PHOENIX TOWER
INTERNATIONAL

# PHOENIX TOWER INTERNATIONAL, ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

*ΙΣΧΥΕΙ ΑΠΟ 15 ΑΥΓΟΥΣΤΟΥ 2023*

## ΣΚΟΠΌΣ

Η Phoenix Tower US Holdings, L.P. και τα παραρτήματα και θυγατρικές της παγκοσμίως (συλλογικά αναφερόμενες ως «PTI», «Phoenix Tower» ή «Εταιρεία»), δεσμεύονται για την προστασία της ασφαλείας των πληροφοριών και τη συνεχή μάθηση και βελτίωση, όπως ορίζεται στην παρούσα Πολιτική Ασφαλείας Πληροφοριών (η «Πολιτική»). Το πεδίο εφαρμογής της παρούσας πολιτικής προορίζεται να είναι περιεκτικό και θα περιλαμβάνει τις απαιτήσεις της Εταιρείας για την ασφάλεια και την προστασία των περιουσιακών στοιχείων της PTI, συμπεριλαμβανομένων των προσωπικών πληροφοριών που μπορούν να ταυτοποιηθούν («PII»), σε όλη την Εταιρεία και τους εγκεκριμένους προμηθευτές της τόσο εντός όσο και εκτός των χώρων εργασίας. Όλοι οι εργαζόμενοι πρέπει να εξετάζουν και να ακολουθούν τις πληροφορίες που περιέχονται στην παρούσα Πολιτική.

## ΠΕΔΊΟ ΕΦΑΡΜΟΓΉΣ

Η παρούσα πολιτική ισχύει για όλους τους εργαζομένους της Phoenix Tower και τους προμηθευτές που υποστηρίζουν ή αλληλεπιδρούν με την Phoenix Tower και τα περιουσιακά στοιχεία πληροφοριών της. Κάθε τμήμα της παρούσας πολιτικής εφαρμόζεται σε συγκεκριμένες πτυχές του προγράμματος ασφαλείας πληροφοριών της PTI.

## ΟΡΙΣΜΟΊ

- **Εμπιστευτικές Πληροφορίες: περιλαμβάνουν αλλά δεν περιορίζονται σε** όλες τις υλικές, μη δημόσιες, επιχειρηματικές πληροφορίες, δικαιώματα πνευματικής ιδιοκτησίας, εμπορικά μυστικά, επιχειρηματική τεχνογνωσία, είτε σε γραπτή είτε σε προφορική μορφή, είτε επισημαίνονται ως τέτοιες είτε όχι, σχετικά με θέματα όπως η επιχειρηματική στρατηγική, οι διαδικασίες, τα οικονομικά, τα σχέδια μάρκετινγκ, οι συμβάσεις και/ή η τεχνολογία. Παραδείγματα περιλαμβάνουν, μεταξύ άλλων:
  - Συμβάσεις, τόσο εκτελεσμένες όσο και στο στάδιο του σχεδιασμού·
  - Υλικό μάρκετινγκ υπό ανάπτυξη· ή
  - Προβλέψεις πωλήσεων ή εσόδων.
- **Ασφάλεια πληροφοριών:** οι διαδικασίες και οι μεθοδολογίες που σχεδιάζονται και εφαρμόζονται για την προστασία εκτυπωμένων, ηλεκτρονικών ή οποιασδήποτε άλλης μορφής εμπιστευτικών, ιδιωτικών ή ευαίσθητων πληροφοριών ή δεδομένων από μη εξουσιοδοτημένη πρόσβαση, χρήση, κατάχρηση, αποκάλυψη, καταστροφή, τροποποίηση ή διατάραξη.
- **Εργαζόμενος:** ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο που ενεργεί ως διευθυντής, αξιωματούχος, μέλος της ομάδας, εργαζόμενος, εργολάβος ή σύμβουλος της PTI, με πλήρη ή μερική απασχόληση, σε προσωρινή ή μόνιμη βάση.
- **Συσκευές για τον Τελικό Χρήστη:** κάθε τεχνολογικό εργαλείο ή συσκευή που

χρησιμοποιείται από έναν υπάλληλο της PTI για την αποθήκευση πληροφοριών ή την πρόσβαση στα συστήματα της PTI, συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου. Παραδείγματα συσκευών για τον τελικό χρήστη περιλαμβάνουν υπολογιστές, φορητούς υπολογιστές, έξυπνα τηλέφωνα, εξωτερικούς σκληρούς δίσκους και συσκευές αποθήκευσης USB.

- **Προσωπικά Ταυτοποιήσιμες Πληροφορίες («PII»):** οποιαδήποτε δεδομένα που θα μπορούσαν δυνητικά να ταυτοποιήσουν ένα συγκεκριμένο άτομο, όπως όνομα, διεύθυνση, ηλεκτρονικό ταχυδρομείο, οικονομικές πληροφορίες, αριθμός κοινωνικής ασφάλισης, αριθμός διαβατηρίου κ.λπ.

## ΕΠΟΠΤΕΊΑ ΠΟΛΙΤΙΚΉΣ

Η Phoenix Tower θεωρεί την Ασφάλεια Πληροφοριών ως μία από τις σημαντικότερες πτυχές της επιχείρησής της.

- Η ανώτερη διοίκηση της Phoenix Tower θα δώσει το παράδειγμα, διασφαλίζοντας ότι η ασφάλεια των πληροφοριών αποτελεί υψηλή προτεραιότητα σε όλες τις τρέχουσες και μελλοντικές επιχειρηματικές δραστηριότητες και πρωτοβουλίες.
- Η παρούσα Πολιτική και κάθε ένα από τα παραρτήματά της θα επανεξετάζονται ετησίως από τον Παγκόσμιο Γενικό Σύμβουλο, ώστε να διασφαλίζεται ότι είναι συναφείς και ενημερωμένες και θα αναθεωρούνται, εφόσον απαιτείται, ώστε να διασφαλίζεται ότι είναι επαρκείς υπό το πρίσμα των εξελισσόμενων νομικών υποχρεώσεων, της τεχνολογίας και των επιχειρηματικών αναγκών.
- Η διοίκηση θα κοινοποιεί τις αναθεωρήσεις της πολιτικής σε όλο το προσωπικό με διάφορα μέσα, όπως ηλεκτρονικές ενημερώσεις, ενημερώσεις, εκπαίδευση, ενημερωτικά δελτία κ.λπ.

Για την επίτευξη ή την υπέρβαση αυτών των στόχων, έχουν εφαρμοστεί οι ακόλουθες πρακτικές:

- Οι εργαζόμενοι υπογράφουν ειδοποίηση παραλαβής, εξέτασης και αναγνώρισης της Πολιτικής Ασφαλείας Πληροφοριών κατά την πρόσληψη/απασχόληση.
- Η ευαισθητοποίηση του προσωπικού θα ενισχύεται περιοδικά, ώστε τα θέματα ασφαλείας πληροφοριών να αποτελούν προτεραιότητα.
- Η εκπαίδευση στην Ασφάλεια Πληροφοριών είναι υποχρεωτική από την αρχή, ξεκινώντας από την ένταξη των εργαζομένων. Οποιαδήποτε τεχνική κατάρτιση θα πρέπει να είναι σχετική με τις αρμοδιότητες της θέσης εργασίας. Όταν τα μέλη του προσωπικού αλλάζουν θέσεις εργασίας ή καθήκοντα, οι ανάγκες τους για την Ασφάλεια Πληροφοριών πρέπει να επανεκτιμώνται και η νέα εκπαίδευση πρέπει να παρέχεται κατά προτεραιότητα.

## 1. ΟΡΓΑΝΩΣΗ ΑΣΦΑΛΕΙΑΣ

1.1 ΟΡΙΣΜΟΣ ΡΟΛΩΝ ΚΑΙ ΕΥΘΥΝΩΝ

Οι ακόλουθοι ρόλοι καθορίζονται στην PTI σχετικά με την ασφάλεια πληροφοριών:

| **ΡΟΛΟΙ** | **ΕΥΘΥΝΕΣ** |
|---|---|
| Διευθυντής Πληροφορικής | Καθορίζει τις απαιτήσεις ασφαλείας των παρεχόμενων υπηρεσιών με την αξιολόγηση των επιπτώσεων ενός περιστατικού που επηρεάζει την ασφάλεια των υπηρεσιών σε βάρος της διαθεσιμότητας, της αυθεντικότητας, της ακεραιότητας, της εμπιστευτικότητας ή της ιχνηλασιμότητας. |
| Διευθυντής Πληροφορικής | Καθορίζει τις απαιτήσεις ασφαλείας των πληροφοριών που υποβάλλονται σε επεξεργασία, με την αξιολόγηση των επιπτώσεων που θα είχε ένα περιστατικό που επηρεάζει την ασφάλεια των πληροφοριών στη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα, την εμπιστευτικότητα ή την ιχνηλασιμότητα. |
| Διευθυντής Πληροφορικής | Καθορίζει τις αποφάσεις για την ικανοποίηση των απαιτήσεων ασφαλείας πληροφοριών και υπηρεσιών, επιβλέποντας την εφαρμογή των αναγκαίων μέτρων και συντάσσοντας εκθέσεις σχετικά με τα θέματα αυτά. |
| Sr Διευθυντής Πληροφορικής | Υπεύθυνος για την ανάπτυξη του συγκεκριμένου τρόπου εφαρμογής της ασφαλείας στα συστήματα και για την εποπτεία της καθημερινής λειτουργίας των συστημάτων, και μπορεί να αναθέτει αρμοδιότητες σε διαχειριστές ή χειριστές υπό την ευθύνη του. |
| Sr Διευθυντής Πληροφορικής | Υπεύθυνος για τα τεχνικά καθήκοντα ασφαλείας, ο οποίος τα εκτελεί. |

## 2. ΠΡΟΣΩΠΙΚΆ ΑΝΑΓΝΩΡΊΣΙΜΕΣ ΠΛΗΡΟΦΟΡΊΕΣ

Αυτή η ενότητα έχει ως στόχο να καθοδηγήσει την προστασία των PII που συλλέγονται από Ιδιοκτήτες, Ενοικιαστές, πελάτες πωλήσεων και Εργαζομένους και θα βοηθήσει τους εργαζομένους να καθορίσουν ποιες πληροφορίες μπορούν να κοινοποιηθούν σε μη Εργαζομένους, καθώς και τη σχετική ευαισθησία των πληροφοριών που δεν θα κοινοποιηθούν εκτός την Phoenix Tower χωρίς την κατάλληλη εξουσιοδότηση.

