

## ΣΚΟΠΟΣ ΚΑΙ ΣΤΟΧΟΙ

Σκοπός της Πολιτικής Ασφάλειας Πληροφοριών είναι η διασφάλιση της συνέχειας των λειτουργιών της *SPEED AIR* και η ελαχιστοποίηση των επιχειρηματικών ζημιών. Αυτό επιτυγχάνεται με την πρόληψη και την ελαχιστοποίηση των επιπτώσεων των συμβάντων ασφάλειας.

Η Διοίκηση και όλοι οι εργαζόμενοι δεσμεύονται στην τήρηση Πολιτικών και Διαδικασιών για την Ασφάλεια Πληροφοριών σύμφωνα με τους εκάστοτε επιχειρηματικούς στόχους και σύμφωνα με όλες τις ισχύουσες ρυθμιστικές απαιτήσεις.

Για το σκοπό αυτό, η *SPEED AIR*:

- Αναπτύσσει και εφαρμόζει πολιτικές και διαδικασίες, λαμβάνοντας υπόψη την προστασία των πληροφοριακών στοιχείων του οργανισμού από όλες τις απειλές, εσωτερικές και εξωτερικές
- Υποχρεούται να συμμορφώνεται με τις επιχειρηματικές και νομικές απαιτήσεις και τις συμβατικές υποχρεώσεις ασφάλειας
- Εξασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων
- Διαθέτει συστήματα προστασίας από μη εξουσιοδοτημένη πρόσβαση
- Δημιουργεί μηχανισμούς για τον εντοπισμό και την επανεξέταση του κινδύνου και των επιπτώσεων των παραβιάσεων σε προστατευμένες πληροφορίες
- Έχει θεσπίσει μηχανισμούς για συνεχή αναγνώριση, αξιολόγηση και αντιμετώπιση των απειλών της ασφάλειας των πληροφοριών
- Αναθεωρεί τακτικά το στρατηγικό πλαίσιο διαχείρισης του κινδύνου
- Καλλιεργεί την εμπιστοσύνη των πελατών, ενεργώντας σύμφωνα με τα πρότυπα ασφαλείας και συστημάτων ελέγχου
- Αναλαμβάνει τη δέσμευση να βελτιώνει συνεχώς το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών μέσω της καθιέρωσης και της τακτικής επανεξέτασης μετρήσιμων στόχων ασφαλείας
- Αναπτύσσει, υλοποιεί και δοκιμάζει πλάνα αποκατάστασης και Συνέχειας Λειτουργιών
- Επικοινωνεί όλες τις σχετικές πολιτικές ασφάλειας στους υπαλλήλους, τους συνεργάτες και άλλα ενδιαφερόμενα μέρη, ανάλογα με την περίπτωση
- Διατηρεί και βελτιώνει την προστασία της ασφάλειας πληροφοριών από όλο το προσωπικό με την παροχή πληροφοριακού υλικού και σχετικών εκπαιδεύσεων.

Η πολιτική αυτή εφαρμόζεται σε συνδυασμό με άλλες, επιμέρους πολιτικές, πρότυπα και διαδικασίες της *SPEED AIR*.

## Πεδίο Εφαρμογής

Αυτή η πολιτική ισχύει για όλους τους χρήστες πληροφοριών και πληροφοριακών πόρων, όπως:

- Οι υπάλληλοι της εταιρείας,
- Οι υπάλληλοι γραφείων προσωρινής απασχόλησης που εργάζονται για τη *SPEED AIR*,
- Οι επιχειρηματικοί εταίροι και το ανάδοχο προσωπικό,

- Συνδεδεμένοι εταίροι της SPEED AIR ή τρίτοι, συμπεριλαμβανομένων προμηθευτών, προμηθευτών συστημάτων επεξεργασίας δεδομένων και ελέγχου διαδικασιών που κατέχουν ή χρησιμοποιούν πληροφορίες ή / και εγκαταστάσεις που ανήκουν στην SPEED AIR.

Αυτή η πολιτική καλύπτει όλα τα περιβάλλοντα Πληροφοριακών Συστημάτων που ανήκουν στην εταιρεία ή παρέχονται συμβεβλημένα με τρίτους για χρήση από την SPEED AIR.

