Όνομα Οργανισμού

Πολιτική Διαχείρισης Προμηθευτών

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Διαχείρισης Προμηθευτών |
| **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](#_Toc158630652)

[1.1. Σύνοψη πολιτικής 4](#_Toc158630653)

[1.2. Πεδίο εφαρμογής 4](#_Toc158630654)

[1.3. Αναθεώρηση και Αξιολόγηση 4](#_Toc158630655)

[1.4. Αναγνώριση των κινδύνων που σχετίζονται με τους εξωτερικούς συνεργάτες 5](#_Toc158630656)

[1.5. Αντιμετωπίζοντας τα θέματα ασφάλειας πληροφοριών των συνεργατών 5](#_Toc158630657)

[1.6. Ασφάλεια πληροφοριών στις συμβάσεις με τους εξωτερικούς συνεργάτες 6](#_Toc158630658)

[1.7. Διατήρηση Μητρώου/Λίστας εξωτερικών συνεργατών 7](#_Toc158630659)

[2. Διαχείριση παρεχόμενων υπηρεσιών εξωτερικού συνεργάτη 7](#_Toc158630660)

[2.1. Παρεχόμενες υπηρεσίες 7](#_Toc158630661)

[2.2. Διαδικασία αξιολόγησης εξωτερικού συνεργάτη/προμηθευτή 8](#_Toc158630662)

[2.3. Παρακολούθηση υπηρεσιών εξωτερικού συνεργάτη 8](#_Toc158630663)

[3. Απαιτήσεις Ασφάλειας Πληροφοριών 9](#_Toc158630664)

[3.1. Έλεγχος προσωπικού 9](#_Toc158630665)

[3.2. Πρόσβαση στις πληροφορίες και τα συστήματα του Οργανισμού 9](#_Toc158630666)

[3.3. Ηλεκτρονική πρόσβαση 10](#_Toc158630667)

[3.4. Περιορισμοί χρόνου πρόσβασης 10](#_Toc158630668)

[3.5. Έλεγχος πρόσβασης στο δίκτυο του Οργανισμού 10](#_Toc158630669)

[3.6. Διαχείριση ιών 11](#_Toc158630670)

[3.7. Διαχείριση περιστατικών ασφάλειας πληροφοριών 11](#_Toc158630671)

[3.8. Κατηγοριοποίηση πληροφοριών 11](#_Toc158630672)

[3.9. Διαχείριση μέσων με πληροφορίες του Οργανισμού 12](#_Toc158630673)

[3.10. Απόρριψη μέσων με πληροφορίες του Οργανισμού 12](#_Toc158630674)

[3.11. Απομάκρυνση εξοπλισμού από τον Οργανισμό 12](#_Toc158630675)

[3.12. Πολιτική ‘άδειου γραφείου’ και ‘καθαρής οθόνης 12](#_Toc158630676)

[3.13. Χρήση ηλεκτρονικού ταχυδρομείου και διαδικτύου 13](#_Toc158630677)

[3.14. Έλεγχος αλλαγών σε λογισμικά και υλισμικά 13](#_Toc158630678)

[Παράρτημα Α – Λίστα εξωτερικών συνεργατών 14](#_Toc158630679)

# Εισαγωγή

# Σύνοψη πολιτικής

Αναγνωρίζοντας τον κίνδυνο που υπάρχει κατά τη διαχείριση πληροφοριών και συστημάτων πληροφορικής του Οργανισμού από εξωτερικούς του συνεργάτες, ο [Όνομα Οργανισμού] εφαρμόζει την εν λόγω πολιτική με στόχο τον έλεγχο του κινδύνου αυτού και τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών του.

Η αξιολόγηση κινδύνου λαμβάνει υπόψη μεταξύ άλλων, νομικές απαιτήσεις, συμβατικές υποχρεώσεις, απαιτήσεις της πολιτικής ασφάλειας, ανάγκες δικτύου / υποδομής.

