, βίντεο, πορνογραφικού υλικού ή λογισμικού αρχείων κατά παράβαση των νόμων περί πνευματικής ιδιοκτησίας καθώς και διακίνηση κάθε προσβλητικού, συκοφαντικού, δυσφημιστικού ή ρατσιστικού υλικού απαγορεύεται, και ο εργαζόμενος θα είναι προσωπικά υπεύθυνος για τυχόν πρόστιμα ή αποφάσεις που ενδέχεται να προκύψουν από την ενέργειά του.

- Απαγορεύεται η λήψη κάθε είδους λογισμικού, ψηφιακών εικόνων, μουσικής, streaming video ή άλλων δεδομένων που ενδεχόμενα μπορεί κάθε εργαζόμενος να κατεβάσει από το Internet (εξαιρούνται όσοι τους έχει χορηγηθεί η σχετική άδεια από το τμήμα IT Υποδομών σε συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφοριακών Συστημάτων).

- Απαγορεύεται κάθε προσπάθεια που συνιστά παραβίαση (επιτυχή ή μη) της ασφάλειας συστημάτων μέσα από το δίκτυο. Στα πλαίσια αυτά εντάσσονται και ενέργειες που υποβαθμίζουν το επίπεδο ασφάλειας ή την ακεραιότητα ενός οποιουδήποτε δικτύου ή συστήματος. Ενδεικτικά αναφέρεται ότι απαγορεύονται ρητά προσπάθειες (επιτυχείς ή μη) άρνησης παροχής υπηρεσιών (Denial of Service attacks), εξάπλωσης ιών ή άλλων βλαπτικών προγραμμάτων (malware) και αποστολής μαζικού ηλεκτρονικού ταχυδρομείου – Spam.

Κανένα ηλεκτρονικό δίκτυο δεν είναι απολύτως ασφαλές. Έτσι παρά τα μέτρα που λαμβάνονται, δεν μπορεί να αποκλεισθεί η πιθανότητα παραβίασης της ασφάλειας των συστημάτων του. Το Τμήμα Πληροφορικής της ΕΤΑΙΡΕΙΑΣ δεσμεύεται ότι θα διερευνά ενδελεχώς τέτοια περιστατικά προκειμένου να εντοπίσει τους πραγματικούς υπεύθυνους.

4.5 Χρήση ηλεκτρονικού ταχυδρομείου (e-mail)

Η επικοινωνία διέπεται από τους κανόνες και τους νόμους που διέπουν την προστασία της ιδιωτικής ζωής και το απόρρητο της επικοινωνίας. Συνεπώς απαγορεύεται η ηλεκτρονική αποστολή πληροφορίας (e-mail) που σχετίζεται με ευαίσθητα ή άκρως ευαίσθητα δεδομένα, μέσω του κοινού ηλεκτρονικού ταχυδρομείου χωρίς προηγούμενη έγκριση υπευθύνου.

Οι εμπιστευτικές πληροφορίες που διαβιβάζονται πρέπει να προστατεύονται επαρκώς. Αυτό επιτυγχάνεται μέσω της κρυπτογράφησης του μηνύματος έτσι ώστε το μήνυμα να μπορεί να αναγνωστεί μόνο από το αποδέκτη που διαθέτει το κατάλληλο κλειδί (encryption key) και κανέναν άλλο.

Όλες οι ηλεκτρονικές επικοινωνίες αποτελούν ιδιοκτησία της εταιρείας και δεν αποτελούν προσωπική περιουσία οποιουδήποτε μέλους της.

Όλοι οι χρήστες είναι υπεύθυνοι για τη διασφάλιση της συμμόρφωσης και το σεβασμό των νομικών διατάξεων για την προστασία του απορρήτου των επικοινωνιών και της διασφάλισης των προσωπικών δεδομένων που ενδεχομένως να έχουν πρόσβαση.

Απαγορεύεται το άνοιγμα συνημμένων (attachments) σε e-mail τα οποία είναι ακατάλληλα ή από άγνωστο αποστολέα. Στη περίπτωση που ληφθεί κάποιο e-mail από ένα άγνωστο αποστολέα ή ένα αποστολέα ο οποίος θεωρείται ύποπτος, δεν ανοίγουμε τα επισυναπτόμενα αρχεία ΚΑΙ ενημερώνουμε τον Υπεύθυνο Ασφαλείας Πληροφοριακών Συστημάτων. Εάν αποφασιστεί αρχικά να μην διαγραφεί το μήνυμα αλλά να σκαναριστεί το συνημμένο, τότε εάν ανιχνευτεί κακόβουλο λογισμικό, το μήνυμα διαγράφεται από τα εισερχόμενα αλλά και από τα διαγραμμένα.