## 2.1 Ορισμοί

Η Phoenix Tower αναγνωρίζει την ανάγκη να διατηρήσει την εμπιστευτικότητα των PII και κατανοεί ότι οι πληροφορίες αυτές είναι μοναδικές για κάθε άτομο και γενικά περιορίζονται σε δεδομένα που είναι σχετικά και απαραίτητα για τους σκοπούς της. Οι PII που καλύπτονται από την παρούσα Πολιτική μπορεί να προέρχονται από διάφορους τύπους ατόμων που εκτελούν καθήκοντα για λογαριασμό της Εταιρείας και περιλαμβάνουν Εργαζομένους, αιτούντες/υποψήφιους, ανεξάρτητους εργολάβους και οποιεσδήποτε PII που διατηρούνται για την πελατειακή βάση της. Οι PII περιλαμβάνουν όλες τις αναγνωρίσιμες πληροφορίες σχετικά με τους Ιδιοκτήτες, τους Ενοικιαστές, τους πελάτες πωλήσεων και τους Εργαζομένους:

- Προσωπικά στοιχεία επικοινωνίας (αριθμοί τηλεφώνου, διευθύνσεις κ.λπ.)·
- Αριθμούς Κοινωνικής Ασφάλισης (ή τους αντίστοιχους αυτών που εκδίδονται από κυβερνητικούς φορείς εκτός των Ηνωμένων Πολιτειών)·
- Αριθμούς Φορολογικού Μητρώου (ή τους αντίστοιχους αυτών που εκδίδονται από κυβερνητικούς φορείς εσόδων εκτός των Ηνωμένων Πολιτειών)·
- Αριθμούς Αναγνώρισης Εργοδότη (ή τους αντίστοιχους αυτών που εκδίδονται από κυβερνητικούς φορείς εκτός των Ηνωμένων Πολιτειών)·
- Αριθμούς κρατικών ή αλλοδαπών αδειών οδήγησης ή αντίγραφα δελτίων ταυτότητας·
- Αριθμούς διαβατηρίων ή αντίγραφα διαβατηρίων·
- Ημερομηνίες γέννησης·
- Εταιρικούς ή ατομικούς αριθμούς πιστωτικών ή χρεωστικών καρτών συναλλαγών (συμπεριλαμβανομένων των αριθμών PIN ή πρόσβασης) που διατηρούνται σε οργανωτικά αρχεία ή σε αρχεία εγκεκριμένων προμηθευτών· ή
- Πληροφορίες τραπεζικών λογαριασμών της PTI ή των επιχειρηματικών της εταίρων.

Οι PII μπορεί να βρίσκονται σε έντυπα ή ηλεκτρονικά αρχεία· και οι δύο μορφές των PII εμπίπτουν στο πεδίο εφαρμογής της παρούσας Πολιτικής.

## 2.2 Αποθήκευση και Χειρισμός Πληροφοριών που Περιέχουν PII

### *Ηλεκτρονικές PII*

Οι PII μπορούν να αποθηκευτούν ηλεκτρονικά με διάφορες μεθόδους και σε διάφορες συσκευές για τον τελικό χρήστη, όπως ενδεικτικά οι ακόλουθες:

- Κινητές υπολογιστικές συσκευές (π.χ. φορητοί υπολογιστές, έξυπνα τηλέφωνα, ταμπλέτες, υπολογιστές, PDA κ.λπ.).
- Προγράμματα ηλεκτρονικού ταχυδρομείου, διαδικτύου και άμεσων μηνυμάτων που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα.
- Τα αφαιρούμενα ηλεκτρονικά μέσα, όπως μονάδες USB, μονάδες CD, εξωτερικοί σκληροί δίσκοι κ.λπ., θα πρέπει να χρησιμοποιούνται μόνο για μη ευαίσθητες PII.

Ευαίσθητες PII, όπως αριθμοί κοινωνικής ασφάλισης, πληροφορίες διαβατηρίου και τραπεζικά ή άλλα οικονομικά δεδομένα δεν πρέπει να αποθηκεύονται σε αφαιρούμενα ηλεκτρονικά μέσα.
- Τοπικοί διακομιστές και διακομιστές Νέφους που ανήκουν στην PTI.
- Διακομιστές με βάση νέφος τρίτων μερών.

Η παρούσα ενότητα Πολιτικής καθορίζει τις απαιτήσεις και τη διαδικασία έγκρισης για τις Συσκευές Για τον Τελικό Χρήστη και οι οποίες ανήκουν, τις διαχειρίζεται ή τις χρονομισθώνει η PTI. Οποιαδήποτε Συσκευή Για τον Τελικό Χρήστη που δεν ανήκει, δεν την χρονομισθώνει ή δεν την διαχειρίζεται η PTI δεν επιτρέπεται να έχει πρόσβαση ή να αφαιρεί τοπικούς διακομιστές που περιέχουν PII, εκτός εάν έχει εγκριθεί εγγράφως από τον Παγκόσμιο Γενικό Σύμβουλο.

- **Φορητές υπολογιστικές συσκευές (δηλαδή φορητοί υπολογιστές, έξυπνα τηλέφωνα, υπολογιστές ταμπλέτας, PDA κ.λπ.)** - Οι PII μπορούν να αποθηκεύονται σε φορητές υπολογιστικές συσκευές, αλλά οι συσκευές αυτές θα πρέπει να προστατεύονται με κωδικό πρόσβασης, να κρυπτογραφούνται και να διαθέτουν δυνατότητες απομακρυσμένης διαγραφής. Αυτή δεν είναι η προτιμώμενη μέθοδος αποθήκευσης PII και οι πληροφορίες που είναι αποθηκευμένες σε φορητές υπολογιστικές συσκευές θα πρέπει να θεωρούνται ως χώρος προσωρινής αποθήκευσης και οι PII θα πρέπει να μεταφέρονται σε διακομιστή της PTI το συντομότερο δυνατό.
- **Ηλεκτρονικό ταχυδρομείο, διαδίκτυο και προγράμματα ανταλλαγής άμεσων μηνυμάτων -** Η Εταιρεία δεν συνιστά τη διαβίβαση PII μέσω του διαδικτύου ή προγραμμάτων ανταλλαγής άμεσων μηνυμάτων. Όταν πρόκειται να διαβιβαστούν οι PII μέσω ηλεκτρονικού ταχυδρομείου, πρέπει να λαμβάνονται τα ακόλουθα μέτρα για να διασφαλιστεί η ασφαλής διαβίβαση και να ελαχιστοποιηθεί ο κίνδυνος παραβίασης μετά την επιβεβαίωση ότι οι εν λόγω PII έχουν αποθηκευτεί στον τοπικό διακομιστή:
    1. Προστασία του εγγράφου με κωδικό πρόσβασης, είτε πρόκειται για pdf, word ή excel. Εάν το έγγραφο είναι σε μορφή που δεν προστατεύεται εύκολα (π.χ. gif ή jpeg), μετατρέψτε το έγγραφο σε αρχείο pdf, προστατέψτε το με κωδικό πρόσβασης σε αυτή τη μορφή και αποθηκεύστε το ξανά. Η «αρχική» μορφή μπορεί να διαγραφεί αυτή τη στιγμή και να αφαιρεθεί από τον κάδο απορριμμάτων.
    2. Στείλτε το έγγραφο με το ηλεκτρονικό ταχυδρομείο με την ένδειξη «**ΕΜΠΙΣΤΕΥΤΙΚΟ**» ως ετικέτα μετά το θέμα
    όνομα στη γραμμή θέματος.
    3. Επικοινωνήστε τηλεφωνικά με τον παραλήπτη για να επιβεβαιώσετε ότι ο παραλήπτης έλαβε το μήνυμα ηλεκτρονικού ταχυδρομείου και να του δώσετε τον κωδικό πρόσβασης. ***ΜΗΝ ΣΤΕΛΝΕΤΕ ΠΟΤΕ ΤΟΝ ΚΩΔΙΚΟ ΠΡΟΣΒΑΣΗΣ ΜΕ ΜΗΝΥΜΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ***
    4. Διαγράψτε το συνημμένο από το αποσταλμένο μήνυμα ηλεκτρονικού ταχυδρομείου.

Οι ευαίσθητες PII, όπως Αριθμοί Κοινωνικής Ασφάλισης, Πληροφορίες Διαβατηρίου και τραπεζικά ή άλλα οικονομικά δεδομένα **δεν** πρέπει να διαβιβάζονται με ηλεκτρονικό ταχυδρομείο.

Εάν η PTI λάβει οποιεσδήποτε PII μέσω διαδικτύου ή προγραμμάτων άμεσων μηνυμάτων ή οποιουδήποτε άλλου μη ασφαλούς μέσου, οι πληροφορίες θα πρέπει να διαβιβασθούν αμέσως στον διακομιστή της PTI (πρώτη προτίμηση) ή να διαβιβασθούν στην αποθήκευση μιας κινητής υπολογιστικής συσκευής και στη συνέχεια να διαγραφούν οριστικά από το πρόγραμμα στο οποίο ελήφθησαν.

- **Αφαιρούμενα ηλεκτρονικά μέσα -** Οι PII μπορούν να αποθηκεύονται σε αφαιρούμενα ηλεκτρονικά μέσα, όπως οι μονάδες USB, για τους σκοπούς της μεταφοράς πληροφοριών μεταξύ μέσων. Οι συσκευές αφαιρούμενων μέσων θα πρέπει να προστατεύονται με κωδικό πρόσβασης και να κρυπτογραφούνται. Αυτή δεν είναι η προτιμώμενη μέθοδος αποθήκευσης PII. Οι πληροφορίες που είναι αποθηκευμένες σε αφαιρούμενα ηλεκτρονικά μέσα θα πρέπει να θεωρούνται ως χώρος προσωρινής αποθήκευσης και οι PII θα πρέπει να μεταφέρονται σε διακομιστή της PTI το συντομότερο δυνατό και να αφαιρούνται από τα αφαιρούμενα μέσα. Ευαίσθητες PII, όπως Αριθμοί Κοινωνικής Ασφάλισης, Πληροφορίες Διαβατηρίου και τραπεζικά ή άλλα οικονομικά δεδομένα **δεν** πρέπει να αποθηκεύονται σε αφαιρούμενα ηλεκτρονικά μέσα.
- **Τοπικός διακομιστής ή διακομιστής Νέφους που ανήκει στην PTI** - Το προτιμώμενο μέρος για την αποθήκευση όλων των PII είναι σε τοπικούς διακομιστές που ανήκουν στην PTI ή σε νέφος και αυτή η μέθοδος αποθήκευσης θα πρέπει πάντα να χρησιμοποιείται πρώτη όταν είναι διαθέσιμη. Όλοι οι φάκελοι και τα δεδομένα που περιέχουν PII πρέπει να επισημαίνονται σαφώς ως τέτοιοι και η πρόσβαση σε αυτούς τους φακέλους θα περιορίζεται μόνο σε εκείνους τους εργαζομένους που απαιτείται να έχουν πρόσβαση στην καθημερινή λειτουργία των καθηκόντων τους.
- **Αποθήκευση έντυπων αντιγράφων (επιτόπου)** - Οι PII που φυλάσσονται στους χώρους των γραφείων θα πρέπει να ασφαλίζονται σε κλειδωμένα συρτάρια και κατά προτίμηση πίσω από κλειδωμένες πόρτες, εάν είναι δυνατόν. Η πρόσβαση σε αυτές τις τοποθεσίες θα πρέπει να περιορίζεται στους Εργαζομένους που χρειάζονται τις πληροφορίες για την εκτέλεση των καθημερινών τους καθηκόντων. Τα κλειδιά αυτών των ασφαλών χώρων θα πρέπει να φυλάσσονται μόνο από τον προϊστάμενο του τμήματος και κάθε πρόσβαση που παρέχεται στους Εργαζομένους θα πρέπει να τεκμηριώνεται σε μορφή ημερολογίου. Σε καμία συνήθη περίπτωση δεν πρέπει να μεταφέρονται εκτός γραφείου έγγραφα που περιέχουν PII και για κάθε τέτοια περίπτωση που απαιτεί την απομάκρυνση των PII από το γραφείο απαιτείται η έγκριση του Διευθύνοντος Συμβούλου. Όλες οι πληροφορίες, τα δεδομένα και τα έγγραφα που περιέχουν PII πρέπει να επισημαίνονται σαφώς, ώστε όλοι οι χρήστες να γνωρίζουν την κυριότητα, την ταξινόμηση και την αξία των πληροφοριών. Οι πληροφορίες, τα δεδομένα και τα έγγραφα που περιέχουν PII θα μεταφέρονται