Τοποθεσίες: Το πεδίο εφαρμογής περιλαμβάνει όλες τις τοποθεσίες, εγκαταστάσεις και σημεία παρουσίας της SPEED AIR.

Κατηγορίες περιουσιακών στοιχείων: Το πεδίο εφαρμογής καλύπτει τις ακόλουθες κατηγορίες περιουσιακών στοιχείων:

- Εξοπλισμό
- Λογισμικό
- Πληροφορίες
- Υπηρεσίες πληροφόρησης και επεξεργασίας
- Ανθρώπινο Δυναμικό.

Περισσότερες λεπτομέρειες σχετικά με τα πληροφοριακά αγαθά, μέσα ή πόρους καταγράφονται στο αντίστοιχο αρχείο απογραφής εξοπλισμού.

## **ΔΕΣΜΕΥΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

Η Διοίκηση της *SPEED AIR* δεσμεύεται να παρέχει συνεχώς την κατεύθυνση και υποστήριξη για την εφαρμογή των απαιτήσεων ασφάλειας σε όλη την εταιρεία.

Η Διοίκηση της *SPEED AIR* έχει καθορίσει ένα καλά δομημένο Πλαίσιο Ασφάλειας Πληροφοριών για την ανάπτυξη, τον έλεγχο και τη διατήρηση της ασφάλειας των πληροφοριών σύμφωνα με τους επιχειρηματικούς στόχους.

Η Διοίκηση της *SPEED AIR* δεσμεύεται και διασφαλίζει ότι η Εταιρική Πολιτική Ασφάλειας θα επανεξετάζεται τακτικά για να επιβεβαιώνεται η εκπλήρωση των επιχειρηματικών στόχων και άλλων απαιτήσεων, η επάρκεια και η αποτελεσματικότητά της, καθώς και η σχετική επικοινωνία με όλους τους υπαλλήλους και τα εξωτερικά ενδιαφερόμενα μέρη.

Η διεύθυνση και το προσωπικό της *SPEED AIR* υποχρεούνται να συμμορφώνονται με τις σχετικές Πολιτικές και Διαδικασίες Ασφαλείας. Όλοι οι χρήστες πρέπει να διαβάσουν, να κατανοήσουν και να συμμορφωθούν με αυτήν την πολιτική και άλλες σχετικές πολιτικές, πρότυπα και διαδικασίες ασφάλειας πληροφοριών. Περαιτέρω πληροφορίες ή διευκρινίσεις παρέχονται από τους αντίστοιχους προϊσταμένους ή και τον Υπεύθυνο Ασφάλειας Πληροφοριών.

## **ΣΤΡΑΤΗΓΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ**

Ασφάλεια πληροφοριών είναι η προστασία των πληροφοριών από απώλειες που προκύπτουν από παραβιάσεις της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Δεν πρέπει να θεωρείται ούτε να αποτελεί προληπτικό ή περιοριστικό παράγοντα των επιχειρηματικών δραστηριοτήτων, αλλά ως μηχανισμός που επιτρέπει την ασφαλή ανταλλαγή πληροφοριών.

Η ασφάλεια των πληροφοριών προστατεύει τις πληροφορίες από ένα ευρύ φάσμα απειλών, προκειμένου να διασφαλιστεί η ομαλή λειτουργία της επιχείρησης, να ελαχιστοποιηθούν οι επιχειρηματικές ζημιές και να μεγιστοποιηθεί η απόδοση των επενδύσεων και των επιχειρηματικών ευκαιριών.