Η πολιτική καλύπτει τουλάχιστον τα ακόλουθα σημεία της σχέσης του [Όνομα Οργανισμού] και των εξωτερικών συνεργατών του:

* αξιολόγηση κινδύνου
* τις πρόνοιες της σύμβασης
* φυσική και ηλεκτρονική πρόσβαση στις πληροφορίες κατά τη αποθήκευση(data at rest), μεταφορά(data in transit) η χρήση τους(data in use)και στα συστήματα πληροφορικής που φιλοξενούν τις πληροφορίες αυτές

# Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για τους υπαλλήλους των εξωτερικών συνεργατών και των υπεργολάβων τους, που έχουν πρόσβαση στις πληροφορίες και στα συστήματα πληροφορικής του [Όνομα Οργανισμού]. Οι κατευθυντήριες γραμμές που καταγράφονται στην πολιτική αφορούν στις δραστηριότητες, πληροφορίες, δεδομένα, λογισμικά, υλισμικά κ.α. τα οποία ανήκουν στον [Όνομα Οργανισμού] ή τα διαχειρίζεται

# Αναθεώρηση και Αξιολόγηση

Ιδιοκτήτης της υφιστάμενης Πολιτικής είναι ο Υπεύθυνος Ασφάλειας Πληροφοριών, ο οποίος είναι υπεύθυνος για την εφαρμογή και την τήρηση της στον [Όνομα Οργανισμού] καθώς και την αναθεώρηση της, σύμφωνα με τις ακόλουθες κατευθυντήριες γραμμές:

* Σε περιπτώσεις σημαντικών αλλαγών στον Οργανισμό
* Σε περιπτώσεις περιστατικών ασφάλειας πληροφοριών ή κανονιστικών αλλαγών
* Ετήσια αναθεώρηση, εφόσον προκύπτει η ανάγκη για:
	+ Βελτίωση της αποτελεσματικότητας της πολιτικής
	+ Ενημέρωση της για αλλαγές στην τεχνολογία.

Εξωτερικοί συνεργάτες

Ο Κανονισμός Κ.Δ.Π. 389/2020 προτείνει:

- Ο [Όνομα Οργανισμού] να επιδεικνύει τη δέουσα επιμέλεια κατά τον εντοπισμό και τη σύναψη συμβατικών σχέσεων με τρίτα μέρη και προμηθευτές, λαμβανομένων υπόψη των κινδύνων τρίτων μερών, μεταξύ άλλων, της εξάρτησης από τον εκάστοτε προμηθευτή, της διαχείρισης περιστατικών και της ευθύνης σε σχέση με την ασφάλεια δικτύων και πληροφοριών.

- Ο [Όνομα Οργανισμού] να διατηρεί κεντρικό αποθετήριο προμηθευτών, πωλητών και άλλων τρίτων μερών για να διασφαλίσει ότι όλες οι σχέσεις με τρίτα μέρη υποστηρίζονται από κατάλληλες συμβατικές ρήτρες, ρόλους, ευθύνες, σε περίπτωση συμβάντων, όσον αφορά την ασφάλεια δικτύων και πληροφοριών.

# Αναγνώριση των κινδύνων που σχετίζονται με τους εξωτερικούς συνεργάτες

Πριν την έναρξη εργασιών, ο Υπεύθυνος Ασφάλειας Πληροφοριών προβαίνει σε αξιολόγηση κινδύνου εξωτερικού συνεργάτη για τον οποίο κρίνει ότι αυτό είναι απαραίτητο, λαμβάνοντας υπόψη την

* κατηγοριοποίηση των πληροφοριών που θα λαμβάνει
* την φυσική ή/και ηλεκτρονική πρόσβαση του στα κτήρια / συστήματα του [Όνομα Οργανισμού]
* τον τρόπο σύνδεσης δικτύων μεταξύ του [Όνομα Οργανισμού] και εξωτερικού συνεργάτη
* τις υφιστάμενες μεθόδους και μέτρα ασφάλειας που εφαρμόζει
* εάν η υφιστάμενη υποδομή του συνεργάτη είναι φυσική ή σε υπολογιστικό νέφος
* εάν ο συνεργάτης βρίσκεται σε χώρα όπου θεωρείται κρίσιμη για τον [Όνομα Οργανισμού] για την διασφάλιση των δεδομένων που θα λαμβάνει ο συνεργάτης

Με αυτό τον τρόπο, αναγνωρίζονται πιθανά αναγκαία επιπρόσθετα μέτρα ασφάλειας που χρειάζεται να αναληφθούν από τον εξωτερικό συνεργάτη.

