



Audit Tax & Business Advisory

ΠΟΛΙΤΙΚΗ ΠΛ01
ΓΕΝΙΚΗ ΠΟΛΙΤΙΚΗ
ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

1. Σκοπός Πολιτικής

Η **PKF ΕΥΡΩΕΛΕΓΚΤΙΚΗ Α.Ε.** επιδιώκει την παροχή υπηρεσιών οικονομικών και φορολογικών ελέγχων και συμβουλευτικής επί χρηματοοικονομικών θεμάτων στους πελάτες της καθώς και διαχείρισης κινδύνων και παροχή υπηρεσιών εσωτερικού ελέγχου, σύμφωνα με το ισχύον Νομικό και Κανονιστικό πλαίσιο και τις λοιπές συμβατικές υποχρεώσεις της, με τρόπο που να προστατεύονται οι πληροφορίες από εκούσια ή ακούσια κλοπή, καταστροφή, ή χρήση κατά παράβαση των Νόμων και των Κανονιστικών Διατάξεων.

Ο σκοπός της Ασφαλείας Πληροφοριών είναι να διασφαλίσει την επιχειρησιακή συνέχεια της Εταιρείας και να ελαχιστοποιήσει τους κινδύνους που απειλούν τις πληροφορίες, αποφεύγοντας περιστατικά ασφαλείας και μειώνοντας τις επιπτώσεις που μπορεί να έχουν τα περιστατικά αυτά.

2. Πεδίο Εφαρμογής

Η Γενική Πολιτική Ασφαλείας Πληροφοριών εφαρμόζεται από όλο το προσωπικό της Εταιρείας που εμπλέκεται στην εκτέλεση των υπηρεσιών, καθώς επίσης και στο χρησιμοποιούμενο εξοπλισμό, αλλά και στις εγκαταστάσεις που χρησιμοποιεί η **PKF ΕΥΡΩΕΛΕΓΚΤΙΚΗ Α.Ε.** στο πλαίσιο εκτέλεσης των υπηρεσιών, συμπεριλαμβανομένων των όποιων πρόσθετων όρων των σχετικών συμβάσεων.

3. Ανάλυση Πολιτικής

3.1 ΓΕΝΙΚΑ

Στόχος της παρούσας πολιτικής είναι να προστατέψει τα πληροφοριακά περιουσιακά στοιχεία της Εταιρείας και των ενδιαφερομένων μερών από όλες τις εσωτερικές, εξωτερικές, εκούσιες ή ακούσιες απειλές. Οι επιμέρους στόχοι της επιχείρησης σχετικά με την Ασφάλεια Πληροφοριών είναι:

- Οι Πληροφορίες να είναι προστατευμένες από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση.
- Να διασφαλίζεται η εμπιστευτικότητα των Πληροφοριών.
- Να διατηρείται η ακεραιότητα των Πληροφοριών.
- Να διατηρείται η διαθεσιμότητα των Πληροφοριών.
- Να διασφαλίζεται η τήρηση των νομικών και κανονιστικών απαιτήσεων.
- Να αναπτύσσονται, να διατηρούνται και να δοκιμάζονται Σχέδια Επιχειρησιακής Συνέχειας.
- Να παρέχεται εκπαίδευση πάνω στην Ασφάλεια Πληροφοριών για όλο το προσωπικό.
- Όλα τα πραγματικά ή καθ' υποψία περιστατικά ασφαλείας να αναφέρονται στον Υπεύθυνο Ενιαίου Διαχειριστικού Συστήματος και να διερευνώνται πλήρως.

Για την επίτευξη των παραπάνω στόχων έχουν αναπτυχθεί και εφαρμόζονται επιμέρους Πολιτικές Ασφαλείας και Διαδικασίες, όπου περιγράφονται οι κατευθύνσεις της Διοίκησης, ο Τρόπος Υλοποίησης της Πολιτικής ή της Διαδικασίας και όλες οι σχετικές αρμοδιότητες του προσωπικού. Όλο το προσωπικό και οι εξωτερικοί συνεργάτες (όταν αυτό απαιτείται) είναι υποχρεωμένοι να εφαρμόζουν τις Πολιτικές Ασφαλείας που εμπίπτουν στο πεδίο των δραστηριοτήτων τους.

