Όνομα Οργανισμού

Πολιτική Ανθρώπινου Δυναμικού & Εκπαίδευσης

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Ανθρώπινου Δυναμικού & Εκπαίδευσης |
| **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. Εισαγωγή 4](#_Toc188430335)

[1.1. Σκοπός 4](#_Toc188430336)

[1.2. Πεδίο Εφαρμογής 4](#_Toc188430337)

[2. Κύκλος Ζωής της εργοδότησης 4](#_Toc188430338)

[2.1. Πριν από την εργοδότηση 4](#_Toc188430339)

[2.2. Παράμετροι εργοδότησης 5](#_Toc188430340)

[3. Κατά την διάρκεια της εργοδότησης 5](#_Toc188430341)

[3.1. Ευθύνες της Διεύθυνσης 6](#_Toc188430342)

[3.2. Ρόλοι και αρμοδιότητες ασφάλειας πληροφοριών 7](#_Toc188430343)

[3.3. Εκπαίδευση, κατάρτιση και ευαισθητοποίηση 7](#_Toc188430344)

[3.3.1. Ετήσιο πρόγραμμα εκπαίδευσης 9](#_Toc188430345)

[3.3.2. Αποτελεσματικότητα του προγράμματος 9](#_Toc188430346)

[3.4. Πειθαρχική διαδικασία 9](#_Toc188430347)

[4. Τερματισμός της εργοδότησης ή αλλαγή της εργασίας 10](#_Toc188430348)

[4.1. Ευθύνες κατά τον τερματισμό 11](#_Toc188430349)

[4.2. Επιστροφή περιουσιακών στοιχείων 11](#_Toc188430350)

[4.3. Αφαίρεση δικαιωμάτων πρόσβασης 11](#_Toc188430351)

[5. Αναθεώρηση 12](#_Toc188430352)

[6. Αναφορές 13](#_Toc188430353)

# Εισαγωγή

# Σκοπός

Σκοπός της Πολιτικής Ανθρώπινου Δυναμικού και της Εκπαίδευσης είναι να διασφαλίσει την προστασία των δεδομένων και των συστημάτων πληροφορικής του [Όνομα Οργανισμού], μέσω της εκπαίδευσης και την ευαισθητοποίησης των υπαλλήλων, την καταγραφή πολιτικών και διαδικασιών για όλο το κύκλο ζωής της εργοδότησης και την ορθή προετοιμασία για την αναγνώριση και την αντιμετώπιση σχετικών απειλών κυβερνοασφάλειας.

# Πεδίο Εφαρμογής

Η παρούσα Πολιτική Ανθρώπινου Δυναμικού και της Εκπαίδευσης εφαρμόζεται σε όλο το προσωπικό και συνεργάτες του [ Όνομα Οργανισμού] καθώς και σε τρίτους φορείς που δραστηριοποιούνται εκ μέρους του, συμπεριλαμβανομένων προσωπικού που εργάζεται με ορισμένου χρόνου συμβάσεις, εξωτερικούς συνεργάτες και εκπαιδευόμενους.

Η πολιτική αυτή έχει σχεδιαστεί για να εξασφαλίσει την ασφάλεια, τη διαχείριση και την ευημερία όλων των προαναφερθέντων κατηγοριών προσωπικού, ενώ παράλληλα διασφαλίζει την συμμόρφωση με τις ισχύουσες νομοθετικές και κανονιστικές διατάξεις. . 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].

# Κύκλος Ζωής της εργοδότησης

# Πριν από την εργοδότηση

Προκειμένου να αποφευχθεί κατάχρηση των πληροφοριών και των συστημάτων πληροφορικής [Όνομα Οργανισμού], ο Οργανισμός διασφαλίζει ότι υπάρχουν οι απαραίτητες διαδικασίες ελέγχου ώστε να εξασφαλιστεί ότι το προσωπικό είναι κατάλληλο για την εργασία που θα του ανατεθεί πριν την πρόσληψη του στον [Όνομα Οργανισμού] .

Στον βαθμό που του επιτρέπει ο νόμος, θα πρέπει να καθορίσει μία διαδικασία και σε συνεργασία με το Τμήμα Ανθρώπινου Δυναμικού (ΑΔ) του [Όνομα Οργανισμού] για όλες τις μελλοντικές προσλήψεις.