# Αντιμετωπίζοντας τα θέματα ασφάλειας πληροφοριών των συνεργατών

Πριν να δοθεί πληροφόρηση ή οποιαδήποτε πρόσβαση σε εξωτερικό συνεργάτη, οι ακόλουθοι παράμετροι χρειάζεται να λαμβάνονται υπόψη στους όρους της συνεργασίας, για σκοπούς ασφάλειας:

* Περιγραφή του προϊόντος / υπηρεσίας που θα παρασχεθεί (βλέπε Πολιτική Ασφάλειας Συστημάτων) την ανάγκη της πρόσβασης και τα χαρακτηριστικά της, για παράδειγμα: τη μέθοδο πρόσβασης και τη χρήση μοναδικών στοιχείων (όνομα χρήστη και κωδικό), τη διαδικασία έγκρισης, τις περιπτώσεις ανάκλησης της έγκρισης και το γεγονός ότι απαγορεύεται οτιδήποτε δεν επιτρέπεται ρητώς
* Προστασία στοιχείων (περιουσιακών ή πληροφορίες), για παράδειγμα: διαδικασίες για προστασία πληροφοριών, διαχείριση γνωστών ευπαθειών, ακεραιότητα του στοιχείου, περιορισμοί στην αντιγραφή ή αποκάλυψη πληροφοριών
* Διευθετήσεις αναφοράς περιστατικών ασφάλειας πληροφοριών και διερεύνησης ανακριβειών σε πληροφορίες
* Το αποδεκτό επίπεδο ποιότητας παρεχόμενων υπηρεσιών
* Το δικαίωμα παρακολούθησης και ελέγχου των εργασιών καθώς και της ανάκλησης εργασιών που δεν συμμορφώνονται με τις εκάστοτε πολιτικές ασφάλειας
* Νομοθετικές υποχρεώσεις π.χ. GDPR, πνευματική ιδιοκτησία.

# Ασφάλεια πληροφοριών στις συμβάσεις με τους εξωτερικούς συνεργάτες

Στη σύμβαση μεταξύ του [Όνομα Οργανισμού] και εξωτερικού συνεργάτη καταγράφονται οι απαιτήσεις ασφάλειας πληροφοριών ώστε να διασφαλιστεί το ελάχιστο απαιτούμενο επίπεδο συμμόρφωσης. Σε αυτή, δύναται να περιλαμβάνονται τα ακόλουθα:

1. Η Πολιτική Ασφάλειας Πληροφοριών του [Όνομα Οργανισμού]
2. Συμφωνία Εμπιστευτικότητας
3. Η Συμφωνία επεξεργασίας προσωπικών δεδομένων (GDPR)
4. Μέτρα ασφάλειας για την προστασία περιουσιακών στοιχείων, για παράδειγμα: διαδικασίες σε σχέση με υλισμικά και λογισμικά, μέτρα για προστασία από κακόβουλα λογισμικά, περιορισμοί στην αντιγραφή ή αποκάλυψη πληροφοριών
5. Μέτρα για τον έλεγχο πρόσβασης, για παράδειγμα: επιτρεπόμενοι μέθοδοι πρόσβασης, ο έλεγχος και η χρήση του ονόματος του χρήστη και του κωδικού, η διαδικασία έγκρισης, η κατάρτιση καταλόγου με τα άτομα που θα έχουν πρόσβαση, το είδος τέτοιας πρόσβασης και τα συστήματα στα οποία θα τους δοθεί, η διαδικασία ανάκλησης
6. Μέτρα για να διασφαλιστεί η επιστροφή ή η καταστροφή των πληροφοριών / του εξοπλισμού στο τέλος ή σε προσυμφωνημένη χρονική περίοδο απο τη λήξη της σύμβασης, ανάλογα με το είδος της πληροφορίας / του εξοπλισμού
7. Διαδικασίες διαχείρισης αλλαγών σε λογισμικά ή υλισμικά
8. Διευθετήσεις για την αναφορά περιστατικών ασφάλειας πληροφοριών στον Προϊστάμενο Ασφάλειας Πληροφοριών, στην περίπτωση που επηρεάζονται πληροφορίες του [Όνομα Οργανισμού]
9. Δικαίωμα ελέγχου – o [Όνομα Οργανισμού] διατηρεί το δικαίωμα να διεξάγει έλεγχο ή να ορίσει τρίτους ελεγκτές για την αξιολόγηση των εργασιών ως προς τη συμμόρφωση των προμηθευτών με τις πολιτικές και τις διαδικασίες ασφάλειας πληροφοριών. Διατηρεί επίσης το δικαίωμα ανάκλησης εργασιών που δεν συμμορφώνονται με τις εκάστοτε πολιτικές ασφάλειας.
10. Νομοθετικές υποχρεώσεις π.χ. πνευματική ιδιοκτησία, Κανονισμοί της Ευρωπαϊκής Επιτροπής
11. Διαδικασίες κλιμάκωσης για επίλυση διαφορών ή διαιτησία
12. Τις υποχρεώσεις και των δύο μερών της σύμβασης
13. Μέτρα για επιχειρησιακή συνέχεια και για ανάκαμψη εργασιών από καταστροφή
14. Απόσυρση των δεδομένων που χρησιμοποιήθηκαν σε ελέγχους (test data).

Οι παράμετροι οι οποίοι δεν θα περιλαμβάνονται στη σύμβαση, ανάλογα με την περίπτωση, θα συμφωνούνται με τον συντονιστή της σύμβασης. Ο συντονιστής της σύμβασης, όπου κρίνει απαραίτητο, σε συνεργασία με τον Προϊστάμενο Ασφάλειας Πληροφοριών, θα καθορίζει τα πιο πάνω, λαμβάνοντας υπόψη και την κρισιμότητα ή / και την ευαισθησία των πληροφοριών που θα διαχειριστεί ο εξωτερικός συνεργάτης.

# Διατήρηση Μητρώου/Λίστας εξωτερικών συνεργατών

Ο [Όνομα Οργανισμού] θα πρέπει να δημιουργήσει μια λίστα με εξωτερικούς συνεργάτες στην οποία λίστα να αναγράφονται τα πιο κάτω:

* Όνομα Οργανισμού
* Όνομα ατόμου επικοινωνίας
* Στοιχεία επικοινωνίας του ατόμου
* Υπηρεσίες που παρέχονται από τον εξωτερικό συνεργάτη
* Πιθανές προσβάσεις στα συστήματα του [Όνομα Οργανισμού]
* Είδος πληροφορίας που επεξεργάζονται, αποθηκεύουν ή διαβιβάζουν
* Διάρκεια πρόσβασης στα συστήματα
* Χρόνος σύμβασης
* Υπεύθυνο άτομο σύμβασης

Αντίγραφο Σύμβασης για εύκολη χρήση

Ανατρέξτε στο παράρτημα Α για περισσότερες πληροφορίες σχετικά με την λίστα εξωτερικών συνεργατών.

# Διαχείριση παρεχόμενων υπηρεσιών εξωτερικού συνεργάτη

# Παρεχόμενες υπηρεσίες

Ο συντονιστής της εκάστοτε σύμβασης διασφαλίζει ότι οι υπηρεσίες που παρέχει ο εξωτερικός συνεργάτης ταυτίζονται με τις συμβατικές του υποχρεώσεις και λαμβάνει εύλογα μέτρα για να διασφαλίσει ότι ο εξωτερικός συνεργάτης συμμορφώνεται με τις σχετικές απαιτήσεις ασφάλειας πληροφοριών.