με ασφάλεια και θα καταστρέφονται με ασφάλεια, ώστε να προστατεύονται από ακούσια αποκάλυψη. Οι πληροφορίες, τα δεδομένα και τα έγγραφα που περιέχουν PII θα αποθηκεύονται με ασφάλεια όταν δεν χρησιμοποιούνται.

- **Αποθήκευση έντυπων αντιγράφων (εκτός του χώρου) -** Η αποθήκευση των PII σε μορφή έντυπου αντιγράφου εκτός του χώρου δεν είναι γενικά επιτρεπτή χωρίς την έγγραφη έγκριση του Διευθύνοντος Συμβούλου. Τα δεδομένα που περιέχουν PII σε μορφή έντυπου αντιγράφου δεν πρέπει να αποστέλλονται σε εξωτερικές εγκαταστάσεις αποθήκευσης ως μέρος των αρχείων του ιστότοπου και σε καμία περίπτωση δεν πρέπει να αποθηκεύονται τέτοια δεδομένα στα σπίτια των Εργαζομένων. Όλες οι πληροφορίες, τα δεδομένα και τα έγγραφα που περιέχουν PII πρέπει να επισημαίνονται σαφώς, ώστε όλοι οι χρήστες να γνωρίζουν την κυριότητα, την ταξινόμηση και την αξία των πληροφοριών. Οι πληροφορίες, τα δεδομένα και τα έγγραφα που περιέχουν PII θα μεταφέρονται με ασφάλεια και θα καταστρέφονται με ασφάλεια για την προστασία από ακούσια αποκάλυψη. Οι πληροφορίες, τα δεδομένα και τα έγγραφα που περιέχουν PII θα αποθηκεύονται με ασφάλεια όταν δεν χρησιμοποιούνται.
- **Μεταφορά Έντυπων Αντιγράφων -** Όταν οι PII πρέπει να μεταφερθούν εκτός των χώρων του γραφείου υπό εγκεκριμένες συνθήκες, αυτό θα πρέπει να γίνεται μόνο από άμεσους Εργαζομένους της PTI. Θα πρέπει να λαμβάνεται επαρκής μέριμνα ώστε να διασφαλίζεται ότι τα δεδομένα που περιέχουν PII είναι ασφαλισμένα (κλειδωμένος χαρτοφύλακας κ.λπ.) και ότι τα δεδομένα αυτά βρίσκονται πάντοτε στην κατοχή του εργαζομένου κατά τη μεταφορά.
- Εκτυπώσεις **σε Μορφή Έντυπων Αντιγράφων -** Η εκτύπωση δεδομένων που περιέχουν PII και αποθηκεύονται ηλεκτρονικά θα πρέπει να αποφεύγεται όσο το δυνατόν περισσότερο. Σε περιπτώσεις όπου αυτό δεν είναι δυνατόν, ο Εργαζόμενος που εκτυπώνει τα δεδομένα θα πρέπει να λάβει προηγούμενη έγκριση από τον προϊστάμενο του τμήματος, αναφέροντας ποιο υλικό εκτυπώνεται και για ποιο λόγο. Ο Εργαζόμενος θα είναι επίσης υπεύθυνος για την καταστροφή των εκτυπώσεων σε μορφή έντυπου αντιγράφου και θα υποβάλει στον προϊστάμενο του τμήματος δήλωση που θα περιέχει την ημερομηνία καταστροφής, την περιγραφή του υλικού που καταστράφηκε και τη μέθοδο που χρησιμοποιήθηκε.

## 2.3 Πρόσβαση σε PII από Εργαζομένους

Κάθε προϊστάμενος τμήματος είναι υπεύθυνος για τον προσδιορισμό και την τήρηση καταλόγου των χρηστών του τμήματός του που πρέπει να έχουν πρόσβαση σε αρχεία (ηλεκτρονικά ή σε μορφή έντυπου αντιγράφου). Ο κατάλογος θα πρέπει να επικαιροποιείται ανάλογα με τις ανάγκες και θα πρέπει τουλάχιστον να επανεξετάζεται ετησίως και σε περίπτωση προσωπικού γεγονότος (π.χ. πρόσληψη, αποχώρηση, απόλυση, προαγωγή). Ο κατάλογος θα παραδίδεται στο τμήμα IT, το οποίο με τη σειρά του θα είναι υπεύθυνο να διασφαλίζει ότι η πρόσβαση σε ηλεκτρονικά αρχεία που περιέχουν PII περιορίζεται σύμφωνα με τον κατάλογο. Κάθε προϊστάμενος τμήματος θα είναι υπεύθυνος να διασφαλίσει ότι η πρόσβαση στα αρχεία έντυπων αντιγράφων που περιέχουν PII περιορίζεται σύμφωνα με τον κατάλογο. Οι προϊστάμενοι των

τμημάτων και/ή οι διευθυντές που ορίζουν πρέπει να επανεξετάζουν την πρόσβαση των χρηστών μετά από οποιαδήποτε αλλαγή στους ρόλους και τις αρμοδιότητες ενός ατόμου που επηρεάζεται από την εργασία του ή από την ιδιότητα του εργαζομένου/ανεξάρτητου συμβασιούχου (συμπεριλαμβανομένης, ενδεικτικά, της καταγγελίας) και να κοινοποιούν εγκαίρως οποιεσδήποτε αλλαγές στο τμήμα IT.

## 2.4 Ρυθμιστικές Απαιτήσεις

Η πολιτική της Εταιρείας είναι να συμμορφώνεται με όλους τους διεθνείς, ομοσπονδιακούς ή Πολιτειακούς νόμους και κανονισμούς σχετικά με την πρόσβαση, τη χρήση, την αποθήκευση και τη διατήρηση των PII. Τα Νομικά Τμήματα και/ή τα Τμήματα Συμμόρφωσης της Phoenix Tower επιβλέπουν όλα τα θέματα κανονιστικής συμμόρφωσης. Εάν οποιαδήποτε διάταξη της παρούσας Πολιτικής έρχεται σε σύγκρουση με νομοθετική απαίτηση της διεθνούς, ομοσπονδιακής ή πολιτειακής νομοθεσίας που διέπει τις PII, η διάταξη(διατάξεις) της Πολιτικής που έρχονται σε σύγκρουση αντικαθίστανται.

## 2.5 Εκπαίδευση

Σε όλους τους νεοπροσλαμβανόμενους που εισέρχονται στην Εταιρεία παρέχεται εισαγωγική εκπαίδευση σχετικά με την ορθή διαχείριση και προστασία των PII και τους παρέχεται αντίγραφο της παρούσας Πολιτικής και των διαδικασιών εφαρμογής για το τμήμα στο οποίο έχουν τοποθετηθεί (εάν υπάρχουν). Οι Εργαζόμενοι σε θέσεις με τακτική συνεχή πρόσβαση σε PII ή όσοι μετατίθενται σε τέτοιες θέσεις λαμβάνουν εκπαίδευση που ενισχύει την παρούσα Πολιτική και τις διαδικασίες για τη διατήρηση των δεδομένων PII και λαμβάνουν εκπαίδευση σχετικά με την ασφάλεια και την προστασία των δεδομένων PII και των δεδομένων ιδιοκτησίας της εταιρείας τουλάχιστον ετησίως. Η εκπαίδευση θα γίνεται υπό την καθοδήγηση του τμήματος IT και θα αποτελεί μέρος του προσανατολισμού των νέων εργαζομένων στην περίπτωση νέων Εργαζομένων. Εάν ένας υφιστάμενος Εργαζόμενος προστεθεί στον κατάλογο πρόσβασης σε PII, ο Εργαζόμενος θα λάβει ξεχωριστή εκπαίδευση σχετικά με τις διατάξεις της παρούσας Πολιτικής.

## 2.6 Επιβεβαίωση Εμπιστευτικότητας

Όλοι οι Εργαζόμενοι της Εταιρείας πρέπει να διατηρούν την εμπιστευτικότητα των PII καθώς και των Εμπιστευτικών Πληροφοριών της εταιρείας στις οποίες ενδέχεται να έχουν πρόσβαση και να κατανοούν ότι τέτοιες PII πρέπει να περιορίζονται μόνο σε όσους έχουν επαγγελματική ανάγκη να τις γνωρίζουν.

## 2.7 Παραβιάσεις Δεδομένων PII/Περιστατικά Ασφαλείας

Εάν ένας Εργαζόμενος αντιληφθεί οποιαδήποτε χρήση, πρόσβαση ή μεταφορά προσωπικών δεδομένων που έρχεται σε αντίθεση με την παρούσα Πολιτική ή οποιοδήποτε περιστατικό ασφαλείας, ο Εργαζόμενος πρέπει να το αναφέρει αμέσως στο Νομικό Τμήμα της Phoenix Tower. Οι βάσεις δεδομένων ή τα σύνολα δεδομένων που περιλαμβάνουν PII μπορεί να παραβιαστούν ακούσια ή μέσω παράνομης εισβολής. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα 6 της παρούσας Πολιτικής.