Αυτή η διαδικασία πρέπει να λαμβάνει υπόψη την εκπαίδευση, την εμπειρία, τα προσόντα, τις αναφορές, κλπ. Μεταξύ άλλων θα πρέπει να καταγράφονται:

* Οι περιγραφές θέσεων εργασίας θα πρέπει να καθοριστούν ώστε να καλύπτουν το κατάλληλο και αναμενόμενο αποτέλεσμα κάθε ρόλου εργασίας. Οι περιγραφές θέσεων εργασίας θα πρέπει να περιλαμβάνουν μεταξύ άλλων και τις ευθύνες ασφάλειας πληροφοριών σε όλους τους απαιτούμενους ρόλους εργασίας.
* Πριν από την πρόσληψη θα πρέπει να πραγματοποιείται κατάλληλη επαλήθευση ιστορικού, της αίτησης με επαλήθευση ακαδημαϊκών και επαγγελματικών προσόντων, τόσο για εσωτερικούς όσο και για εξωτερικούς συνεργάτες και έλεγχο λευκού ποινικού μητρώου. Τα αρχεία θα πρέπει να αποθηκεύονται στο προσωπικό αρχείο του υπαλλήλου.

# Παράμετροι εργοδότησης

Όλοι οι νεοεισερχόμενοι χρειάζεται να συμφωνήσουν και να υπογράψουν τις σχετικές παραμέτρους/συμβάσεις εργοδότησης με τον [Όνομα Οργανισμού]. Οι συμβάσεις εργοδότησης των εργαζομένων πρέπει να ορίζουν με σαφήνεια τις υποχρεώσεις και τις ευθύνες των εργαζομένων για την ασφάλεια πληροφοριών. Οι κανόνες και πολιτικές ισχύουν τόσο για το προσωπικό του [Όνομα Οργανισμού] όσο και για τις υπηρεσίες που παρέχονται μέσω τρίτων μερών, επηρεάζοντας την ασφάλεια του [Όνομα Οργανισμού] .

Οι συμβάσεις θα πρέπει να περιλαμβάνουν μεταξύ άλλων τα ακόλουθα:

* την ευθύνη για τη διαχείριση της ασφάλειας των πληροφοριών σε όλο τον κύκλο ζωής της εργοδότηση τους, καθώς και την κατανόηση των ευθυνών των υπαλλήλων σχετικά με αυτές τις πληροφορίες.
* τη συμφωνία εμπιστευτικότητας (πριν την έναρξη της εργασίας και της πρόσβασης στις πληροφορίες και συστήματα πληροφοριών του Οργανισμού ). Την ευθύνη των υπάλληλων του Οργανισμού να τηρούν τους νόμους και τους κανονισμούς σχετικές με την εργασία του [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 έχουν εκπαιδευτεί για την εκτέλεση καθηκόντων που σχετίζονται με τις απαιτήσεις ασφάλειας πληροφοριών των συγκεκριμένων ρόλων εργασίας.

2) Η συχνότητα αυτών των εκπαιδεύσεων καθορίζεται σε συνεργασία με τον Υπεύθυνο Ασφάλειας Πληροφοριών και το Τμήμα Ανθρώπινου Δυναμικού του [Όνομα Οργανισμού].

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 Ανθρώπινου Δυναμικού.

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) Ύπαρξη τεκμηριωμένης πειθαρχικής διαδικασίας που να απεικονίζει ενέργειες που πρέπει να ληφθούν σε περίπτωση παραβίασης της ασφάλειας πληροφοριών.

