Όνομα Οργανισμού

Πολιτική Ανθρώπινου Δυναμικού

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Ανθρώπινου Δυναμικού |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

Πίνακας Περιεχομένων

[1. Σκοπός 4](#_Toc158630486)

[2. Πριν από την εργοδότηση 4](#_Toc158630487)

[2.1. Έλεγχοι επαλήθευσης 4](#_Toc158630488)

[2.2. Παράμετροι εργοδότησης 5](#_Toc158630489)

[3. Κατά την διάρκεια της εργοδότησης 5](#_Toc158630490)

[3.1. Ευθύνες της Διεύθυνσης 6](#_Toc158630491)

[3.2. Ρόλοι και αρμοδιότητες ασφάλειας πληροφοριών 6](#_Toc158630492)

[3.3. Εκπαίδευση, κατάρτιση και ευαισθητοποίηση 7](#_Toc158630493)

[3.4. Πειθαρχική διαδικασία 7](#_Toc158630494)

[4. Τερματισμός της εργοδότησης και αλλαγή της εργασίας 7](#_Toc158630495)

[4.1. Ευθύνες 8](#_Toc158630496)

[4.2. Επιστροφή περιουσιακών στοιχείων 8](#_Toc158630497)

[4.3. Αφαίρεση δικαιωμάτων πρόσβασης 9](#_Toc158630498)

[5. Αναγνώριση Κινδύνων 9](#_Toc158630499)

# Σκοπός

Σκοπός της Πολιτικής είναι να διασφαλίσει ότι το προσωπικό, προμηθευτές και τρίτοι που δραστηριοποιούνται εκ μέρους [Όνομα Οργανισμού], κατανοούν τις ευθύνες και τα καθήκοντα τους. Επιπρόσθετα, σκοπός της είναι να περιορίσει τον κίνδυνο απάτης και να προστατεύσει τα φυσικά και λογικά περιουσιακά στοιχεία [Όνομα Οργανισμού].

Η παρόν Πολιτική περιγράφει τις ενέργειες που πρέπει να γίνονται πριν, κατά τη διάρκεια, με τον τερματισμό ή με την αλλαγή απασχόλησης, του συμβολαίου, της συμφωνίας του προσωπικού ή προμηθευτών ή τρίτων, που δραστηριοποιούνται εκ μέρους [Όνομα Οργανισμού].

# Πριν από την εργοδότηση

Προκειμένου να αποφευχθεί κατάχρηση των πληροφοριών και των συστημάτων πληροφορικής [Όνομα Οργανισμού], ο Οργανισμός διασφαλίζει ότι υπάρχουν οι κατάλληλες ασφαλιστικές δικλείδες ώστε να εξασφαλιστεί ότι το προσωπικό είναι κατάλληλο για την εργασία που θα του ανατεθεί.

1) Μια αντικειμενική διαδικασία θα πρέπει να καθοριστεί σε συνδυασμό με το Τμήμα Ανθρώπινου Δυναμικού (ΑΔ) [Όνομα Οργανισμού] για όλες τις μελλοντικές προσλήψεις. Αυτή η διαδικασία πρέπει να λαμβάνει υπόψη την εκπαίδευση, την εμπειρία, τα προσόντα, τις αναφορές, κλπ.

2) Οι περιγραφές θέσεων εργασίας θα πρέπει να καθοριστούν ώστε να καλύπτουν το κατάλληλο και αναμενόμενο αποτέλεσμα κάθε ρόλου εργασίας.

3) Οι περιγραφές θέσεων εργασίας θα πρέπει να περιλαμβάνουν ευθύνες ασφάλειας πληροφοριών σε όλους τους απαιτούμενους ρόλους εργασίας.

4) Πριν από την πρόσληψη θα πρέπει να πραγματοποιείται κατάλληλη επαλήθευση ιστορικού, σύμφωνα με την ελληνική νομοθεσία ή άλλων απαιτήσεων, οι οποίες μπορεί να θεωρηθούν κατάλληλες. Τα αρχεία θα πρέπει να αποθηκεύονται στο προσωπικό αρχείο του υπαλλήλου.