### 2.8 Παραβάσεις των Πολιτικών και Διαδικασιών σχετικά με τις PII

Η Phoenix Tower θεωρεί ότι η προστασία των δεδομένων PII είναι ύψιστης σημασίας. Οι παραβιάσεις της παρούσας Πολιτικής ή των διαδικασιών της θα έχουν ως αποτέλεσμα πειθαρχικές ενέργειες, οι οποίες μπορεί να περιλαμβάνουν την αναστολή ή την απόλυση σε περίπτωση σοβαρών ή επαναλαμβανόμενων παραβιάσεων.

### 2.9 Παρακολούθηση της Χρήσης των Συστημάτων Ηλεκτρονικών Υπολογιστών

Η Εταιρεία έχει το δικαίωμα και τη δυνατότητα να παρακολουθεί τις ηλεκτρονικές πληροφορίες που δημιουργούνται και/ή κοινοποιούνται από άτομα που χρησιμοποιούν τα συστήματα και τα δίκτυα ηλεκτρονικών υπολογιστών της Εταιρείας, συμπεριλαμβανομένων των μηνυμάτων ηλεκτρονικού ταχυδρομείου και της χρήσης του Διαδικτύου. Δεν αποτελεί πολιτική ή πρόθεση της Εταιρείας να παρακολουθεί συνεχώς όλη τη χρήση του υπολογιστή από τους εργαζομένους ή άλλους χρήστες των συστημάτων και του δικτύου υπολογιστών της Εταιρείας. Ωστόσο, οι χρήστες των συστημάτων θα πρέπει να γνωρίζουν ότι η Εταιρεία μπορεί να παρακολουθεί τη χρήση, συμπεριλαμβανομένων, ενδεικτικά, των προτύπων χρήσης του Διαδικτύου (π.χ. ιστότοπος στον οποίο γίνεται πρόσβαση, διάρκεια σύνδεσης, ώρα πρόσβασης την ημέρα), καθώς και τα ηλεκτρονικά αρχεία και μηνύματα των εργαζομένων, στο βαθμό που είναι απαραίτητο για να διασφαλιστεί ότι το Διαδίκτυο και άλλες ηλεκτρονικές επικοινωνίες χρησιμοποιούνται σύμφωνα με το νόμο και την πολιτική της Εταιρείας. Η χρήση των συστημάτων ηλεκτρονικών υπολογιστών και των δικτύων της Εταιρείας θα θεωρείται ως θετική αναγνώριση και συγκατάθεση για την ανωτέρω περιγραφόμενη παρακολούθηση.

## 3. ΑΠΟΔΕΚΤΉ ΧΡΉΣΗ

Σκοπός της παρούσας ενότητας είναι να διασφαλίσει την αποδεκτή χρήση του εξοπλισμού ηλεκτρονικών υπολογιστών που ανήκει, τον χρονομισθώνει ή τον διαχειρίζεται η Phoenix Tower. Η ακατάλληλη χρήση εκθέτει την Phoenix Tower σε κινδύνους, όπου συμπεριλαμβάνονται επιθέσεις από ιούς, παραβίαση συστημάτων και υπηρεσιών δικτύου, βλάβη της φήμης και νομικά ζητήματα.

### 3.1 Γενική Χρήση και Ιδιοκτησία

- Οι χρήστες πρέπει να γνωρίζουν ότι τα δεδομένα που δημιουργούν ή οι εφαρμογές που χρησιμοποιούν τα δεδομένα στα εταιρικά συστήματα παραμένουν ιδιοκτησία της Phoenix Tower. Οι Εργαζόμενοι δεν θα πρέπει να έχουν καμία προσδοκία ιδιωτικότητας για τις δραστηριότητές τους κατά τη χρήση του εξοπλισμού υπολογιστών της PTI και καμία προσδοκία ιδιοκτησίας, ακόμη και μετά την αποχώρησή τους από την Εταιρεία.
- Για λόγους ασφαλείας και συντήρησης του δικτύου, εξουσιοδοτημένα άτομα εντός της Phoenix Tower μπορούν να παρακολουθούν τον εξοπλισμό, τα συστήματα και την κυκλοφορία του δικτύου ανά πάσα στιγμή.
- Η Phoenix Tower διατηρεί το δικαίωμα να ελέγχει τα δίκτυα και τα συστήματα σε περιοδική βάση για να διασφαλίζει τη συμμόρφωση με την παρούσα Πολιτική.

## 3.2 Πληροφορίες Ασφάλειας και Ιδιοκτησίας

- Οι πληροφορίες που διατηρούνται στα συστήματα της Phoenix Tower και περιέχουν PII θα επισημαίνονται σαφώς ως τέτοιες σύμφωνα με την ενότητα «Προσωπικά Αναγνωρίσιμες Πληροφορίες» της παρούσας Πολιτικής. Οι χρήστες θα προσπαθούν να διατηρούν τις πληροφορίες αυτές ασφαλείς.
- Διατηρείτε τους κωδικούς πρόσβασης ασφαλείς και μην μοιράζεστε λογαριασμούς. Οι εξουσιοδοτημένοι χρήστες είναι υπεύθυνοι για την ασφάλεια και την ακεραιότητα των κωδικών πρόσβασης και των λογαριασμών τους.
- Οι εργαζόμενοι πρέπει να είναι ιδιαίτερα προσεκτικοί όταν ανοίγουν συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνουν από άγνωστους αποστολείς, τα οποία ενδέχεται να περιέχουν ιούς ή κακόβουλο λογισμικό.
- Τα συστήματα που αποθηκεύουν εμπιστευτικές πληροφορίες της Phoenix Tower ή που χρησιμοποιούνται για την επεξεργασία πληροφοριών δεν πρέπει να απομακρύνονται από τις εγκαταστάσεις της Phoenix Tower χωρίς την επίσημη έγκριση της διοίκησης.
- Οι εργαζόμενοι δεν θα πρέπει να χρησιμοποιούν λειτουργίες αυτόματης συμπλήρωσης του προγράμματος περιήγησης ιστού ή άλλες λειτουργίες που αποθηκεύουν πληροφορίες για το ID χρήστη και τον κωδικό πρόσβασης σε διαδικτυακές επιχειρηματικές εφαρμογές.

## 3.3 Απαγορευμένες Δραστηριότητες

- Συμμετοχή σε οποιαδήποτε δραστηριότητα που είναι παράνομη σύμφωνα με την τοπική, πολιτειακή, ομοσπονδιακή ή διεθνή νομοθεσία κατά τη χρήση πόρων που ανήκουν στην Phoenix Tower.
- Η εξαγωγή λογισμικού, τεχνικών πληροφοριών, λογισμικού κρυπτογράφησης ή τεχνολογίας, κατά παράβαση των διεθνών ή περιφερειακών νόμων περί ελέγχου των εξαγωγών, είναι παράνομη. Πριν από την εξαγωγή οποιουδήποτε

αμφισβητούμενου υλικού θα ζητείται η γνώμη της αρμόδιας διεύθυνσης.

- Χρήση ενός υπολογιστικού περιουσιακού στοιχείου της Phoenix Tower για την ενεργό συμμετοχή στην προμήθεια ή τη μετάδοση υλικού που παραβιάζει τους νόμους περί σεξουαλικής παρενόχλησης ή εχθρικού εργασιακού περιβάλλοντος.
- Παράκαμψη του ελέγχου ταυτότητας χρήστη ή της ασφαλείας οποιουδήποτε κεντρικού υπολογιστή, δικτύου ή λογαριασμού. Απαγορεύεται αυστηρά η μη εξουσιοδοτημένη χρήση ID δικτύου διαφορετικού από το δικό σας.
- Μη εξουσιοδοτημένες απόπειρες καταστρατήγησης της ασφαλείας του δικτύου, της προστασίας δεδομένων, της ασφαλείας κωδικών πρόσβασης ή της εγκατάστασης/χρήσης λογισμικού που έχει σχεδιαστεί για την καταστρατήγηση οποιασδήποτε ασφαλείας ή πολιτικής που δημιουργήθηκε και εφαρμόστηκε από την Phoenix Tower.
- Απόπειρα παραβίασης ή χειραγώγησης της δικτυακής επικοινωνίας ή των αρχείων άλλου υπαλλήλου.
- Παραβίαση οποιουδήποτε νόμου περί πνευματικών δικαιωμάτων και των διατάξεων περί δίκαιης χρήσης. Αυτό περιλαμβάνει την αντιγραφή ή την «πειρατεία» λογισμικού ή
  παραβίαση αδειών χρήσης/συμβάσεων λογισμικού.
- Εγκατάσταση ανεπίσημων εφαρμογών σε οποιοδήποτε περιουσιακό στοιχείο της Phoenix Tower χωρίς την προηγούμενη συγκατάθεση του τμήματος IT.
- Αποκάλυψη εμπιστευτικών πληροφοριών και/ή εμπορικών μυστικών.
- Οι χρήστες δεν πρέπει να αποκτούν σκόπιμα πρόσβαση σε συστήματα της Εταιρείας για τα οποία δεν έχουν εξουσιοδότηση ή επαγγελματική ανάγκη να γνωρίζουν.

## 4. ΧΡΉΣΗ ΗΛΕΚΤΡΟΝΙΚΟΎ ΤΑΧΥΔΡΟΜΕΊΟΥ

Η παρούσα ενότητα αποσκοπεί στην παροχή κατευθυντήριων γραμμών για την αποδεκτή χρήση του ηλεκτρονικού ταχυδρομείου και στην περιγραφή των διαδικασιών διατήρησης του ηλεκτρονικού ταχυδρομείου.

### 4.1 Επιτρεπόμενη Χρήση

- Το εταιρικό ηλεκτρονικό ταχυδρομείο και τα συστήματα ηλεκτρονικού ταχυδρομείου πρέπει να χρησιμοποιούνται μόνο για επαγγελματικούς σκοπούς και πρέπει να συνάδουν με τις πολιτικές και τις διαδικασίες της PTI για την ηθική συμπεριφορά, την ασφάλεια και τη συμμόρφωση με τους ισχύοντες νόμους και τις επιχειρηματικές πρακτικές. Οποιαδήποτε προσωπική επικοινωνία στο εταιρικό ηλεκτρονικό ταχυδρομείο πρέπει να είναι περιορισμένη.
- Οι Εργαζόμενοι δεν έχουν καμία προσδοκία ιδιωτικότητας για οτιδήποτε αποθηκεύουν, αποστέλλουν ή λαμβάνουν στο σύστημα ηλεκτρονικού ταχυδρομείου της Εταιρείας. Η PTI μπορεί να παρακολουθεί τα μηνύματα χωρίς προηγούμενη ειδοποίηση.
- Οι εργαζόμενοι πρέπει να υποβάλλουν καταγγελία με Αυθεντικοποίηση

Πολλαπλών Παραγόντων.