# Διαδικασία αξιολόγησης εξωτερικού συνεργάτη/προμηθευτή

Ο [Όνομα Οργανισμού] θα πρέπει να θεσπίσει διαδικασία για αξιολόγηση ενός συνεργάτη/προμηθευτή με ενσωμάτωση ολοκληρωμένων απαιτήσεων ασφάλειας πληροφοριών σε μορφή απαιτήσεων/κριτηρίων συμμόρφωσης. Τα κριτήρια αυτά τα οποία δύναται να κάνουν αναφορά σε σχετικά πρότυπα ασφαλείας, όπως το ISO 27001, για τον καθορισμό βασικών προσδοκιών, θα πρέπει να ενσωματώνονται στα έγγραφα διαγωνισμών που εκδίδει ο [Όνομα Οργανισμού] για εξασφάλιση προμηθειών, υπηρεσιών και έργων.

Με τον σαφή καθορισμό αυτών των προσδοκιών, ο [Όνομα Οργανισμού] δύναται να ελαχιστοποιήσει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης, παραβιάσεων και απώλειας δεδομένων του μέσω συνεργατών/προμηθευτών.

Η διαδικασία αυτή δύναται να χρησιμοποιείτε από τον [Όνομα Οργανισμού] για επαναξιολόγηση του συνεργάτη/προμηθευτή όποτε κρίνεται απαραίτητο

# Παρακολούθηση υπηρεσιών εξωτερικού συνεργάτη

Ο συντονιστής της εκάστοτε σύμβασης παρακολουθεί τη συμμόρφωση του εξωτερικού συνεργάτη με το απαιτούμενο επίπεδο υπηρεσιών που σύμφωνα με τη σύμβαση χρειάζεται να λαμβάνει ο [Όνομα Οργανισμού]. Σημαντική παράμετρος είναι η αναφορά ενδεχόμενου περιστατικού ασφάλειας πληροφοριών ώστε να είναι σε θέση ο [Όνομα Οργανισμού] να το χειριστεί εγκαίρως. Ο συντονιστής χρειάζεται να προβαίνει στα ακόλουθα κατά τη διάρκεια της σύμβασης:

* Παρακολούθηση της αποδοτικότητας των υπηρεσιών
* Θεώρηση των δελτίων / καταστάσεων του εξωτερικού συνεργάτη σε σχέση με τις παρεχόμενες υπηρεσίες
* Τακτικές συναντήσεις για συζήτηση των συμφωνηθέντων, της απόδοσης και της εφαρμογής της σύμβασης, των πολιτικών και των διαδικασιών. Νοείται ότι ο [Όνομα Οργανισμού] μπορεί να προβεί σε έλεγχο για να διασφαλίσει ότι τηρούνται η σύμβαση, οι πολιτικές και οι διαδικασίες
* Αναγνώριση θεμάτων προς επίλυση καθώς και ενδεχόμενων διαφωνιών.

Ο συντονιστής της σύμβασης προβαίνει σε πρόχειρη αξιολόγηση των κινδύνων που αναγνωρίζει και όπου κρίνει απαραίτητο, αποτείνεται στο Προϊστάμενο Ασφάλειας Πληροφοριών για πραγματοποίηση της σχετικής αξιολόγησης και ενδεχομένως της εφαρμογής επιπρόσθετων μέτρων ασφάλειας.

Για αλλαγές στα συστήματα πληροφορικής του [Όνομα Οργανισμού], ο εξωτερικός συνεργάτης χρειάζεται να υιοθετήσει τη σχετική Διαδικασία Διαχείρισης Αλλαγών Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης).

# Απαιτήσεις Ασφάλειας Πληροφοριών

Όλοι οι εξωτερικοί συνεργάτες του [Όνομα Οργανισμού] χρειάζεται να ικανοποιούν τις απαιτήσεις ασφάλειας πληροφοριών του [Όνομα Οργανισμού]. Αυτές είναι οι βασικές αρχές ασφάλειας στον [Όνομα Οργανισμού] και αποτελούν το ελάχιστο επίπεδο ασφάλειας που απαιτεί ο Οργανισμός από τον εκάστοτε εξωτερικό συνεργάτη.