5) Όλοι οι υποψήφιοι (συμπεριλαμβανομένων των εξωτερικών μερών) θα πρέπει να υπογράφουν «συμφωνία μη αποκάλυψης» (non-disclosure agreement - NDA).

# Έλεγχοι επαλήθευσης

Πριν από την εργοδότηση στον [Όνομα Οργανισμού], θα διενεργηθούν στους πιθανούς υπαλλήλους έλεγχοι επαλήθευσης των πληροφοριών που τους αφορούν. Τα αποτελέσματα των ελέγχων αυτών χρειάζεται να ληφθούν πριν να αποκτήσει ο υποψήφιος πρόσβαση στις πληροφορίες και στα συστήματα πληροφοριών [Όνομα Οργανισμού].

Τέτοιοι έλεγχοι επαλήθευσης περιλαμβάνουν τουλάχιστον τα ακόλουθα:

1. **Αίτηση**: Η αίτηση του υποψήφιου υπαλλήλου χρειάζεται να ελέγχεται από πλευράς πληρότητας.
2. **Ακαδημαϊκά** **και** **επαγγελματικά** **προσόντα**: Εάν καταγράφονται οποιαδήποτε ακαδημαϊκά ή επαγγελματικά προσόντα, αυτά χρειάζονται να επαληθευτούν με το πρωτότυπο πιστοποιητικό.
3. **Έλεγχος** **ταυτότητας**: Η ταυτότητα του υποψήφιου υπάλληλου χρειάζεται να ελέγχεται πριν από την πρόσληψη. Για την επαλήθευση της ταυτότητας μπορεί να χρησιμοποιηθεί δελτίο ταυτότητας, διαβατήριο, πιστοποιητικό γέννησης ή άδεια οδήγησης.
4. **Έλεγχο** **λευκού** **ποινικού** **μητρώου**.

Για περαιτέρω πληροφορίες σχετικά με τους ελέγχους επαλήθευσης σε Προμηθευτές και Τρίτους, ανατρέξτε στην Πολιτική Διαχείρισης Προμηθευτών.

# Παράμετροι εργοδότησης

Όλοι οι νεοεισερχόμενοι χρειάζεται να συμφωνήσουν και να υπογράψουν τις σχετικές παραμέτρους εργοδότησης με τον [Όνομα Οργανισμού], οι οποίες περιλαμβάνουν τα ακόλουθα:

* την ευθύνη για τη διαχείριση της ασφάλειας των πληροφοριών
* τη συμφωνία εμπιστευτικότητας (πριν την έναρξη της εργασίας και της πρόσβασης στις πληροφορίες και συστήματα πληροφοριών του Οργανισμού)

Όλοι οι υπάλληλοι του Οργανισμού θα τηρούν τον Νόμο και τους Κανονισμούς [Όνομα Οργανισμού] καθώς και τις εγκυκλίους/εσωτερικές οδηγίες του.

# Κατά την διάρκεια της εργοδότησης

Όλοι οι υπάλληλοι και οι εξωτερικοί συνεργάτες [Όνομα Οργανισμού] αναμένεται ότι γνωρίζουν και διασφαλίζουν τις ευθύνες τους σε σχέση με την ασφάλεια των πληροφοριών.

1) Όλοι οι χρήστες θα πρέπει να εκπαιδευτούν για την εκτέλεση καθηκόντων που σχετίζονται με τις απαιτήσεις ασφάλειας πληροφοριών των συγκεκριμένων ρόλων εργασίας.

2) Η συχνότητα αυτών των εκπαιδεύσεων θα πρέπει να καθορίζεται σε συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφοριών και το Τμήμα ΑΔ.

3) Η διαδικασία επαγωγής περιλαμβάνει θέματα ευαισθητοποίησης σχετικά με την ασφάλεια των πληροφοριών και, εάν απαιτείται, ειδικές εκπαιδεύσεις με βάση τους ρόλους εργασίας.