4.2 Ηλεκτρονικό ταχυδρομείο που περιέχει PII

- Εάν πρόκειται να μεταβιβαστούν PII μέσω ηλεκτρονικού ταχυδρομείου, πρέπει να ληφθούν τα ακόλουθα μέτρα για να διασφαλιστεί η ασφαλής διαβίβαση και να ελαχιστοποιηθεί ο κίνδυνος παραβίασης μετά την επιβεβαίωση ότι οι εν λόγω PII έχουν αποθηκευτεί στον τοπικό διακομιστή:
    1. Προστασία του εγγράφου με κωδικό πρόσβασης, είτε πρόκειται για pdf, word ή excel. Εάν το έγγραφο είναι σε μορφή που δεν προστατεύεται εύκολα (π.χ. gif ή jpeg), μετατρέψτε το έγγραφο σε αρχείο pdf, προστατέψτε το με κωδικό πρόσβασης σε αυτή τη μορφή και αποθηκεύστε το ξανά. Η «αρχική» μορφή μπορεί να διαγραφεί αυτή τη στιγμή και να αφαιρεθεί από τον κάδο απορριμμάτων.
    2. Στείλτε το έγγραφο με το ηλεκτρονικό ταχυδρομείο με την ένδειξη «**ΕΜΠΙΣΤΕΥΤΙΚΟ**» ως ετικέτα μετά το θέμα
    όνομα στη γραμμή θέματος.
    3. Επικοινωνήστε τηλεφωνικά με τον παραλήπτη για να επιβεβαιώσετε ότι ο παραλήπτης έλαβε το μήνυμα ηλεκτρονικού ταχυδρομείου και να του δώσετε τον κωδικό πρόσβασης. ***ΠΟΤΕ ΜΗΝ ΣΤΕΛΝΕΤΕ ΤΟΝ ΚΩΔΙΚΟ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΙΔΙΟ ΜΗΝΥΜΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΜΕ ΤΙΣ PII***
    4. Διαγράψτε το συνημμένο από το αποσταλμένο μήνυμα ηλεκτρονικού ταχυδρομείου.

- Ευαίσθητες PII, όπως Αριθμοί Κοινωνικής Ασφάλισης, Πληροφορίες Διαβατηρίου και τραπεζικά ή άλλα οικονομικά δεδομένα **δεν** πρέπει να αποστέλλονται σε ηλεκτρονικό ταχυδρομείο.
- Εάν η PTI λάβει οποιεσδήποτε PII μέσω ηλεκτρονικού ταχυδρομείου, διαδικτύου ή προγραμμάτων ανταλλαγής άμεσων μηνυμάτων, οι πληροφορίες θα πρέπει να μεταφερθούν αμέσως στον τοπικό διακομιστή (πρώτη προτίμηση) ή να μεταφερθούν στον αποθηκευτικό χώρο μιας φορητής υπολογιστικής συσκευής και στη συνέχεια να διαγραφούν οριστικά από το πρόγραμμα στο οποίο ελήφθησαν.

4.3 Απαγορευμένες Δραστηριότητες Ηλεκτρονικού Ταχυδρομείου και Επικοινωνιών

- Χρήση του ηλεκτρονικού ταχυδρομείου της PTI για εμπορικές χρήσεις που δεν σχετίζονται με την PTI ή για συχνή προσωπική χρήση.
- Αυτόματη προώθηση του ηλεκτρονικού ταχυδρομείου της PTI σε συστήματα ή πλατφόρμες ηλεκτρονικού ταχυδρομείου τρίτων.
- Διαγραφή ή τροποποίηση του μηνύματος νομικής αποποίησης ευθύνης που δημιουργείται από το σύστημα και επισυνάπτεται σε κάθε μήνυμα ηλεκτρονικού ταχυδρομείου της PTI.

- Αποστολή μη ζητηθέντων μηνυμάτων ηλεκτρονικού ταχυδρομείου, συμπεριλαμβανομένης της αποστολής «ανεπιθύμητης αλληλογραφίας» ή άλλου διαφημιστικού υλικού ή υλικού προσέλκυσης σε άτομα που δεν έχουν ζητήσει ρητά τέτοιο υλικό (ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου).
- Η δημιουργία ή η διανομή διασπαστικών ή προσβλητικών μηνυμάτων. Οι Εργαζόμενοι που λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου με αυτό το περιεχόμενο από οποιονδήποτε υπάλληλο της Phoenix Tower θα αναφέρουν το θέμα αμέσως στον προϊστάμενό τους.
- Χρήση λογαριασμών ηλεκτρονικού ταχυδρομείου που δεν ανήκουν στην Phoenix Tower (Hotmail, Gmail κ.λπ.) για επίσημες υποθέσεις της Phoenix Tower ή προώθηση μηνυμάτων ηλεκτρονικού ταχυδρομείου που λαμβάνονται σε λογαριασμούς ηλεκτρονικού ταχυδρομείου της Phoenix Tower σε προσωπικούς ή μη λογαριασμούς ηλεκτρονικού ταχυδρομείου της Phoenix Tower (Hotmail, Gmail κ.λπ.).
- Συνδρομή σε ηλεκτρονικές υπηρεσίες ή άλλες συμβάσεις με χρήση διευθύνσεων ηλεκτρονικού ταχυδρομείου της PTI χωρίς έγκυρο επαγγελματικό λόγο.

## 4.4 Κινητές Συσκευές

- Οι Εργαζόμενοι πρέπει να λάβουν προηγούμενη έγκριση από τον διευθυντή ή τον προϊστάμενό τους πριν επιχειρήσουν να αποκτήσουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο της PTI μέσω προσωπικών κινητών συσκευών.
- Η Phoenix Tower παρέχει πρόσβαση στο ηλεκτρονικό ταχυδρομείο μέσω φορητών προσωπικών συσκευών σύμφωνα με την παρούσα Πολιτική. Η Phoenix Tower δεν ευθύνεται για την απώλεια δεδομένων σε περίπτωση διαγραφής μιας συσκευής (είτε λόγω λάθους του χρήστη είτε λόγω εφαρμοζόμενων χαρακτηριστικών ασφαλείας). Η παρούσα πολιτική ισχύει για όλες τις φορητές Συσκευές Τελικού Χρήστη και κάθε άλλη συσκευή που μπορεί να έχει πρόσβαση στις υπηρεσίες ηλεκτρονικού ταχυδρομείου της Phoenix Tower και/ή στα προστατευμένα δεδομένα της Phoenix Tower. Η συμμόρφωση με την παρούσα Πολιτική αποτελεί απαίτηση για όλες τις φορητές υπολογιστικές συσκευές που αποθηκεύουν ή έχουν πρόσβαση σε προστατευόμενα δεδομένα της Phoenix Tower.
- Οι χρήστες που χρησιμοποιούν φορητή υπολογιστική συσκευή για να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο, τα δεδομένα, τα αρχεία ή τα έγγραφα της Phoenix Tower θα πρέπει να εφαρμόζουν τα ακόλουθα χαρακτηριστικά ασφαλείας στο βαθμό που είναι διαθέσιμα στη συσκευή:
    - Να έχει ρυθμιστεί ώστε να αποσυνδέεται ή να απενεργοποιείται το πολύ δέκα (10) λεπτά μετά την τελευταία δραστηριότητα του χρήστη.
    - Απαιτείται κωδικός πρόσβασης ενεργοποίησης ή κωδικός πρόσβασης.
    - Απαιτείται ελάχιστο μήκος κωδικού πρόσβασης τεσσάρων (4) χαρακτήρων ή πλήκτρων.
    - Να παρέχεται επαναφορά της συσκευής (διαγραφή δεδομένων) εάν ένας λανθασμένος κωδικός πρόσβασης εισαχθεί περισσότερες από

οκτώ (8) διαδοχικές φορές, όταν αυτό είναι τεχνικά εφικτό.
- Η συσκευή πρέπει να είναι κρυπτογραφημένη.

- Οι χρήστες που χρησιμοποιούν φορητή υπολογιστική συσκευή για να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο, τα δεδομένα, τα αρχεία ή τα έγγραφα της Phoenix Tower θα πρέπει να προσκομίσουν τη συσκευή τους στο τμήμα IT για να διασφαλιστεί η εφαρμογή αυτών των χαρακτηριστικών ασφαλείας.

### 4.5 Διάθεση Εξοπλισμού

Πριν από την διάθεση ή τη μεταφορά, όλες οι φορητές υπολογιστικές συσκευές και οι σχετικές κάρτες μνήμης θα πρέπει να καθαρίζονται πλήρως από όλα τα δεδομένα της Phoenix Tower. Μετά τον τερματισμό της πρόσβασης ενός Εργαζομένου στα συστήματα της Phoenix Tower, το άτομο θα πρέπει να φέρει τη φορητή υπολογιστική συσκευή του στο τμήμα IT, ώστε το τμήμα IT να αφαιρέσει όλα τα δεδομένα της Phoenix Tower από τη συσκευή.

### 4.6 Αναφορά

- Η απώλεια, η κλοπή ή οποιαδήποτε μη εξουσιοδοτημένη χρήση φορητής Συσκευής Τελικού Χρήστη που έχει χρησιμοποιηθεί για την αποθήκευση ή την πρόσβαση σε προστατευμένες πληροφορίες της Phoenix Tower συνιστά αποκάλυψη και πρέπει να αναφέρεται στο τμήμα IT της Phoenix Tower.
- Το τμήμα IT θα συντονίζεται με το Νομικό Τμήμα και τον προϊστάμενο του χρήστη για να καθορίσει τον βαθμό στον οποίο θα πρέπει να διαγραφεί ή να καθαριστεί μια προσωπική συσκευή τελικού χρήστη που ανήκει στην PTI μετά από απώλεια ή κλοπή και κατά τη λήξη της απασχόλησης του χρήστη στην PTI. Εάν διαπιστωθεί ότι η απομακρυσμένη διαγραφή είναι απαραίτητη και δυνατή, το τμήμα IT θα προσπαθήσει να περιορίσει τα δεδομένα που θα διαγραφούν μόνο στις πληροφορίες της Phoenix Tower στο βαθμό που αυτό είναι τεχνικά δυνατό στις συσκευές που ανήκουν στην PTI και/ή στις συσκευές στις οποίες ισχύουν οι επιστροφές.

## 5. ΧΡΉΣΗ ΤΟΥ ΔΙΑΔΙΚΤΎΟΥ

Η Εταιρεία θα παρέχει πρόσβαση στο Διαδίκτυο σε εργαζομένους και εργολάβους που είναι συνδεδεμένοι στο εσωτερικό δίκτυο και έχουν επαγγελματική ανάγκη για την πρόσβαση αυτή.

Το Διαδίκτυο είναι ένα επιχειρηματικό εργαλείο για την Εταιρεία. Πρέπει να χρησιμοποιείται για επιχειρηματικούς σκοπούς, όπως: επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου με προμηθευτές και επιχειρηματικούς εταίρους, λήψη χρήσιμων επιχειρηματικών πληροφοριών και έρευνα για σχετικά τεχνικά και επιχειρηματικά θέματα.