Ο τελικός στόχος της Πολιτικής Ασφάλειας Πληροφοριών της *SPEED AIR* είναι να εξασφαλίσει τα ακόλουθα:

- Οι πληροφορίες προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και διατηρείται η εμπιστευτικότητα των πληροφοριών,
- Διατηρείται η ακεραιότητα των πληροφοριών μέσω της προστασίας από μη εξουσιοδοτημένη τροποποίηση
- Εξασφαλίζεται η διαθεσιμότητα πληροφοριών στους εξουσιοδοτημένους χρήστες εάν και όποτε απαιτείται
- πληρούνται οι κανονιστικές, νομοθετικές και άλλες απαιτήσεις
- Διευκολύνονται οι επιχειρηματικοί στόχοι

Όλοι οι υπάλληλοι της *SPEED AIR*, οι εμπλεκόμενοι και τα τρίτα μέρη τηρούν αυτή την πολιτική ασφάλειας πληροφοριών και τις κατάλληλες επι μέρους πολιτικές και διαδικασίες υποστήριξης. Αυτές οι πολιτικές ακολουθούν τις καλύτερες πρακτικές ασφαλείας.

## ΡΟΛΟΙ ΚΑΙ ΕΥΘΥΝΕΣ

Όλοι οι χρήστες που έχουν πρόσβαση σε εταιρικούς πόρους πληροφοριών είναι υπεύθυνοι για την αποτελεσματική προστασία των δεδομένων. Η ανάθεση συγκεκριμένων ρόλων και ευθυνών είναι απαραίτητη όσον αφορά την ασφάλεια πληροφοριών και την εφαρμογή του συστήματος Ασφαλείας.

Οι κύριοι ρόλοι και οι ευθύνες αναφορικά με την ασφάλεια των πληροφοριών καθορίζονται και τεκμηριώνονται ως μέρος της περιγραφής των θέσεων εργασίας και εγκρίνονται από τη Διοίκηση.

Η διοίκηση διασφαλίζει ότι υπάρχουν όλοι οι απαραίτητοι ανθρώπινοι πόροι, και ότι οι δεξιότητες και οι ικανότητες τους παραμένουν αποτελεσματικές με την αντίστοιχη υποστήριξη π.χ. εκπαίδευση, εργαλεία κλπ.

## ΠΟΛΙΤΙΚΕΣ ΚΑΙ ΔΙΑΔΙΚΑΣΙΕΣ

Η ασφάλεια Πληροφοριών επιτυγχάνεται με την εφαρμογή πρακτικών σύμφωνα με καθορισμένες εταιρικές πολιτικές και διαδικασίες. Αυτοί οι έλεγχοι, οι πολιτικές και οι διαδικασίες μπορούν να ομαδοποιηθούν στις ακόλουθες ομάδες:

- **Διαχείριση της ίδιας της Ασφάλειας Πληροφοριών**  
Στόχος είναι η παροχή κατευθύνσεων και υποστήριξης από τη Διοίκηση για την ασφάλεια των πληροφοριών σύμφωνα με τις επιχειρηματικές απαιτήσεις και τους σχετικούς νόμους και κανονισμούς. Καθορίζει τον τρόπο με τον οποίο γράφονται και αναθεωρούνται οι πολιτικές.
- **Οργάνωση της Ασφάλειας Πληροφοριών**  
Στόχος είναι η δημιουργία ενός πλαισίου διαχείρισης για την έναρξη και τον έλεγχο της εφαρμογής και της λειτουργίας της ασφάλειας των πληροφοριών εντός του οργανισμού. Καθορίζει την ανάθεση αρμοδιοτήτων και διαδικασιών που σχετίζονται με την ασφάλεια, και θέματα όπως η επικοινωνία με τις Αρχές και άλλους εξωτερικούς φορείς.
- **Φορητές συσκευές, ιδιόκτητες συσκευές και Τηλε-εργασία**  
Στόχος είναι να εξασφαλιστεί η ασφάλεια της τηλε-εργασίας και της χρήσης κινητών συσκευών