4) Όλοι οι εργαζόμενοι θα πρέπει να ενημερώνονται για τις πολιτικές ασφάλειας πληροφοριών [Όνομα Οργανισμού] καθώς και για την πειθαρχική διαδικασία σε περίπτωση μη συμμόρφωσης με αυτές τις πολιτικές.

5) Οποιοσδήποτε υπάλληλος παρεμβαίνει ή αρνείται να συνεργαστεί για τη διερεύνηση της μη συμμόρφωσης με αυτές τις πολιτικές θα πρέπει να υπόκειται σε πειθαρχικά μέτρα, έως και τη λήξη της εργασίας.

6) Τα αρχεία παρακολούθησης της κατάρτισης ή / και της ευαισθητοποίησης και οι λεπτομέρειες της εκπαίδευσης ή / και της ευαισθητοποίησης θα πρέπει να τεκμηριώνονται και να τηρούνται.

7) Το Τμήμα Ανθρώπινου Δυναμικού θα πρέπει να ενημερώνει αμέσως το Τμήμα Πληροφορικής για τις εσωτερικές μεταβιβάσεις εργαζομένων.

8) Το Τμήμα Πληροφορικής θα πρέπει να εξασφαλίζει την άμεση τροποποίηση των δικαιωμάτων λογικής πρόσβασης των υπαλλήλων μετά από ειδοποίηση από το Τμήμα ΑΔ.

9) Ο υπεύθυνος ασφάλειας πληροφοριών θα πρέπει να αναθεωρεί περιοδικά την καταλληλόλητα των λογικών και φυσικών δικαιωμάτων πρόσβασης σύμφωνα με τις ευθύνες εργασίας τους.

10) Πρέπει να υπάρχει τεκμηριωμένη πειθαρχική διαδικασία που να απεικονίζει ενέργειες που πρέπει να ληφθούν σε περίπτωση παραβίασης της ασφάλειας πληροφοριών.

11) Οι προϊστάμενοι των τμημάτων θα πρέπει να διασφαλίζουν επαρκή συμμετοχή των μελών της ομάδας τους για την εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια των πληροφοριών.

# Ευθύνες της Διεύθυνσης

Η Διεύθυνση, σε συνεργασία με τον Προϊστάμενο Ανθρώπινου Δυναμικού και τον Προϊστάμενο Ασφάλειας Πληροφοριών, είναι υπεύθυνη να διασφαλίσει ότι οι υπάλληλοι και οι εξωτερικοί συνεργάτες:

* γνωρίζουν τον ρόλο και τις ευθύνες τους σε σχέση με την ασφάλεια των πληροφοριών και τι αναμένεται από αυτούς
* έχουν επίπεδο γνώσεων ασφάλειας πληροφοριών ανάλογο με τον ρόλο τους
* συμμορφώνονται με τις παραμέτρους εργοδότησης, στους οποίους συμπεριλαμβάνεται η ασφάλεια πληροφοριών

# Ρόλοι και αρμοδιότητες ασφάλειας πληροφοριών

Συγκεκριμένοι υπάλληλοι [Όνομα Οργανισμού] είναι απαραίτητο όπως καταγράψουν τον ρόλο και τις αρμοδιότητες τους σε σχέση με την ασφάλεια πληροφοριών στην περιγραφή εργασίας τους.

Ο υπάλληλος χρειάζεται να περιλάβει στην περιγραφή εργασίας του αναφορά στην ασφάλεια πληροφοριών αν ισχύουν για την περίπτωση του ένα ή περισσότερα από τα πιο κάτω:

* Ιδιοκτήτης πολιτικών και διαδικασιών ασφάλειας πληροφοριών
* Συντονισμός και εποπτεία θεμάτων ασφάλειας πληροφοριών
* Ιδιοκτήτης πληροφορίας

# Εκπαίδευση, κατάρτιση και ευαισθητοποίηση

Όλοι οι υπάλληλοι [Όνομα Οργανισμού] και, κατά περίπτωση, οι εξωτερικοί συνεργάτες χρειάζεται να λάβουν κατάλληλη κατάρτιση και τακτικές ενημερώσεις σε σχέση με τις πολιτικές και διαδικασίες ασφάλειας πληροφοριών, ανάλογες με τη θέση εργασίας τους.