Η υπηρεσία Διαδικτύου δεν επιτρέπεται να χρησιμοποιείται για τη μετάδοση, ανάκτηση ή αποθήκευση επικοινωνιών με χαρακτήρα διάκρισης ή παρενόχλησης ή υποτιμητικό για οποιοδήποτε άτομο ή ομάδα, άσεμνο ή πορνογραφικό, δυσφημιστικό ή απειλητικό χαρακτήρα για «αλυσιδωτές επιστολές» ή για οποιονδήποτε άλλο παράνομο σκοπό ή για προσωπικό όφελος.

## 6. **ΠΡΟΣΩΠΙΚΌ**

Σκοπός του παρόντος τμήματος είναι να μειωθεί ο κίνδυνος ανθρώπινου λάθους, κλοπής, απάτης ή κατάχρησης των εγκαταστάσεων. Επειδή η ασφάλεια των πληροφοριακών αγαθών μας αποτελεί κρίσιμη συνιστώσα του επιχειρηματικού μας μοντέλου, είναι ζωτικής σημασίας όλοι οι Εργαζόμενοι της Phoenix Tower να υπόκεινται σε ορισμένα πρότυπα για να διασφαλίζεται η αξιοπιστία και η ασφάλεια.

### 6.1 Αποθήκευση PII στα Συστήματα της Εταιρείας

- Παρά τον σεβασμό της Phoenix Tower για την ιδιωτική ζωή των εργαζομένων στον χώρο εργασίας, διατηρεί το δικαίωμα πρόσβασης σε όλες τις πληροφορίες που δημιουργούνται και αποθηκεύονται στα συστήματα της Phoenix Tower.
- Η Phoenix Tower έχει το δικαίωμα να παρακολουθεί όλες τις πληροφορίες που λαμβάνονται, αποθηκεύονται, μεταδίδονται και/ή δημιουργούνται σε συστήματα της Phoenix Tower.

### 6.2 Κοινή χρήση Εμπιστευτικών Πληροφοριών

- Οι Εμπιστευτικές Πληροφορίες θα κοινοποιούνται μόνο σε άλλα εξουσιοδοτημένα πρόσωπα.
- Οι πληροφορίες του οργανισμού έχουν τα δικά τους ατομικά επίπεδα ευαισθησίας και δεν πρέπει να αποκαλύπτονται σε προσωπικό που δεν έχει εξουσιοδότηση πρόσβασης στις πληροφορίες αυτές.
- Όλα τα δεδομένα και οι πληροφορίες που δεν είναι δημόσια, σχετικά με την επιχείρηση της Phoenix Tower και τους Εργαζομένους της, πρέπει να παραμένουν πάντοτε εμπιστευτικά.
- Οι εμπιστευτικές πληροφορίες δεν πρέπει να αποκαλύπτονται σε μέλη της οικογένειας που δεν έχουν άδεια να λαμβάνουν τις πληροφορίες αυτές.

## 7. **ΦΥΣΙΚΉ ΑΣΦΆΛΕΙΑ**

Το τμήμα αυτό απαγορεύει τη μη εξουσιοδοτημένη φυσική πρόσβαση στις εγκαταστάσεις και τις πληροφορίες της Phoenix Tower και αποτρέπει τη ζημία ή την παρεμβολή στις κανονικές επιχειρηματικές λειτουργίες. Η παρούσα Πολιτική καλύπτει επίσης όλη τη φυσική ασφάλεια των εισόδων, των χώρων εργασίας των γραφείων και άλλων κρίσιμων περιοχών που πρέπει να είναι ασφαλείς για την προστασία των περιουσιακών στοιχείων.

## 7.1 Φυσική Ασφάλεια

- Οι πόρτες ασφαλείας, οι αναγνώστες καρτών και τα πληκτρολόγια PIN χρησιμοποιούνται για την ασφάλεια των χώρων με κρίσιμες πληροφορίες. Μόνο εξουσιοδοτημένοι Εργαζόμενοι μπορούν να εισέλθουν σε αυτούς τους ασφαλείς χώρους.
- Το προσωπικό θα παρακολουθείται ηλεκτρονικά ανάλογα με τους χώρους στους οποίους του έχει χορηγηθεί πρόσβαση. Αυτό γίνεται για να μετριαστούν οι κίνδυνοι κλοπής, βανδαλισμού και μη εξουσιοδοτημένης χρήσης των συστημάτων.
- Οι χώροι στους οποίους γίνεται χειρισμός ασφαλών πληροφοριών (συμπεριλαμβανομένων των εγκαταστάσεων επεξεργασίας πληροφοριών και υπολογιστών) θα υπόκεινται σε αυστηρούς ελέγχους πρόσβασης, ώστε να διασφαλίζεται ότι δεν επιτρέπεται η πρόσβαση σε μη εξουσιοδοτημένους Εργαζομένους ή σε άτομα εκτός του οργανισμού.

## 7.2 Διασφάλιση Μη Επιτηρούμενων Σταθμών Εργασίας και Εγκαταστάσεων Εργασίας

- Ο εξοπλισμός πρέπει πάντα να προστατεύεται κατάλληλα, ιδίως όταν μένει αφύλακτος.
- Πριν φύγετε από το γραφείο σας, εάν το γραφείο σας δεν είναι ορατό, ο υπολογιστής σας πρέπει να αποσυνδεθεί ή να κλειδωθεί για να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση.
- Οι εκτυπωτές και τα φαξ θα καθαρίζονται καθημερινά από ευαίσθητα δεδομένα. Τα ευαίσθητα έγγραφα που αποστέλλονται σε εκτυπωτές ή φαξ πρέπει να ασφαλίζονται αμέσως μετά την εκτύπωσή τους.

## 7.3 Δανεισμός Κλειδιών, Κωδικών Ασφαλείας ή Καρτών Πρόσβασης Ασφαλείας σε Άλλους

- Η χρήση κλειδιών, είτε φυσικών είτε ηλεκτρονικών, για την πρόσβαση σε ασφαλείς χώρους πρέπει να περιορίζεται αυστηρά στον Εργαζόμενο στον οποίο έχουν εκχωρηθεί τα κλειδιά. Απαγορεύεται ο δανεισμός κλειδιών, κωδικών ασφαλείας ή καρτών πρόσβασης ασφαλείας σε μη Εργαζομένους της PTI και/ή σε εξωτερικά πρόσωπα.
- Η μη τήρηση της παρούσας Πολιτικής μπορεί να θεωρηθεί ως παραβίαση της ασφαλείας και υπόκειται σε πειθαρχικά μέτρα.

## 7.4 Αντιμετώπιση Ξένων στις Εγκαταστάσεις

- Εάν ένας ξένος δεν συνοδεύεται από έναν Εργαζόμενο της Phoenix Tower, οι Εργαζόμενοι θα αμφισβητήσουν την παρουσία του ξένου στις εγκαταστάσεις του οργανισμού.

## 8. ΈΛΕΓΧΟΣ ΠΡΌΣΒΑΣΗΣ

Ένα θεμελιώδες στοιχείο της Πολιτικής μας για την Ασφάλεια των Πληροφοριών είναι ο έλεγχος της πρόσβασης στους κρίσιμους πόρους πληροφοριών που απαιτούν προστασία από μη εξουσιοδοτημένη αποκάλυψη ή τροποποίηση. Η θεμελιώδης έννοια του ελέγχου πρόσβασης είναι ότι τα δικαιώματα εκχωρούνται σε άτομα ή συστήματα που είναι εξουσιοδοτημένα να έχουν πρόσβαση σε συγκεκριμένους πόρους. Οι έλεγχοι πρόσβασης υπάρχουν σε διάφορα επίπεδα του συστήματος, συμπεριλαμβανομένου του δικτύου. Ο έλεγχος πρόσβασης υλοποιείται με ID σύνδεσης και κωδικό πρόσβασης. Σε επίπεδο εφαρμογής και βάσης δεδομένων, μπορούν να εφαρμοστούν άλλες μέθοδοι ελέγχου πρόσβασης για τον περαιτέρω περιορισμό της πρόσβασης. Τα συστήματα εφαρμογών και βάσεων δεδομένων μπορούν να περιορίσουν τον αριθμό των εφαρμογών και των βάσεων δεδομένων που είναι διαθέσιμες στους χρήστες με βάση τις απαιτήσεις της εργασίας τους.

### 8.1 Πρόσβαση Χρήστη στο Σύστημα και το Δίκτυο - Κανονική Ταυτοποίηση Χρήστη

Όλοι οι χρήστες θα πρέπει να διαθέτουν μοναδικό ID σύνδεσης και κωδικό πρόσβασης για πρόσβαση στα συστήματα. Ο κωδικός πρόσβασης του χρήστη πρέπει να τηρείται εμπιστευτικά και ΔΕΝ ΠΡΕΠΕΙ να κοινοποιείται στη διοίκηση & στο εποπτικό προσωπικό και/ή σε οποιονδήποτε άλλο εργαζόμενο. Όλοι οι χρήστες πρέπει να συμμορφώνονται με τους ακόλουθους κανόνες σχετικά με τη δημιουργία και τη διατήρηση των κωδικών πρόσβασης:

- Ο κωδικός πρόσβασης πρέπει να είναι πολύπλοκος. :
  - Το ελάχιστο μήκος ενός κωδικού πρόσβασης πρέπει να είναι 8 χαρακτήρες.
  - Πρέπει να αποτελείται από συνδυασμό αλφαριθμητικών χαρακτήρων (κεφαλαία και πεζά γράμματα, αριθμητικά ψηφία και ειδικά σύμβολα).
  - Αλφάβητο με μικρά γράμματα.
  - Αλφάβητο με κεφαλαία γράμματα.
  - Σύμβολα: . : { } ! @ # $ % ^ & * ? _ ~ -
  - Αριθμοί από 0 έως 9.
  - Δεν πρέπει να περιέχει διαδοχικούς πανομοιότυπους χαρακτήρες.
  - Ως σύσταση, ο κωδικός πρόσβασης δεν θα πρέπει να είναι ο ίδιος με οποιονδήποτε από τους 5 τελευταίους κωδικούς πρόσβασης που χρησιμοποιήθηκαν.
- Δηλαδή, μην χρησιμοποιείτε κανένα κοινό όνομα, ουσιαστικό, ρήμα, επίρρημα ή επίθετο. Αυτοί οι εύκολοι κωδικοί πρόσβασης μπορούν εύκολα να σπάσουν με τη χρήση τυποποιημένων «εργαλείων χάκερ».
- Οι κωδικοί πρόσβασης δεν πρέπει να αναρτώνται πάνω ή κοντά σε τερματικά υπολογιστών ή να είναι με άλλο τρόπο εύκολα προσβάσιμοι στο τερματικό.
- Ο κωδικός πρόσβασης πρέπει να αλλάζει κάθε 60 ημέρες.
- Οι λογαριασμοί χρηστών θα παγώσουν μετά από 5 αποτυχημένες προσπάθειες σύνδεσης.
- Τα IDs σύνδεσης και οι κωδικοί πρόσβασης θα ανασταλούν μετά από 20 ημέρες

χωρίς χρήση.