11) Οι προϊστάμενοι των τμημάτων διασφαλίζουν την 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 Υπεύθυνο Ασφάλειας Πληροφοριών, είναι υπεύθυνοι να:

* καθορίσει και να καταγράψει τους ρόλους και τις αρμοδιότητες των εργαζομένων, ενημερώνοντάς τους για τις αντίστοιχες υποχρεώσεις και ευθύνες τους.
* καταρτίσει σχέδια εκπαίδευσης για να επιβεβαιώνει ότι οι υπάλληλοί έχουν επίπεδο γνώσεων ασφάλειας πληροφοριών ανάλογο με τον ρόλο τους και να συμμορφώνονται με τις παραμέτρους εργοδότησης, στους οποίους συμπεριλαμβάνεται η ασφάλεια πληροφοριών σύμφωνα με τις πρόνοιες της παραγράφου 3.3 πιο κάτω.
* διεξάγει τακτικούς και έκτακτους ελέγχους για να διασφαλίσει ότι οι υπάλληλοι γνωρίζουν τον ρόλο και τις ευθύνες τους και συμμορφώνονται με τις υποχρεώσεις και ευθύνες τους. Αυτοί οι έλεγχοι περιλαμβάνουν δοκιμές για την αξιολόγηση της αποτελεσματικότητας της εκπαίδευσης και της συμμόρφωσης με τις πολιτικές, διαδικασίες και μέτρα ασφαλείας του [Όνομα Οργανισμού] .
* αναλύσει τα αποτελέσματα των ελέγχων για να αξιολογηθεί η συμμόρφωση του προσωπικού. Σε περίπτωση εύρεσης προβλημάτων, πρέπει να ενεργοποιούνται οι ανάλογες διαδικασίες για την αντιμετώπιση είτε για περιστατικά ασφάλειας είτε για την εφαρμογή τυχόν πειθαρχικών ή άλλων μέτρων.

# Ρόλοι και αρμοδιότητες ασφάλειας πληροφοριών

Συγκεκριμένοι υπάλληλοι του [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 του [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. Στόχος του προγράμματος είναι η κατανόηση των βασικών αρχών ασφάλειας πληροφοριών και κυβερνοασφάλειας, η ευαισθητοποίηση σε σχέση με τις σύγχρονες κυβερνοαπειλές καθώς και η εκπαίδευση στην αντιμετώπιση κυβερνοεπιθέσεων και αντιδράσεις σε περιστατικά.

Πιο συγκεκριμένα:

* Ο [Όνομα Οργανισμού] πρέπει να εφαρμόζει ολιστικό πρόγραμμα εκπαίδευσης και ευαισθητοποίησης των εργαζομένων σχετικά με θέματα προστασίας και ασφάλειας πληροφοριών και να πραγματοποιεί δράσεις με στόχο την εξοικείωση των εργαζομένων και την μείωση της πιθανότητας εμφάνισης περιστατικών σύμφωνα με το [ΤΑ1] της Απόφασης Κ.Δ.Π 389/2020.
* Οι στόχοι για την εκπαίδευση των εργαζομένων σχετικά με την ασφάλεια πληροφοριών πρέπει να είναι καθορισμένοι και να διατηρούνται.
* Το πρόγραμμα εκπαίδευσης του [Όνομα Οργανισμού] σε θέματα Ασφάλειας Πληροφοριών και κυβερνοασφάλειας πρέπει να σχεδιάζεται λαμβάνοντας υπόψη τους ρόλους και τα καθήκοντα των εργαζομένων και να περιλαμβάνει τουλάχιστον μια ετήσια εκπαίδευση και ενημέρωση των εργαζομένων σχετικά με τις Πολιτικές Ασφάλειας του [Όνομα Οργανισμού]
* Το πρόγραμμα εκπαίδευσης του [Όνομα Οργανισμού] σε θέματα Ασφάλειας Πληροφοριών/κυβερνοασφάλειας πρέπει να σχεδιάζεται εξασφαλίζοντας ότι παρέχει επαρκή ενημέρωση σχετικά με τους ρόλους και τις αρμοδιότητες του προσωπικού όσον αφορά την Ασφάλεια Πληροφοριών.
* Το πρόγραμμα εκπαίδευσης του [Όνομα Οργανισμού] σε θέματα Ασφάλειας Πληροφοριών και κυβερνοασφάλειας θα πρέπει να έχει δημιουργηθεί σύμφωνα με τις πολιτικές και τις σχετικές διαδικασίες του οργανισμού, λαμβάνοντας υπόψη τις πληροφορίες του οργανισμού που θα πρέπει να προστατεύονται και τα μέτρα που έχουν εφαρμοστεί για την προστασία των πληροφοριών από πιθανή απώλεια δεδομένων ή/και παραβίαση προσβάσεων σύμφωνα με το [ΤΑ2] της Απόφασης Κ.Δ.Π 389/2020.
* Η Ανώτατη Διεύθυνση του [Όνομα Οργανισμού] έχει τη ευθύνη για έγκριση του ετήσιου προγράμματος εκπαίδευσης και ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών ώστε να προάγεται η δέσμευση και η κουλτούρα ασφάλειας για τις πληροφορίες του [Όνομα Οργανισμού].
* Η αποτελεσματικότητα του προγράμματος εκπαιδεύσεων, καθώς και το επίπεδο γνώσεων και ευαισθητοποίησης του Προσωπικού σε θέματα Ασφάλειας Πληροφοριών αξιολογούνται περιοδικά (τουλάχιστον ετησίως).
* Η διαδικασία εκπαίδευσης και ευαισθητοποίησης εργαζομένων/συνεργατών πρέπει να περιλαμβάνει περιοδικές δράσεις καθ’ όλη τη διάρκεια της σχέσης εργοδότησης/συνεργασίας, από την πρόσληψη/ανάθεση μέχρι τη λήξη της.
* Δραστηριότητες ευαισθητοποίησης, όπως εκστρατείες (π.χ. μια «ημέρα ασφάλειας πληροφοριών») και έκδοση φυλλαδίων ή ενημερωτικών δελτίων (π.χ ηλεκτρονικά μηνύματα), θα πρέπει να περιλαμβάνονται στο πρόγραμμα εκπαιδεύσεων.
* Το Τμήμα Ανθρώπινου Δυναμικού του [Όνομα Οργανισμού] θα πρέπει να διατηρεί τεκμήρια σχετικά με την ολοκλήρωση εκπαιδεύσεων και τα αποτελέσματα αυτών.
* Συστήνεται όπως δημιουργηθούν κανάλια επικοινωνίας με εσωτερικές ή εξωτερικές ομάδες και σχετικές με την ασφάλεια πληροφοριών, ώστε το προσωπικό να παραμένει ενημερωμένο με τις πιο πρόσφατες συνιστάμενες πρακτικές, τεχνικές και τεχνολογίες ασφάλειας.
* Για την εφαρμογή του προγράμματος εκπαίδευσης ο [Όνομα Οργανισμού] δύναται να ακολουθεί τις πιο κάτω πρακτικές ευαισθητοποίησης:
  + Παροχή εκπαιδευτικού υλικού μέσω προσαρμοσμένων πλατφόρμων.
  + Πραγματοποίηση εκπαιδεύσεων μέσω παρουσιάσεων, σεμιναρίων, και προσομοιωμένων ασκήσεων.
  + Πραγματοποίηση περιοδικών ελέγχων κατανόησης του περιεχομένου του προγράμματος.
  + Συνεχής ενημέρωση για νέες απειλές μέσω ενημέρωσης του ετήσιου τοπίου κυβερνοαπειλων και τεχνικές δράσεις μετριασμού των απειλών.

# Ετήσιο πρόγραμμα εκπαίδευσης

Οι ανάγκες των αρμόδιων ατόμων για εκπαίδευση και ενημέρωση σε θέματα ασφάλειας πληροφοριών αναγνωρίζονται:

* Κατά την εκπόνηση του ετήσιου προγράμματος εκπαίδευσης και ενημέρωσης σε θέματα ασφάλειας πληροφοριών
* Κατά την εκπόνηση του ετήσιου προϋπολογισμού του [Όνομα Οργανισμού]
* Κατά τη συμπλήρωση των ετήσιων αξιολογήσεων εκπαίδευσης και των ετήσιων αξιολογήσεων απόδοσης
* Ως αποτέλεσμα ενεργειών από διάφορες δραστηριότητες του [Όνομα Οργανισμού] π.χ. Ασκήσεις, Διαχείριση περιστατικών ασφάλειας, αξιολόγηση κινδύνων
* Ως αποτέλεσμα αλλαγής στις επιχειρησιακές ανάγκες του [Όνομα Οργανισμού].