Η Διοίκηση δεσμεύεται για την παροχή όλων των απαραίτητων πόρων και μέσων για την εφαρμογή της παρούσας και των επιμέρους Πολιτικών Ασφαλείας.

Για την τεκμηρίωση της εφαρμογής του Συστήματος Διαχείρισης Ασφαλείας Πληροφοριών στο πλαίσιο της εφαρμογής του Ενιαίου Διαχειριστικού Συστήματος, η Εταιρεία συμπληρώνει με ευθύνη του Υπευθύνου Ενιαίου Διαχειριστικού Συστήματος την **Δήλωση Εφαρμοσιμότητας E01/ΠΛ01**.

3.2 ΑΡΜΟΔΙΟΤΗΤΕΣ

3.2.1 Αρμοδιότητες Διοίκησης

Οι βασικές αρμοδιότητες της Διοίκησης σε σχέση με τη διαχείριση της Ασφαλείας Πληροφοριών στην Εταιρεία είναι:

- Η διαμόρφωση της πολιτικής της **PKF ΕΥΡΩΕΛΕΓΚΤΙΚΗ Α.Ε.** σε σχέση με την Ασφάλεια Πληροφοριών.
- Η έγκριση και η ανασκόπηση των Πολιτικών Ασφαλείας Πληροφοριών, καθώς και των σχετικών Διαδικασιών και Οδηγιών Εργασίας.
- Η έγκριση των Σχεδίων Διαχείρισης των Κινδύνων και των Σχεδίων Διαχείρισης Εκτάκτων Αναγκών (Εταιρικής Συνέχειας).
- Η διασφάλιση των πόρων που απαιτούνται για την αποτελεσματική εφαρμογή του Συστήματος Διαχείρισης Ασφαλείας Πληροφοριών, στο πλαίσιο της εφαρμογής του Ενιαίου Διαχειριστικού Συστήματος.
- Η δημιουργία των απαραίτητων συνθηκών στην Εταιρεία για την προώθηση της κατανόησης και εμπέδωσης από το προσωπικό του ρόλου και των ευθυνών του που συνδέονται με την Ασφάλεια Πληροφοριών.
- Η μέριμνα για τη συνεχή βελτίωση στο πλαίσιο της εφαρμογής του Ενιαίου Διαχειριστικού Συστήματος.
- Η λήψη αποφάσεων για την επιβολή κυρώσεων σε περιπτώσεις πειθαρχικών παραπτώματων σε σχέση με την Ασφάλεια Πληροφοριών.

3.2.2 Αρμοδιότητες Υπεύθυνου Ενιαίου Διαχειριστικού Συστήματος

Εκπρόσωπος της Διοίκησης σε θέματα Ασφαλείας Πληροφοριών είναι ο Υπεύθυνος Ενιαίου Διαχειριστικού Συστήματος (ΥΕΔΣ), που ορίζεται από αυτήν και επιπλέον των άλλων καθηκόντων του, έχει τις κάτωθι υπευθυνότητες:

- Συνεργασία με τη Διοίκηση για την ανάπτυξη Πολιτικών Ασφαλείας, Διαδικασιών και πρότυπων μεθόδων, σύμφωνα με την Γενική Πολιτική Ασφαλείας της Εταιρείας.
- Μέριμνα για την εφαρμογή, διατήρηση και παρακολούθηση των Πολιτικών Ασφαλείας, ώστε να διασφαλίζεται η τήρηση των νομοκανονιστικών απαιτήσεων, της εκάστοτε ισχύουσας νομοθεσίας και των απαιτήσεων των προτύπων.
- Ενημέρωση της Διοίκησης για την επίδοση και βελτίωση των Πολιτικών Ασφαλείας.
- Ενημέρωση του καταλόγου πληροφοριακών στοιχείων της Εταιρείας και διαβάθμιση της σπουδαιότητάς τους, σε συνεργασία με τα αρμόδια επιχειρησιακά στελέχη.
- Συντονισμός των στελεχών της επιχείρησης για τον εντοπισμό και την αξιολόγηση των κινδύνων που απειλούν τα πληροφοριακά αγαθά της **PKF ΕΥΡΩΕΛΕΓΚΤΙΚΗ Α.Ε.**
- Συνεργασία με τη Διοίκηση για τον καθορισμό των απαραίτητων ελέγχων για την αντιμετώπιση των κινδύνων.
- Παρακολούθηση και αναφορά στη Διοίκηση για οποιοδήποτε περιστατικό ασφαλείας και ενεργοποίηση του αντίστοιχου σχεδίου και στρατηγικής για την αντιμετώπιση και την αποφυγή επανεμφάνισής του.