Οι χρήστες δεν επιτρέπεται να έχουν πρόσβαση σε αρχεία κωδικών πρόσβασης σε κανένα στοιχείο υποδομής δικτύου. Τα αρχεία κωδικών πρόσβασης στους διακομιστές θα παρακολουθούνται για πρόσβαση από μη εξουσιοδοτημένους χρήστες. Απαγορεύεται αυστηρά η αντιγραφή, ανάγνωση, διαγραφή ή τροποποίηση ενός αρχείου κωδικού πρόσβασης σε οποιοδήποτε σύστημα υπολογιστή.

Οι χρήστες δεν θα μπορούν να συνδεθούν ως Διαχειριστής Συστήματος. Οι χρήστες που χρειάζονται αυτό το επίπεδο πρόσβασης στα συστήματα παραγωγής πρέπει να ζητήσουν λογαριασμό ειδικής πρόσβασης, όπως περιγράφεται σε άλλο σημείο του παρόντος εγγράφου.

Τα IDs σύνδεσης και οι κωδικοί πρόσβασης των εργαζομένων θα απενεργοποιούνται το συντομότερο δυνατό, εάν ο εργαζόμενος αποχωρήσει, καταγγελθεί η σύμβασή του, απολυθεί, τεθεί σε διαθεσιμότητα, τεθεί σε άδεια ή αποχωρήσει με άλλο τρόπο από την εργασία του γραφείου της Εταιρείας.

Οι Προϊστάμενοι/Διευθυντές πρέπει να επικοινωνούν αμέσως και άμεσα με το τμήμα IT της Εταιρείας για να αναφέρουν οποιαδήποτε αλλαγή στην κατάσταση του εργαζομένου που απαιτεί τον τερματισμό ή την τροποποίηση των δικαιωμάτων πρόσβασης του εργαζομένου στη σύνδεση.

Οι εργαζόμενοι που ξεχνούν τον κωδικό πρόσβασής τους πρέπει να καλέσουν το τμήμα IT ή να ακολουθήσουν τα εργαλεία που παρέχονται από το τμήμα IT για να τους χορηγηθεί νέος κωδικός πρόσβασης στον λογαριασμό τους. Ο εργαζόμενος πρέπει να ταυτοποιηθεί με τον αριθμό του (π.χ. αριθμός εργαζομένου) στο τμήμα IT.

Οι εργαζόμενοι είναι υπεύθυνοι για όλες τις συναλλαγές που πραγματοποιούνται κατά τη διάρκεια των συνεδριών σύνδεσης που ξεκινούν με τη χρήση του κωδικού πρόσβασης και του ID του εργαζομένου. Οι εργαζόμενοι δεν πρέπει να συνδέονται σε έναν υπολογιστή και στη συνέχεια να επιτρέπουν σε άλλο άτομο να χρησιμοποιεί τον υπολογιστή ή να μοιράζονται με άλλο τρόπο την πρόσβαση στα συστήματα υπολογιστών.

### 8.2 Πρόσβαση Διαχειριστή Συστήματος

Οι Διαχειριστές Συστήματος, οι διαχειριστές δικτύων και οι διαχειριστές ασφαλείας θα έχουν πρόσβαση με υψηλά προνόμια σε κεντρικά συστήματα, δρομολογητές, κόμβους και τείχη προστασίας, όπως απαιτείται για την εκπλήρωση των καθηκόντων τους.

Όλοι οι κωδικοί πρόσβασης των διαχειριστών του συστήματος θα **ΔΙΑΓΡΑΦΟΝΤΑΙ** αμέσως μετά την απομάκρυνση, καταγγελία της σύμβασής τους, απόλυση ή άλλη αποχώρηση από την εταιρεία οποιουδήποτε εργαζομένου που έχει πρόσβαση σε αυτούς τους κωδικούς πρόσβασης. Οι κωδικοί πρόσβασης των εργαζομένων που τίθενται σε διοικητική ή πειθαρχική άδεια αναστέλλονται έως ότου αποκατασταθεί η ενεργός εργασιακή τους κατάσταση.

## 8.3 Ειδική Πρόσβαση

Οι λογαριασμοί ειδικής πρόσβασης παρέχονται σε άτομα που χρειάζονται προσωρινά προνόμια διαχειριστή συστήματος για την εκτέλεση της εργασίας τους. Αυτοί οι λογαριασμοί παρακολουθούνται από την Εταιρεία και απαιτούν την άδεια του τμήματος IT της Εταιρείας του χρήστη. Η παρακολούθηση των λογαριασμών ειδικής πρόσβασης γίνεται με την καταχώρηση των χρηστών σε μια συγκεκριμένη περιοχή και την περιοδική δημιουργία αναφορών προς τη διοίκηση. Οι αναφορές θα δείχνουν ποιος έχει επί του παρόντος λογαριασμό ειδικής πρόσβασης, για ποιο λόγο και πότε θα λήξει. Οι ειδικοί λογαριασμοί λήγουν σε 2 ημέρες και δεν ανανεώνονται αυτόματα χωρίς γραπτή άδεια.

## 8.4 Σύνδεση σε Δίκτυα Τρίτων

Η παρούσα πολιτική θεσπίζεται για να διασφαλιστεί μια ασφαλής μέθοδος σύνδεσης μεταξύ της Εταιρείας και όλων των εταιρειών τρίτου μέρους και άλλων οντοτήτων που απαιτείται να ανταλλάσσουν ηλεκτρονικά πληροφορίες με την Εταιρεία.

Ο όρος «Τρίτος» αναφέρεται σε προμηθευτές, συμβούλους και επιχειρηματικούς εταίρους που συνεργάζονται με την Εταιρεία, καθώς και σε άλλους εταίρους που έχουν ανάγκη να ανταλλάσσουν πληροφορίες με την Εταιρεία. Οι δικτυακές συνδέσεις τρίτων πρέπει να χρησιμοποιούνται μόνο από τους εργαζομένους του τρίτου μέρους, μόνο για τους επιχειρηματικούς σκοπούς της Εταιρείας. Η Εταιρεία τρίτο μέρος θα διασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση σε πληροφορίες στο δίκτυο της Εταιρείας. Ο τρίτος δεν θα επιτρέπει τη ροή της κίνησης μέσω του Διαδικτύου ή άλλων ιδιωτικών δικτύων στο δίκτυο της εταιρείας. Ως σύνδεση δικτύου τρίτου ορίζεται μία από τις ακόλουθες επιλογές συνδεσιμότητας:

- Μια σύνδεση δικτύου θα τερματίζει σε ένα Τείχος Προστασίας και ο τρίτος θα υπόκειται στους τυπικούς κανόνες αυθεντικοποίησης της εταιρείας.

Αυτή η πολιτική ισχύει για όλα τα αιτήματα σύνδεσης τρίτων και για όλες τις υπάρχουσες συνδέσεις τρίτων. Σε περιπτώσεις όπου οι υφιστάμενες συνδέσεις δικτύου τρίτων δεν πληρούν τις απαιτήσεις που περιγράφονται στο παρόν έγγραφο, θα επανασχεδιαστούν όπως απαιτείται.

Όλα τα αιτήματα για συνδέσεις τρίτων πρέπει να υποβάλλονται με γραπτή αίτηση και να εγκρίνονται από το τμήμα IT.

## 8.5 Σύνδεση Συσκευών στο Δίκτυο

Μόνο εξουσιοδοτημένες συσκευές μπορούν να συνδεθούν στο δίκτυο(α) της Εταιρείας. Οι εξουσιοδοτημένες συσκευές περιλαμβάνουν PCs και σταθμούς εργασίας που ανήκουν στην Εταιρεία και συμμορφώνονται με τις οδηγίες διαμόρφωσης της Εταιρείας. Άλλες

εξουσιοδοτημένες συσκευές περιλαμβάνουν συσκευές υποδομής δικτύου που χρησιμοποιούνται για τη διαχείριση και την παρακολούθηση του δικτύου.

Οι χρήστες δεν πρέπει να συνδέουν στο δίκτυο: μη εταιρικούς υπολογιστές που δεν είναι εξουσιοδοτημένοι, δεν ανήκουν και/ή δεν ελέγχονται από την Εταιρεία. Απαγορεύεται ρητά στους χρήστες να συνδέουν οποιαδήποτε μη εταιρική συσκευή, όπως φορητούς υπολογιστές, ηλεκτρονικούς υπολογιστές, εξωτερικούς σκληρούς δίσκους, τηλέφωνα, ταμπλέτες, στο δίκτυο της εταιρείας.

ΣΗΜΕΙΩΣΗ: Οι χρήστες δεν επιτρέπεται να συνδέουν οποιαδήποτε συσκευή που θα μπορούσε να μεταβάλει τα χαρακτηριστικά τοπολογίας του δικτύου ή οποιεσδήποτε μη εξουσιοδοτημένες συσκευές αποθήκευσης (π.χ. στικάκια και CDs με δυνατότητα εγγραφής).

### 8.6 Απομακρυσμένη Πρόσβαση

Μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν απομακρυσμένη πρόσβαση στο δίκτυο της Εταιρείας. Η απομακρυσμένη πρόσβαση παρέχεται στους εργαζομένους, τους εργολάβους και τους επιχειρηματικούς εταίρους της Εταιρείας που έχουν νόμιμη επαγγελματική ανάγκη να ανταλλάσσουν πληροφορίες, να αντιγράφουν αρχεία ή προγράμματα ή να έχουν πρόσβαση σε εφαρμογές υπολογιστών. Οι εξουσιοδοτημένες συνδέσεις μπορεί να είναι απομακρυσμένος υπολογιστής προς το δίκτυο ή απομακρυσμένο δίκτυο προς το δίκτυο της εταιρείας. Η μόνη αποδεκτή μέθοδος απομακρυσμένης σύνδεσης στο εσωτερικό δίκτυο είναι η χρήση ασφαλούς ID.

### 8.7 Μη Εξουσιοδοτημένη Απομακρυσμένη Πρόσβαση

Απαγορεύεται η σύνδεση κεντρικών βάσεων δεδομένων στον υπολογιστή ή τον σταθμό εργασίας ενός χρήστη που είναι συνδεδεμένος στο Τοπικό Δίκτυο (LAN) της Εταιρείας χωρίς την έγγραφη άδεια της Εταιρείας. Επιπλέον, οι χρήστες δεν μπορούν να εγκαθιστούν προσωπικό λογισμικό που έχει σχεδιαστεί για να παρέχει απομακρυσμένο έλεγχο του υπολογιστή ή του σταθμού εργασίας. Αυτός ο τύπος απομακρυσμένης πρόσβασης παρακάμπτει τις εγκεκριμένες εξαιρετικά ασφαλείς μεθόδους απομακρυσμένης πρόσβασης και αποτελεί απειλή για την ασφάλεια ολόκληρου του δικτύου.