# Αποτελεσματικότητα του προγράμματος

Η αποτελεσματικότητα του προγράμματος δύναται να αξιολογείται μέσω:

* Συμμετοχή και κατανόηση από το προσωπικό μέσω λειτουργιών που παρέχουν ειδικές πλατφόρμες εκπαίδευσης και αξιολόγησης.
* Ανάλυσης στατιστικών περιστατικών κυβερνοεπιθέσεων και οι τρόποι/χρόνοι αντιμετώπισης των περιστατικών αυτών.
* Συλλογή ανατροφοδοτήσεων από τους συμμετέχοντες.

Η διαρκής βελτίωση του προγράμματος εξασφαλίζει την καλύτερη προστασία του [Όνομα Οργανισμού] από τις νεότερες και πιο σύγχρονες κυβερνοαπειλές και τη συμμετοχή όλων των εργαζομένων στον ενιαίο στόχο της ανθεκτικότητας από κυβερνοεπιθέσεις.

# Πειθαρχική διαδικασία

Υπάρχει καταγραμμένη επίσημη πειθαρχική διαδικασία, σύμφωνα με τους ισχύοντες νόμους και κανονισμούς, για ανάληψη δράσης σε περίπτωση παραβίασης θεμάτων που σχετίζονται με την ασφάλεια πληροφοριών. Η διαδικασία αυτή θα πρέπει έχει επικοινωνηθεί στους υπαλλήλους, για την καλύτερη συμμόρφωση με τις υποχρεώσεις και τις ευθύνες τους.

Η διαδικασία αυτή ακολουθείται για τις περιπτώσεις σοβαρής τεκμηριωμένης παραβίασης ασφάλειας πληροφοριών, η οποία έχει υψηλό αντίκτυπο στον [Όνομα Οργανισμού] βάσει της αξιολόγησης κινδύνου. Στη διαδικασία καταγράφονται 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, αν ο παραβάτης είχε την κατάλληλη εκπαίδευση, καθώς και τη σχετική νομοθεσία, συμβατικές υποχρεώσεις και άλλους σχετικούς παράγοντες.

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

# Τερματισμός της εργοδότησης ή αλλαγή της εργασίας

Το Τμήμα Ανθρώπινου Δυναμικού του [Όνομα Οργανισμού] 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 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 θα ανακληθεί κατά την ημερομηνία διακανονισμού των οφειλών ή την ημερομηνία αναχώρησης από τον [Όνομα Οργανισμού] (όποιο είναι νωρίτερα).

4) Το Τμήμα Ανθρώπινου Δυναμικού, που έρχεται σε επαφή με άλλα τμήματα, θα 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 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 καθορίζει 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) Τυχόν εξοπλισμός που διατίθεται στον χρήστη θα πρέπει να επιστρέφεται με ασφάλεια για οποιαδήποτε περαιτέρω αναθεώρηση ή ενέργεια.

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

10) Σε περίπτωση απόλυσης υπαλλήλου, δεν θα πρέπει να επιτρέπεται σε αυτό να έχει πρόσβαση σε οποιαδήποτε πληροφορία ή εγκατάσταση επεξεργασίας πληροφοριών. 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 κατά τον τερματισμό

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

Το Τμήμα Ανθρώπινου Δυναμικού είναι υπεύθυνο, σε συνεργασία με τον οικείο Προϊστάμενο και το Τμήμα Πληροφορικής του [Όνομα Οργανισμού] , 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, προστασία προσωπικών δεδομένων 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 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 με ασφάλεια στον Οργανισμό.

# Αφαίρεση δικαιωμάτων πρόσβασης

Τα δικαιώματα πρόσβασης τόσο στις εγκαταστάσεις του [Όνομα Οργανισμού] όσο και σε πληροφορίες και συστήματα επεξεργασίας πληροφοριών, των υπαλλήλων και των εξωτερικών συνεργατών, χρειάζεται να αφαιρεθούν αμέσως μετά τη λήξη της εργοδότησης, 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 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 Ανθρώπινου Δυναμικού για τις προσβάσεις στα κτήρια
* Η Υποδοχή, ώστε από την ημερομηνία τερματισμού το συγκεκριμένο άτομο να τυγχάνει χειρισμού ως επισκέπτης, κ.ά.