- Παρακολούθηση της αποτελεσματικότητας των ελέγχων που εφαρμόζονται για την αντιμετώπιση των κινδύνων και αναφέρει σχετικά στη Διοίκηση.
- Οργάνωση και διενέργεια Εσωτερικών Επιθεωρήσεων για τον έλεγχο της αποτελεσματικότητας του Συστήματος.
- Επικοινωνία με εξωτερικούς Φορείς σε σχέση με τη Διαχείριση της Ασφαλείας Πληροφοριών.
- Μέριμνα για την εκπαίδευση του προσωπικού σχετικά με τη Διαχείριση της Ασφαλείας και τη σημασία της συμμετοχής στην εφαρμογή του Συστήματος.
- Προετοιμασία και συντονισμός της Ανασκόπησης του Ενιαίου Διαχειριστικού Συστήματος από την Διοίκηση.

Ο ΥΕΔΣ αναφέρεται απευθείας στην Διοίκηση για όλα τα θέματα σχετικά με την Ασφάλεια Πληροφοριών και είναι εξουσιοδοτημένος να ενεργεί για λογαριασμό της πάνω σ' αυτά.

3.2.3 Αρμοδιότητες Ομάδας Διαχείρισης Ασφαλείας Πληροφοριών

Ως μέλη της Ομάδας Διαχείρισης Ασφαλείας Πληροφοριών ορίζονται:

- Ο Υπεύθυνος Ενιαίου Διαχειριστικού Συστήματος (ΥΕΔΣ).
- Ο Υπεύθυνος ΙΤ.
- Ο Τεχνικός Ασφαλείας.

Οι βασικές αρμοδιότητες της Ομάδας Διαχείρισης Ασφαλείας Πληροφοριών είναι:

- Η εξέταση των δραστηριοτήτων της Εταιρείας που εμπίπτουν στο πεδίο εφαρμογής που σχετίζεται με την Ασφάλεια Πληροφοριών του Ενιαίου Διαχειριστικού Συστήματος και ο εντοπισμός των εμπλεκόμενων πληροφοριακών περιουσιακών στοιχείων και των κινδύνων που τα απειλούν.
- Η εκτίμηση και αξιολόγηση της επικινδυνότητας των εντοπισθέντων κινδύνων.
- Η εξέταση οι προτάσεις και η καταγραφή μέτρων ελέγχου για την αντιμετώπιση των κινδύνων.
- Η περιοδική ανασκόπηση της αποτελεσματικότητας των πλάνων διαχείρισης των κινδύνων.
- Ο εντοπισμός των περιπτώσεων κατάστασης εκτάκτου ανάγκης και συντονισμών των ενεργειών για την κατάρτιση και έγκριση σχεδίων εκτάκτου ανάγκης.
- Η ανασκόπηση της αποτελεσματικότητας των σχεδίων εκτάκτου ανάγκης.

3.2.4 Αρμοδιότητες Προσωπικού

Οι βασικές αρμοδιότητες του εμπλεκόμενου προσωπικού στο Ενιαίο Διαχειριστικό Σύστημα και ειδικότερα για την Διαχείριση Ασφαλείας της είναι:

- Η εφαρμογή των Πολιτικών Ασφαλείας, των σχετικών Διαδικασιών και οδηγιών εργασίας που εμπίπτουν κατά την εκτέλεση της εργασίας του.

- Η άμεση αναφορά στον ΥΕΔΣ οποιουδήποτε περιστατικού ασφαλείας εμπίπτει στην αντίληψή του.

4. Εφαρμογή Πολιτικής

Οποιοσδήποτε εργαζόμενος παραβιάσει την παρούσα Πολιτική Ασφαλείας μπορεί να υπόκειται σε πειθαρχικές κυρώσεις κατά την κρίση της Διοίκησης της Εταιρείας.