Δεν ακολουθούμε υπερσυνδέσεις (hyperlinks) οι οποίες επισυνάπτονται σε e-mails, εάν ο αποστολέας δεν είναι έμπιστος. Σε κάθε περίπτωση ελέγχουμε τα επισυναπτόμενα πριν τα ανοίξουμε.

Δεν συμμετέχουμε στην δημιουργία, αποστολή και διαβίβαση "chain-mail" (αλυσιδωτά μηνύματα που προωθούνται από χρήστη σε χρήστη) και δεν απαντάμε ποτέ στα spam e-mails (ανεπίκλητα) ούτε και στην υποτιθέμενη ένδειξη διαγραφής, γιατί έτσι διαπιστώνεται η εγκυρότητα της ηλεκτρονικής μας διεύθυνσης και επομένως θα αποτελούμε πολύτιμο στόχο για τους ειδικούς σκάνερ (spammers). Επίσης τέτοιες κινήσεις είναι επικίνδυνες στην είσοδο ή την διάδοση ενός μολυσμένου μηνύματος. Σε περίπτωση ανίχνευσης ενός τέτοιου e-mail διαγράφουμε το e-mail όχι μόνο από τα εισερχόμενα αλλά και από διαγραμμένα. Πρέπει να γνωρίζουμε ότι απαγορεύεται και διώκεται ποινικά η σκόπιμη διάδοση spam e-mails.

Η χρήση instant messaging (άμεση αποστολή μηνυμάτων) μέσω των εφαρμογών που παρέχουν παράλληλα τη δυνατότητα μετάδοσης φωνής ή / και εικόνας (πχ. Skype, yahoo business manager, ICQ, MSN messenger, Viber) και άλλων επικοινωνιών από το προσωπικό (πχ. κλήση από PC σε τηλέφωνο, από τηλέφωνο σε PC) συμπεριλαμβανομένων και των γραπτών μηνυμάτων, αποτελούν κινήσεις επικίνδυνες για την είσοδο ή την διάδοση ενός μολυσμένου μηνύματος, συνεπώς απαγορεύονται. Εξαιρείται το Cisco Jabber που παρέχει η εταιρεία

Απαγορεύεται η αποστολή e-mail ή άλλων ηλεκτρονικών επικοινωνιών, με απόκρυψη ή αποστολή αντ' αυτού ή αποστολή με προσπάθεια παραποίησης της ταυτότητας του χρήστη.

Δεν επιτρέπεται η χρήση περιπλεκτών (scramblers), re-mailer υπηρεσιών, ή άλλων σχετικών υπηρεσιών – κρυπτογραφικών εργαλείων που δεν είναι αποδεκτοί ή / και εγκεκριμένοι από τον οργανισμό.

Επικοινωνούμε πάντα τηλεφωνικά με τον αποδέκτη/αποστολέα της αλληλογραφίας αν πρόκειται για επαλήθευση/επιβεβαίωση τραπεζικού λογαριασμού ή αλλαγή αυτού

4.6 Ασύρματη πρόσβαση και ασύρματες συσκευές

Κανένας εργαζόμενος δεν μπορεί να επωφεληθεί της ασύρματης επικοινωνίας (εταιρικό ασύρματο δίκτυο) χωρίς την έγκριση του υπεύθυνου IT υποδομών. Η πρόσβαση στο τοπικό δίκτυο περιορίζεται στους εργαζόμενους και τους συνεργάτες που έχουν σχετική έγκριση.

Οι ασύρματες συσκευές που χρησιμοποιούνται πρέπει να ανήκουν στην εταιρεία και να πληρούν τις προδιαγραφές της ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων), δηλ. της Ανεξάρτητης Εθνικής Αρχής η οποία ελέγχει, ρυθμίζει και εποπτεύει την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου.