# Πειθαρχική διαδικασία

Χρειάζεται να υπάρχει καταγραμμένη επίσημη πειθαρχική διαδικασία, σύμφωνα με τους ισχύοντες νόμους και κανονισμούς, η οποία να έχει ήδη επικοινωνηθεί στους υπαλλήλους, ώστε να τυγχάνουν χειρισμό οι περιπτώσεις παραβίασης της ασφάλειας πληροφοριών.

Η διαδικασία αυτή ακολουθείται για τις περιπτώσεις σοβαρής γνωστής και αποδεδειγμένης παραβίασης ασφάλειας πληροφοριών, η οποία έχει υψηλό αντίκτυπο στον [Όνομα Οργανισμού] βάσει την αξιολόγηση κινδύνου. Στη διαδικασία προδιαγράφονται επίπεδα ώστε να λαμβάνονται υπόψη παράγοντες όπως η φύση και η βαρύτητα της παραβίασης και της επίπτωσης που αυτή θα έχει στον [Όνομα Οργανισμού], κατά πόσον είναι το πρώτο ή επαναλαμβανόμενο παράπτωμα.

Η υπό αναφορά διαδικασία λειτουργεί ως αποτρεπτική για ενδεχόμενη παραβίαση ασφάλειας πληροφοριών.

# Τερματισμός της εργοδότησης και αλλαγή της εργασίας

Το Τμήμα Διοίκησης και Ανθρώπινου Δυναμικού είναι υπεύθυνο να διασφαλίσει ότι υπάρχει καταγραμμένη διαδικασία τερματισμού της εργοδότησης ή αλλαγής της εργασίας διαφυλάσσοντας τα συμφέροντα του [Όνομα Οργανισμού]:

1) Το Τμήμα Ανθρώπινου Δυναμικού θα πρέπει να ειδοποιεί αμέσως τα αρμόδια τμήματα (π.χ. Τμήμα Πληροφορικής, κλπ.) για περιπτώσεις τερματισμού εργασίας ώστε να σχεδιάζονται άμεσα οι ενέργειες κατάργησης των δικαιωμάτων πρόσβασης και των προνομίων του υπαλλήλου.

2) Το Τμήμα Ανθρώπινου Δυναμικού πρέπει να περιλαμβάνει στην ειδοποίηση την τελευταία εργάσιμη ημέρα του χρήστη στον [Όνομα Οργανισμού].

3) Όλη η λογική και φυσική πρόσβαση πρέπει να ανακληθεί κατά την ημερομηνία διακανονισμού των οφειλών ή την ημερομηνία αναχώρησης από τον [Όνομα Οργανισμού] (όποιο είναι νωρίτερο).

4) Το Τμήμα Ανθρώπινου Δυναμικού, που έρχεται σε επαφή με άλλα τμήματα, θα πρέπει να επιβάλλει μια διαδικασία τερματισμού χρήστη, συμπεριλαμβανομένης της ανάκλησης των δικαιωμάτων πρόσβασης χρήστη και της επιστροφής αγαθών.

5) Όλα τα δικαιώματα πρόσβασης, είτε φυσικά είτε λογικά για τις εγκαταστάσεις επεξεργασίας πληροφοριών / πληροφορίες του [Όνομα Οργανισμού], θα πρέπει να ανακαλούνται στο τέλος της υπηρεσίας για κάθε χρήστη.

6) Το Τμήμα Ανθρώπινου Δυναμικού διασφαλίζει ότι όλοι εργαζόμενοι οι οποίοι παραιτούνται συμπληρώνουν ένα έντυπο τερματισμού εργασίας πριν αποχωρήσουν από τον [Όνομα Οργανισμού] καθώς και την διατήρηση των συγκεκριμένων αρχείων.