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.

# Αναθεώρηση

Ιδιοκτήτης της υφιστάμενης πολιτικής είναι ο/η Προϊστάμενος/η του Τμήματος Ανθρώπινου Δυναμικού, ο/η οποίος/α είναι υπεύθυνος/η για την εφαρμογή, τήρηση και αναθεώρηση της πολιτικής αυτής. Όλες οι πολιτικές και διαδικασίες σχετικές με τη Διαχείριση Ανθρώπινου Δυναμικού θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] (π.χ. όσον αφορά την οργανωτική δομή, τις επιχειρηματικές δραστηριότητες και τις τάσεις της αγοράς, τις νομικές, κανονιστικές απαιτήσεις και τις απαιτήσεις συμμόρφωσης, την εφαρμογή νέων συστημάτων, τους νέους κινδύνους, τις αναδυόμενες απειλές κλπ.).

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Ασφάλεια Ανθρώπινων Πόρων | HRS1 | Κύκλος ζωής της εργοδότησης | Να υλοποιούνται επαρκή μέτρα για την εξασφάλιση ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, τα οποία έχουν πρόσβαση σε οργανωτικούς πόρους, υποστηρίζουν την πολιτική ασφάλειας πληροφοριών και τους στόχους του οργανισμού. |
| Ασφάλεια Ανθρώπινων Πόρων | HRS2 | Παρακολούθηση εργαζομένων | Να εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού συμμορφώνονται με την πολιτική ασφάλειας πληροφοριών και τηρούν τις ευθύνες ασφάλειας τους καθ’ όλη τη διάρκεια του κύκλου ζωής της απασχόλησης. |
| Ασφάλεια Ανθρώπινων Πόρων | HRS3 | Πειθαρχικά μέτρα και επιβολή | Να εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, είναι υπεύθυνα για τις εκούσιες ή ακούσιες δραστηριότητες που επηρεάζουν τους στόχους ασφάλειας πληροφοριών του οργανισμού. |
| Ασφάλεια Ανθρώπινων Πόρων | HRS4 | Εξωτερικοί συνεργάτες | Να εξασφαλιστεί ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας του οργανισμού. |
| Ασφάλεια Ανθρώπινων Πόρων | HRS5 | Προστασία από απειλές που προέρχονται από εσωτερικά πρόσωπα | Να εξασφαλιστεί η προστασία από απειλές κατά της ασφάλειας δικτύων και πληροφοριών από το εσωτερικό του οργανισμού. |
| Ασφάλεια Ανθρώπινων Πόρων | HRS6 | Συμφωνίες εργοδότησης και αποδεκτή χρήση | Να διασφαλιστεί ότι οι ευθύνες που αφορούν την ασφάλεια πληροφοριών και την αποδεκτή χρήση των στοιχείων ενεργητικού, ενσωματώνονται στις συμφωνίες εργοδότησης και στις διαδικασίες έναρξης απασχόλησης, για την επίτευξη υπευθυνότητας και ευαισθητοποίησης. |
| Ευαισθητοποίηση και Εκπαίδευση | TA1 | Ευαισθητοποίηση σχετικά με την ασφάλεια πληροφοριών | Να θεσπιστεί πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών για όλα τα στελέχη εντός του οργανισμού, λαμβάνοντας υπόψη τα στοιχεία που περιγράφονται στις πολιτικές, τα πρότυπα, τις κατευθυντήριες γραμμές και τις διαδικασίες ασφάλειας πληροφοριών. |
| Ευαισθητοποίηση και Εκπαίδευση | TA2 | Ευαισθητοποίηση και εκπαίδευση σε θέματα ασφάλειας πληροφοριών | Να παρέχει εκπαίδευση προς όλα τα στελέχη του οργανισμού, όπως ορίζεται στο πρόγραμμα ασφάλειας πληροφοριών. |
| Ασφάλεια Δεδομένων | DS5 | Πρόληψη απώλειας δεδομένων και διαρροής δεδομένων | Να εξασφαλιστεί η προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων. |