Οι έχοντες το δικαίωμα πρόσβασης δεν παραχωρούν τους κωδικούς πρόσβασης σε οποιοδήποτε εξωτερικό ή εσωτερικό συνεργάτη ενδιαφερθεί και ζητήσει πρόσβαση (χωρίς την έγκριση του Υπεύθυνου Ασφαλείας Πληροφοριακών Συστημάτων).

Ο κωδικός πρόσβασης πρέπει να πληροί τις προδιαγραφές που προβλέπονται από την πολιτική και την διαδικασία ελέγχου πρόσβασης της εταιρείας.

Δεν επιτρέπεται απομακρυσμένη πρόσβαση στο δίκτυο LAN, WAN, η οποιασδήποτε εφαρμογής λογισμικού, εάν ο εργαζόμενος δεν έχει έγκριση..

Αποφεύγουμε να συνδεόμαστε σε ασύρματα δίκτυα που δεν είναι ασφαλή και δεν κάνουν χρήση κλειδιού με αλγόριθμο κρυπτογράφησης WPA2. Αν χρειαστεί να συνδεθούμε δεν κάνουμε πλοήγηση σε sites που δεν είναι ασφαλή (http) παρά μόνο σε αυτά που είναι secure (https) και γενικά αποφεύγουμε σύνδεση σε sites που απαιτούν χρήση username/password.

Αποφεύγουμε τη χρήση ξένου Η/Υ για να εισέρθουμε σε sites της εταιρείας ή σύνδεση σε αυτή. Αυτές οι συνδέσεις θα γίνονται αποκλειστικά από προσωπικό σας ή εταιρικό Η/Υ (ασύρματα ή ενσύρματα)

4.7 Εγκατάσταση λογισμικού

Κανένας υπολογιστής δεν πρέπει να συνδέεται στο δίκτυο εάν δεν πρόκειται να χρησιμοποιηθεί για επιχειρησιακή δραστηριότητα.

Το λογισμικό που συνδέεται στο δίκτυο πρέπει να είναι κατάλληλα διαμορφωμένο, οι πληροφορίες να προστατεύονται και να ελέγχονται ώστε να μην τεθεί σε κίνδυνο η ακεραιότητά, η εμπιστευτικότητα και η διαθεσιμότητά τους.

4.8 Αποδεκτή χρήση κινητού εξοπλισμού

Το προσωπικό φέρει προσωπικά την ευθύνη για κάθε σταθερό ή φορητό υπολογιστή ή εξοπλισμό ή παρελκυόμενο (accessory) το οποίο ήθελε κλαπεί κατά την διάρκεια που ευρίσκεται υπό την εποπτεία του.

Παρακάτω ακολουθούν μερικές συμβουλές για το πώς το προσωπικό θα προστατεύει τον εξοπλισμό του.

- Μην αφήνετε το φορητό υπολογιστή αφύλακτο ή σε ακλείδωτο όχημα ακόμη και εάν το όχημα είναι παρκαρισμένο στο γκαράζ
- Ποτέ μην το αφήνετε το φορητό υπολογιστή σε άμεση θέα
- Εάν υπάρχει ανάγκη να το αφήσετε στο αυτοκίνητό, είναι καλύτερο να είναι σε κλειδωμένο ντουλάπι ή στο port baggage ή σκεπασμένο με κλειδωμένες τις πόρτες
- Εξαιρετικά υψηλές θερμοκρασίες ή ισχυρά ηλεκτρομαγνητικά πεδία μπορεί να καταστρέψουν τον υπολογιστή
- Όταν ταξιδεύετε, μεταφέρετε τον υπολογιστή σας σε μια σκούρα θήκη ή σε τσάντα.
- Μην αφήνετε τον υπολογιστή σας όταν αποχωρείτε από μια αίθουσα συνεδριάσεων, πάρτε τον μαζί σας
- Μην δίνεται τον υπολογιστή σαν αποσκευή στα ταξίδια
- Εάν χρησιμοποιήσετε τον υπολογιστή σας στο σπίτι, φροντίστε να έχετε λάβει κάθε μέτρο για την προστασία του (πχ να βρίσκεται σε αρχειοθήκη που να κλειδώνει, να έχει γνωστοποιηθεί στο γραφείο και να υπάρχει προστασία της επικοινωνίας σε περίπτωση διασύνδεσης με το τοπικό δίκτυο)
- Η ασφαλιστική κάλυψη πρέπει να προστατεύει τον εξοπλισμό εκτός χώρων εργασίας.
- Εάν διαπιστώσετε κλοπή αναφέρεται αμέσως την κλοπή
- Να είναι κρυπτογραφημένα τα αρχεία στον υπολογιστή