7) Το Τμήμα Ανθρώπινου Δυναμικού θα πρέπει να καθορίσει τα κανάλια από όπου θα ειδοποιούνται τα διάφορα τμήματα (π.χ. Τμήμα Πληροφορικής, κλπ.) για ανάκληση της λογικής και φυσικής πρόσβασης σε περιπτώσεις τερματισμού της εργασίας.

8) Ο εξοπλισμός που διατίθεται στον χρήστη θα πρέπει να κατασχεθεί με ασφάλεια για οποιαδήποτε περαιτέρω αναθεώρηση ή ενέργεια.

9) Η επικοινωνία και οι συντονισμένες ενέργειες που εμπλέκονται στη διαδικασία τερματισμού θα πρέπει να ελέγχονται και περιορίζονται σε συγκεκριμένα άτομα από τις κατάλληλες υπηρεσίες.

10) Ο απολυθείς υπάλληλος δεν επιτρέπεται να έχει πρόσβαση σε οποιαδήποτε πληροφορία ή εγκατάσταση επεξεργασίας πληροφοριών.

11) Ο απολυθείς υπάλληλος συνοδεύεται έξω από τις εγκαταστάσεις του οργανισμού, για να ολοκληρώσει τυχόν εκκρεμείς εργασίες της διαδικασίας τερματισμού.

Η προαναφερθείσα διαδικασία περιλαμβάνει τα ακόλουθα:

# Ευθύνες

Οι ευθύνες κατά τον τερματισμό ή αλλαγή της εργοδότησης χρειάζεται να καθοριστούν και να οριστούν στα αρμόδια άτομα.

Το Τμήμα Διοίκησης και Ανθρώπινου Δυναμικού είναι υπεύθυνο, σε συνεργασία με τον οικείο Προϊστάμενο και το Τμήμα Πληροφορικής, για την εφαρμογή της διαδικασίας τερματισμού της εργοδότησης ή αλλαγής της εργασίας. Στην περίπτωση τερματισμού της εργοδότησης, υπενθυμίζεται από τον Προϊστάμενο στον υπάλληλο η ανάγκη τήρησης συγκεκριμένων υποχρεώσεων και μετά την αποχώρηση του, όπως είναι η συμφωνία εμπιστευτικότητας, πνευματικής ιδιοκτησίας κ.ά.

# Επιστροφή περιουσιακών στοιχείων

Όλοι οι υπάλληλοι και εξωτερικοί συνεργάτες του [Όνομα Οργανισμού] χρειάζεται να επιστρέψουν όλα τα περιουσιακά στοιχεία του που έχουν στην κατοχή τους, πριν τον τερματισμό της εργοδότησης τους.

Το Τμήμα Διοίκησης και Ανθρώπινου Δυναμικού, σε συνεργασία με τον οικείο Προϊστάμενο και το Τμήμα Πληροφορικής, διασφαλίζει ότι οποιοδήποτε περιουσιακό στοιχείο ήταν στην κατοχή του υπαλλήλου που θα τερματίσει τις υπηρεσίες του επιστρέφεται στον Οργανισμό. Ως εκ τούτου, ακυρώνονται επίσης οι προσβάσεις τόσο στις εγκαταστάσεις του [Όνομα Οργανισμού] όσο και στα συστήματα πληροφορικής του. Στην περίπτωση που ο οικείος Προϊστάμενος κρίνει ότι ο εν λόγω υπάλληλος διαθέτει γνώσεις οι οποίες είναι απαραίτητες για την επιχειρησιακή συνέχεια του Οργανισμού, έχει την ευθύνη να διασφαλίσει τη μεταφορά τους σε δεύτερο υπάλληλο του Τμήματος/Υπηρεσίας.

# Αφαίρεση δικαιωμάτων πρόσβασης

Τα δικαιώματα πρόσβασης σε πληροφορίες και συστήματα επεξεργασίας πληροφοριών, των υπαλλήλων και των εξωτερικών συνεργατών, χρειάζεται να αφαιρεθούν αμέσως μετά τη λήξη της απασχόλησης, σύμβασης ή συμφωνίας, ή να ρυθμιστούν με την αλλαγή εργασίας.