- **Ασφάλεια Ανθρώπινων Πόρων**  
Σκοπός είναι να διασφαλιστεί ότι οι εργαζόμενοι και οι συμβασιούχοι, είναι κατάλληλοι για τους ρόλους τους, γνωρίζουν, κατανοούν και εκπληρώνουν τις ευθύνες τους για την ασφάλεια των πληροφοριών. Περιλαμβάνει τους ελέγχους πριν, κατά τη διάρκεια και μετά την απασχόληση.
- **Διαχείριση περιουσιακών στοιχείων**  
Αποσκοπεί στο να προσδιορίσει τα περιουσιακά στοιχεία αποθήκευσης και επεξεργασίας, συμπεριλαμβανομένων των πληροφοριών και να ορίσει τις κατάλληλες ευθύνες προστασίας βάσει διαβάθμισης της αξίας και της κρισιμότητάς τους.
- **Έλεγχος πρόσβασης**  
Στόχος είναι ο περιορισμός της πρόσβασης σε πληροφορίες και εγκαταστάσεις επεξεργασίας πληροφοριών, συστημάτων και εφαρμογών, ώστε να επιτρέπεται μόνο η εξουσιοδοτημένη πρόσβαση και να εμποδίζεται η μη εξουσιοδοτημένη πρόσβαση.
- **Κρυπτογραφία**  
Στόχος είναι να προσδιοριστούν οι έλεγχοι και τα μέτρα σχετικά με τη χρήση της κρυπτογραφίας
- **Φυσική και περιβαλλοντική ασφάλεια**  
Σκοπός είναι να οριστούν οι χώροι, τα όρια τους, οι ασφαλείς περιοχές και οι δέοντες έλεγχοι εισόδου, για προστασία από απειλές, ασφάλεια του εξοπλισμού, ασφαλή απομάκρυνση, καθαρό γραφείο και «καθαρή» οθόνη κ.λπ.
- **Διαχείριση λειτουργιών**  
Στόχος είναι ο καθορισμός ελέγχων στις διαδικασίες λειτουργίας, η προστασία από κακόβουλο λογισμικό και απώλεια δεδομένων, η καταγραφή, η παρακολούθηση, η εγκατάσταση, η πρόληψη τρωτών σημείων, ο έλεγχος κ.λπ. εξοπλισμού και συστημάτων
- **Επικοινωνίες**  
Στόχος είναι η προστασία της ασφάλειας των πληροφοριών σε δίκτυα, η ασφαλής μεταφορά πληροφοριών, η ασφαλής αποστολή e-mail
- **Απόκτηση, Ανάπτυξη και Συντήρηση Πληροφοριακού Συστήματος**  
Στόχος είναι να διασφαλιστεί ότι η απόκτηση, ανάπτυξη και δοκιμή συστημάτων επεξεργασίας πληροφοριών γίνονται πάντα κατά τρόπο που να εξασφαλίζεται η ασφάλεια πληροφοριών
- **Σχέσεις με Προμηθευτές**  
Καθορίζει τους ελέγχους που πρέπει να συμπεριλαμβάνονται στις συμφωνίες και τον τρόπο παρακολούθησης των προμηθευτών
- **Διαχείριση Περιστατικών Ασφάλειας Πληροφοριών**  
Στόχος είναι να εξασφαλιστεί συνεπής και αποτελεσματική διαχείριση περιστατικών ασφάλειας πληροφοριών, συμπεριλαμβανομένης της εκτίμησης των συμβάντων, της ανταπόκρισης, της συλλογής αποδεικτικών στοιχείων, της επικοινωνίας σχετικά με τα γεγονότα και της απόκτησης γνώσεων και εμπειριών από περιστατικά.
- **Διαχείριση Επιχειρηματικής Συνέχειας**  
Στόχος είναι να διασφαλιστεί η διαθεσιμότητα πληροφοριών και μέσων για την επεξεργασία τους, σε κάθε περίπτωση, όπως και μετά από γεγονός που θα προκαλέσει αδυναμία χρήσης των συνηθών εγκαταστάσεων της εταιρείας
- **Συμμόρφωση**  
Στοχεύει στον καθορισμό ελέγχων για τον προσδιορισμό των εφαρμοστέων νόμων και κανονισμών, την προστασία της πνευματικής ιδιοκτησίας και την προστασία των προσωπικών δεδομένων των φυσικών προσώπων

Η Διοίκηση της *SPEED AIR* δεσμεύεται για το σύνολο των Πολιτικών και Διαδικασιών Ασφάλειας Πληροφοριών και διασφαλίζει ότι η πολιτική αυτή κοινοποιείται, είναι κατανοητή, υλοποιείται και διατηρείται σε όλα τα επίπεδα του οργανισμού καθώς και ότι επανεξετάζεται τακτικά για συνεχή καταλληλότητα.