## 9. ΑΝΤΙΜΕΤΏΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΏΝ ΚΑΙ ΑΝΑΦΟΡΆ ΠΑΡΑΒΊΑΣΗΣ ΔΕΔΟΜΈΝΩΝ

Σε περίπτωση περιστατικού ασφαλείας, είναι σημαντικό οι Εργαζόμενοι της Phoenix Tower να είναι σε θέση να αναγνωρίσουν και να αντιδράσουν κατάλληλα. Κάθε πιθανό περιστατικό θα διερευνάται σε επίπεδο που κρίνεται κατάλληλο από τη Νομική Υπηρεσία και το τμήμα IT. Η σωστή και έγκαιρη αντιμετώπιση περιστατικών ασφαλείας πληροφοριών θα συμβάλει στην προστασία των περιουσιακών στοιχείων της Phoenix Tower.

## 9.1 Αναφορά

- Κάθε εργαζόμενος είναι υπεύθυνος για την άμεση αναφορά όλων των εντοπισμένων ή ύποπτων αδυναμιών ασφαλείας πληροφοριών, συμπεριλαμβανομένων ενδεικτικά πιθανών ή πραγματικών παραβιάσεων δεδομένων PII, στο τμήμα IT και/ή στο Νομικό Τμήμα/Τμήμα Συμμόρφωσης:
    - Γραμμή επικοινωνίας: 1-844-348-5247 ή https://secure.ethicspoint.com
    - Διεύθυνση ηλεκτρονικού ταχυδρομείου: privacy@phoenixintnl.com
- Η παραβίαση της εμπιστευτικότητας ή η μη εξουσιοδοτημένη αποκάλυψη Εμπιστευτικών Πληροφοριών της Phoenix Tower θεωρείται επίσης περιστατικό ασφαλείας πληροφοριών και πρέπει να αναφέρεται όπως περιγράφεται ανωτέρω.
- Το τμήμα IT θα καταγράφει τα αναφερόμενα περιστατικά ασφαλείας για να παρακολουθεί τόσο τους τύπους των περιστατικών ασφαλείας όσο και τον όγκο των περιστατικών που συμβαίνουν στην Phoenix Tower.
- Τα αποδεικτικά στοιχεία που σχετίζονται με παραβίαση της ασφαλείας των πληροφοριών πρέπει να συλλέγονται δεόντως σύμφωνα με τις οδηγίες του διευθυντή του τμήματος IT και να διαβιβάζονται στο τμήμα IT. Πρέπει να συλλέγονται για τη συμμόρφωση με τις νομοθετικές, κανονιστικές ή συμβατικές υποχρεώσεις και την αποφυγή παραβιάσεων του ποινικού ή αστικού δικαίου.
- Μετά τη διεξαγωγή μιας αρχικής έρευνας, ο διευθυντής του τμήματος IT θα καθορίσει εάν το συμβάν είναι πράγματι περιστατικό ασφαλείας πληροφοριών. Εάν έχει συμβεί ένα περιστατικό ασφαλείας, η Νομική Υπηρεσία θα καθορίσει εάν το περιστατικό συνιστά παραβίαση δεδομένων για την οποία απαιτείται αναφορά, καθώς και για τις παραβιάσεις δεδομένων που αφορούν PII.
- Η νομική υπηρεσία θα διατηρεί αρχείο των αναφερόμενων περιστατικών ασφαλείας που συνιστούν παραβίαση δεδομένων.
- Οι πληροφορίες που αφορούν περιστατικά ασφαλείας πληροφοριών μπορούν να δημοσιοποιούνται μόνο από εξουσιοδοτημένα πρόσωπα. Οι εργαζόμενοι δεν μπορούν να δημοσιοποιούν πληροφορίες σχετικά με ένα περιστατικό ασφαλείας εκτός της PTI χωρίς τη ρητή άδεια της Νομικής ομάδας.
- Μετά το περιστατικό ή την παραβίαση δεδομένων, το τμήμα IT θα είναι υπεύθυνο για τη διεξαγωγή συνάντησης με όλους τους επηρεαζόμενους/αρμόδιους Εργαζομένους και μέρη για να επανεξετάσει τα αποτελέσματα της έρευνας και να συζητήσει τη βασική αιτία του περιστατικού. Κάθε Εργαζόμενος που εμπλέκεται στην ανακάλυψη ή τη διερεύνηση ενός
- περιστατικού ασφαλείας πρέπει να παρευρίσκεται σε αυτή τη συνάντηση.
- Οι υπάλληλοι της Phoenix Tower ή οι τρίτοι εργολάβοι που εμπλέκονται σε περιστατικό ασφαλείας ή διαπιστώνεται ότι έχουν παραβιάσει την Πολιτική Ασφαλείας Πληροφοριών της Phoenix Tower, ανεξαρτήτως πρόθεσης, θα βρεθούν αντιμέτωποι με πειθαρχική επιτροπή, η οποία θα καθορίσει την υπαιτιότητα, τη διορθωτική και άλλη κατάλληλη δράση.

## 9.2 Κοινοποίηση της παραβίασης δεδομένων

- **Κοινοποίηση στην εποπτική αρχή:** η PTI, ως Υπεύθυνος Επεξεργασίας Δεδομένων θα γνωστοποιεί στην Εθνική Εποπτική Αρχή αμέσως (όταν λάβει γνώση του περιστατικού) και, το αργότερο, εντός 72 ωρών από τη στιγμή που έλαβε γνώση του περιστατικού, συμπεριλαμβανομένων των ωρών που παρήλθαν κατά τη διάρκεια των Σαββατοκύριακων και των αργιών. Για την επικοινωνία, η PTI θα πρέπει να χρησιμοποιεί το έντυπο κοινοποίησης, ανά χώρα, που προβλέπεται στη **Διαδικασία Διαχείρισης Συμβάντων**.

- **Ενημέρωση των υποκειμένων των δεδομένων:** Η PTI, ως υπεύθυνος επεξεργασίας δεδομένων, οφείλει να ενημερώνει τους θιγόμενους για παραβιάσεις ασφαλείας όταν η παραβίαση θα μπορούσε να έχει αρνητικό αντίκτυπο στα προσωπικά τους δεδομένα ή στην ιδιωτική τους ζωή.

## 10. ΑΠΟΡΡΗΤΟ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ

Η PTI δεσμεύεται να λάβει τα τεχνικά και οργανωτικά μέτρα που είναι αναγκαία για την εφαρμογή των διατάξεων και των αρχών της προστασίας των δεδομένων και, ως εκ τούτου, για την εξασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων. Για τον σκοπό αυτό, η PTI πρέπει να εξετάζει τη λήψη των αναγκαίων νομικών, τεχνικών και οργανωτικών μέτρων από τη φάση ανάπτυξης και σχεδιασμού των προϊόντων και υπηρεσιών ή από την αρχική στιγμή που προτείνεται από την PTI οποιοδήποτε έργο, πρωτοβουλία ή ιδέα που περιλαμβάνει την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα.

Για την εφαρμογή των νομικών μέτρων πρέπει να ζητείται η γνώμη του Υπεύθυνου για τα θέματα προστασίας δεδομένων, ενώ για τα τεχνικά και οργανωτικά μέτρα πρέπει να ζητείται η γνώμη του επικεφαλής του τμήματος IT.

Για το σκοπό αυτό, κάθε υπεύθυνος τομέα, έργου ή νέας διαδικασίας πρέπει να διασφαλίζει ότι η προστασία της ιδιωτικής ζωής εφαρμόζεται κατά τον σχεδιασμό και εξ ορισμού, επιπλέον προς τη συμμόρφωση με τις βασικές αρχές του κανονισμού.

## 11. ΠΡΌΣΘΕΤΑ ΜΈΤΡΑ ΑΣΦΑΛΕΊΑΣ

Για την προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών, η PTI έχει εφαρμόσει τα ακόλουθα μέτρα ασφαλείας:

### 11.1 Ανίχνευση και διαχείριση ευπαθειών και κακόβουλου λογισμικού.

Σε σχέση με τη συνεχή διαδικασία ανίχνευσης και διαχείρισης ευπαθειών, αυτό το μέτρο ασφαλείας εφαρμόζεται για τον εντοπισμό, την αξιολόγηση, την αντιμετώπιση και την αναφορά των ευπαθειών ασφαλείας των συστημάτων. Για τον σκοπό αυτό, η PTI έχει εφαρμόσει τα εργαλεία Microsoft Defender και Zscaler για την ανίχνευση και τη διαχείριση των ευπαθειών και του κακόβουλου λογισμικού.

## 11.2 Πολιτική Διαχείρισης Διορθώσεων

Σε σχέση με τη διαχείριση των διορθώσεων, η PTI έχει αναπτύξει μια πολιτική διαχείρισης διορθώσεων, η οποία αναφέρει ότι οι διορθώσεις που δημοσιεύονται από τη Microsoft θα εγκαθίστανται ως Intune, Zero day. Έλεγχος Πρόσβασης στο Δίκτυο.

## 11.3 Μηχανισμοί Κρυπτογράφησης

Όσον αφορά τους μηχανισμούς κρυπτογράφησης, η PTI έχει εφαρμόσει τέτοιους μηχανισμούς, τόσο στη βάση δεδομένων όσο και στον σκληρό δίσκο των φορητών υπολογιστών. Με αυτόν τον τρόπο, οι πληροφορίες που είναι αποθηκευμένες στις συσκευές δεν είναι προσβάσιμες σε περίπτωση μη εξουσιοδοτημένης πρόσβασης. Χρησιμοποιούνται μηχανισμοί κρυπτογράφησης, τόσο στις βάσεις δεδομένων όσο και στον σκληρό δίσκο των φορητών υπολογιστών. Σε αυτήν την περίπτωση, έχει εφαρμοστεί ένας μηχανισμός διαγραφής, σε περίπτωση απώλειας ή κλοπής του εξοπλισμού, ο οποίος, επιπλέον προς τα μέτρα ασφαλείας κρυπτογράφησης δεδομένων, μπορεί να εκτελέσει απομακρυσμένη διαγραφή.

## 11.4 Διαχείριση Λογαριασμού

Σε σχέση με τη διαχείριση λογαριασμού. Η PTI έχει εφαρμόσει μηχανισμούς που αναφέρονται ως Privileged Identity Management (PIM) και Privileged Access Management (PAM).