Κατά τη λήψη της επιστολής παραίτησης υπαλλήλου, ο οικείος Προϊστάμενος κρίνει αν τα υφιστάμενα δικαιώματα πρόσβασης του υπαλλήλου χρειάζεται να επανεξεταστούν και να μειωθούν ενώ ακόμη εργάζεται και ενημερώνει ανάλογα το Τμήμα Πληροφορικής.

Με τον τερματισμό της εργοδότησης από τον [Όνομα Οργανισμού], τα δικαιώματα πρόσβασης υπαλλήλου απενεργοποιούνται άμεσα, και διαγράφονται οι λογαριασμοί όταν δεν είναι πλέον απαραίτητη η πρόσβαση.

Τα δικαιώματα πρόσβασης των υπαλλήλων του [Όνομα Οργανισμού] πρέπει να ελέγχονται από τον οικείο Προϊστάμενο όταν αλλάζουν οι ρόλοι τους, και ανακαλείται οποιαδήποτε πρόσβαση δεν είναι πλέον αναγκαία.

Σε όλες τις περιπτώσεις, το Τμήμα Διοίκησης και Ανθρώπινου Δυναμικού είναι απαραίτητο να ενημερώνει έγκαιρα τα αρμόδια άτομα ώστε να διεκπεραιωθούν οι ενέργειες του κάθε ενός, όπως για παράδειγμα:

* Το Τμήμα Πληροφορικής για τις προσβάσεις στα ηλεκτρονικά συστήματα
* Το Τμήμα Διοίκησης και Ανθρώπινου Δυναμικού για τις προσβάσεις στα κτήρια
* Η Υποδοχή, ώστε από την ημερομηνία τερματισμού το συγκεκριμένο άτομο να τυγχάνει χειρισμού ως επισκέπτης, κ.ά.

# Αναγνώριση Κινδύνων

Η διαδικασία αναγνώρισης κινδύνων στοχεύει στην αναγνώριση των κινδύνων που ενδέχεται να αντιμετωπίσει ο οργανισμός, σχετικά με το προσωπικό του.

1. Ρόλοι και Αρμοδιότητες:
* Υπεύθυνοι Ασφαλείας:

Ρόλος: Οργάνωση και εποπτεία της διαδικασίας αναγνώρισης κινδύνων.

Αρμοδιότητες: Καθοδήγηση ομάδων αναγνώρισης κινδύνων, αξιολόγηση αποτελεσμάτων.

* Ομάδες Αναγνώρισης Κινδύνων:

Ρόλος: Αναγνώριση κινδύνων στον τομέα τους.

Αρμοδιότητες: Συλλογή δεδομένων, ανάλυση τάσεων, αναγνώριση ευπαθειών.

* Διοίκηση Προσωπικού:

Ρόλος: Υποστήριξη στην αναγνώριση κινδύνων που αφορούν το προσωπικό.

Αρμοδιότητες: Παροχή πληροφοριών, συνεργασία με τις ομάδες αναγνώρισης.

1. Κριτήρια Αναγνώρισης Κινδύνων:
* Αναλυτική Εκτίμηση:

Αναλυτική αξιολόγηση των δραστηριοτήτων και του περιβάλλοντος εργασίας.

* Συχνότητα και Σοβαρότητα:

Ανάλυση συχνότητας και σοβαρότητας κινδύνων για προτεραιοποίηση.

* Συνεργασία με Ομάδες:

Ενσωμάτωση γνώσεων από διάφορες ομάδες για ολοκληρωμένη αναγνώριση.

1. Αρχεία Αναγνώρισης Κινδύνων:
* Αναφορές Ομάδων:

Αρχεία με τα αποτελέσματα των ομάδων αναγνώρισης.

* Αξιολογήσεις Προσωπικού:

Αρχεία που περιλαμβάνουν αξιολογήσεις κινδύνων σχετικά με το προσωπικό.

* Αναθεώρηση και Ενημέρωση