4.9 Άλλες υποχρεώσεις System Administrator

- Ελέγχεται καθημερινά το λογισμικό προστασίας προκειμένου αυτό να λειτουργεί συνεχώς και αποτελεσματικά (antivirus logs, statistics).
- Αν δεν είναι εφικτή η αφαίρεση της μόλυνσης:
    - τα υπολογιστικά συστήματα στα οποία ανιχνεύεται κάποιος ιός ή άλλο κακόβουλο λογισμικό, απομονώνονται άμεσα από το δίκτυο της εταιρείας και παραμένουν εκτός δικτύου μέχρι την οριστική αντιμετώπιση,
    - το προσβεβλημένο αρχείο απομακρύνεται από το σύστημα και αντίγραφό του αποστέλλεται στην κατασκευάστρια εταιρεία του ειδικού λογισμικού προστασίας.
- Ελέγχεται η εγκυρότητα των στοιχείων ενημέρωσης του λογισμικού προτού εγκατασταθούν στο σύστημα και εγκαθίστανται οι Νομίμως διαθέσιμες ενημερώσεις ακολουθώντας τα βήματα που καθορίζονται από τον οίκο – νόμιμο προμηθευτή του λογισμικού. Αν απαιτούνται αλλαγές στις "default" ρυθμίσεις του λογισμικού, ώστε να καλυφθούν με καλύτερο τρόπο οι ανάγκες της εταιρείας και να βελτιωθεί η χρήση του, γίνεται η αλλαγή της αντίστοιχης ρύθμισης του λογισμικού και εγκαθίστανται τα αντίστοιχα patches, μόνο εάν η προέλευσή τους είναι νομίμως διαθέσιμη. Δεν εγκαθίστανται ποτέ, s/w patches από άγνωστες πηγές.

4.10 Πρόσβαση και έλεγχος των εταιρικών ηλεκτρονικών συσκευών

Η ΕΤΑΙΡΕΙΑ δικαιούται να προβεί σε έλεγχο των δεδομένων που αποθηκεύονται σε εταιρική ηλεκτρονική συσκευή εργαζόμενου, στην περίπτωση που η εν λόγω πρόσβαση και ο έλεγχος των δεδομένων αυτών είναι απολύτως αναγκαία για την ικανοποίηση έννομου συμφέροντος της εταιρείας (π.χ. έλεγχος διαρροής τεχνογνωσίας, εμπιστευτικών πληροφοριών ή

εμπορικών/επιχειρηματικών απορρήτων) υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων του εργαζομένου, χωρίς, σε καμία περίπτωση, να θίγονται οι θεμελιώδεις ελευθερίες αυτού. Η ΕΤΑΙΡΕΙΑ δικαιούται σε περίπτωση που για λόγους ασφαλείας διενεργείται έλεγχος σε δεδομένα προσωπικού χαρακτήρα, να αρνηθεί προσωρινά την πρόσβαση του εργαζόμενου στα δεδομένα αυτά μέχρι το πέρας του ελέγχου, προκειμένου να μην αλλοιωθεί το αποτέλεσμα της έρευνας.

Οι ειδικότερες διαδικασίες περιγράφονται επακριβώς στην Πολιτική πρόσβασης και ελέγχου των εταιρικών ηλεκτρονικών συσκευών που χρησιμοποιούν οι εργαζόμενοι.

5. Συμμόρφωση με την πολιτική

Ο Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων και ο Εσωτερικός Έλεγχος θα επαληθεύσει τη συμμόρφωση με την πολιτική αυτή με διάφορους τρόπους όπως, μέσα από συστήματα παρακολούθησης της κίνησης των δεδομένων και άλλους.

Οποιαδήποτε εξαίρεση στην παραπάνω πολιτική θα πρέπει να επαληθεύεται από τον **Υπεύθυνο Ασφάλειας Πληροφοριακών Συστημάτων** προκειμένου να δώσει συγκεκριμένες οδηγίες και κατευθύνσεις

6. Σχετικά Πρότυπα, Πολιτικές και Διαδικασίες

- Εταιρική Πολιτική Προστασίας Δεδομένων

7. Ορισμοί - Ορολογία