Οι εξωτερικοί συνεργάτες χρειάζεται να λαμβάνουν τα απαραίτητα και τα εύλογα μέτρα για να διασφαλίσουν ότι δεν παραβιάζεται οποιαδήποτε παράμετρος ασφάλειας κατά τη διάρκεια της σύμβασης τους. Ο [Όνομα Οργανισμού] διατηρεί το δικαίωμα να ζητήσει από τον εξωτερικό συνεργάτη να παρέχει τα τεκμήρια για να αποδείξει ότι προέβηκε στις απαιτούμενες ενέργειες, καθώς και να πραγματοποιήσει έλεγχο ασφάλειας πληροφοριών ώστε να επιβεβαιώσει την επάρκεια των ενεργειών του συνεργάτη.

# Έλεγχος προσωπικού

Ο εξωτερικός συνεργάτης είναι υπεύθυνος για την επιβεβαίωση της ταυτότητας και της επαγγελματικής επάρκειας του προσωπικού του που θα εμπλακεί σε οποιαδήποτε εργασία του [Όνομα Οργανισμού] και ως εκ τούτου θα έχει πρόσβαση σε κτήριο, συστήματα ή πληροφορίες του. Ο εξωτερικός συνεργάτης είναι επίσης υπεύθυνος, το προσωπικό του που θα έχει πρόσβαση στις πληροφορίες του [Όνομα Οργανισμού] να υπογράψει σχετική συμφωνία εμπιστευτικότητας ή οτιδήποτε άλλο αντίστοιχο το οποίο να διασφαλίζει την εμπιστευτικότητα των πληροφοριών του Οργανισμού.

Για περισσότερες λεπτομέρειες μπορείτε να ανατρέξετε στην ‘Πολιτική Διαχείρισης Ανθρώπινου Δυναμικού’ του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

# Πρόσβαση στις πληροφορίες και τα συστήματα του Οργανισμού

Οποιαδήποτε απώλεια στην εμπιστευτικότητα, στην ακεραιότητα ή στη διαθεσιμότητα του δικτύου ή των συστημάτων του [Όνομα Οργανισμού] θα μπορούσε να μειώσει την ικανότητα τους για υποστήριξη των διαδικασιών του Οργανισμού.

Πρόσβαση του εξωτερικού συνεργάτη σε σύστημα πληροφορικής ή κτήριο του [Όνομα Οργανισμού] θα δίνεται κατόπιν εφαρμογής της σχετικής Διαδικασίας Διαχείρισης Πρόσβασης Χρηστών και των οδηγιών για διαχειριστές των συστημάτων ασφαλείας των κτηρίων του [Όνομα Οργανισμού] (βλέπε Πολιτική Ελέγχου Πρόσβασης).

Η φυσική πρόσβαση των εξωτερικών συνεργατών στα κτήρια του [Όνομα Οργανισμού] θα παρακολουθείται ανά τακτά χρονικά διαστήματα από το συντονιστή της σύμβασης, σε σχέση με τη συμμόρφωση του προσωπικού του συνεργάτη με τις διαδικασίες ασφάλειας και λαμβάνοντας υπόψη ενδεχόμενους υψηλούς κινδύνους, περιστατικά κ.α.

# Ηλεκτρονική πρόσβαση

Είναι απαραίτητο ο εξωτερικός συνεργάτης να εφαρμόζει τα ακόλουθα για να του δοθεί ηλεκτρονική πρόσβαση στα συστήματα του [Όνομα Οργανισμού]:

1. Να έχει αποδεχθεί τη συμμόρφωση του με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών του [Όνομα Οργανισμού] και να έχει υπογράψει συμφωνία εμπιστευτικότητας
2. Να ζητήσει πρόσβαση για διεκπεραίωση των καθηκόντων του στη βάση της αρχής της αναγκης γνώσης. Πρόσβαση θα δοθεί μόνο όταν ικανοποιηθεί ο ιδιοκτήτης του εκάστοτε συστήματος για τη σχετική ανάγκη
3. Η πρόσβαση θα περιορίζεται στα συμφωνημένα, μέθοδο, δικαιώματα και επίπεδο λειτουργικότητας
4. Η πρόσβαση θα γίνεται μέσω μοναδικού ονόματος χρήστη και μοναδικού κωδικού, τον οποίο θα χρησιμοποιεί το ενδεδειγμένο άτομο για να ταυτοποιείται στα συστήματα του [Όνομα Οργανισμού]
5. Ο συνεργάτης είναι υπεύθυνος για την τήρηση της εμπιστευτικότητας των κωδικών του. Σε καμία περίπτωση δεν επιτρέπεται οι χρήστες να κοινοποιούν τα στοιχεία ταυτοποίησης τους στα συστήματα του [Όνομα Οργανισμού]
6. Ο συνεργάτης να ενημερώνει το συντονιστή της σύμβασης όταν η πρόσβαση στα συστήματα του [Όνομα Οργανισμού] δεν είναι πλέον αναγκαία.

Το Τμήμα Πληροφορικής είναι υπεύθυνο να θεωρεί τις προσβάσεις των εξωτερικών συνεργατών σε τακτικά χρονικά διαστήματα (όχι πέραν των τεσσάρων μηνών) και να επιβεβαιώνει ή να αφαιρεί την πρόσβαση των χρηστών του εξωτερικού συνεργάτη.

# Περιορισμοί χρόνου πρόσβασης

Η πρόσβαση των χρηστών του εξωτερικού συνεργάτη στα συστήματα του [Όνομα Οργανισμού] χρειάζεται να είναι απενεργοποιημένη και να ενεργοποιείται από τα αρμόδια άτομα του Τμήματος Πληροφορικής όταν αυτοί επιβεβαιώσουν την ταυτότητα των χρηστών. Οποιαδήποτε ύποπτη ενέργεια χρειάζεται ανάλογα να αναφέρεται στο συντονιστή της σύμβασης ή στον Προϊστάμενο Ασφάλειας Πληροφοριών.

# Έλεγχος πρόσβασης στο δίκτυο του Οργανισμού

Όλες οι εξ’ αποστάσεως συνδέσεις στα συστήματα πληροφορικής του [Όνομα Οργανισμού] χρειάζεται να έχουν την εκ των προτέρων έγκριση του Προϊσταμένου του Τμήματος Πληροφορικής. Ανάλογα με την επικινδυνότητα και την κρισιμότητα της υπό αναφορά σύνδεσης, το Τμήμα Πληροφορικής βεβαιώνεται για τις ελάχιστες απαιτήσεις ασφάλειας και ο εξωτερικός συνεργάτης είναι υπεύθυνος να διασφαλίσει την επάρκεια της ασφάλειας του συστήματος το οποίο θα συνδεθεί στο δίκτυο της. Οι προσβάσεις σε εξωτερικά δίκτυα γίνονται με ασφάλεια μέσω ‘Firewall’ ή άλλης ενδεδειγμένης μεθόδου ασφάλειας δικτύου η οποία θα εγκριθεί από τον Προϊστάμενο του Τμήματος Πληροφορικής.

# Διαχείριση ιών

Το κατάλληλο λογισμικό κατά των ιών είναι απαραίτητο να εγκατασταθεί σε όλους τους υπολογιστές και τους εξυπηρετητές με πρόσβαση στο δίκτυο του [Όνομα Οργανισμού], να είναι ενεργό και ενημερωμένο. Η απαίτηση αυτή είναι αναγκαία και για τον εξοπλισμό των εξωτερικών συνεργατών παρά το γεγονός ότι απαγορεύεται η σύνδεση άλλου εξοπλισμού στο δίκτυο του Οργανισμού, πέραν αυτό που του ανήκει

Ως εκ τούτου, οι χρήστες φορητών υπολογιστών και οι χρήστες των εξωτερικών συνεργατών οι οποίοι χρησιμοποιούν υπολογιστές για να εργαστούν εκτός του εργασιακού περιβάλλοντος του [Όνομα Οργανισμού], πρέπει να διαθέτουν ενεργό και ενημερωμένο λογισμικό κατά των ιών.

Απαγορεύεται η προσπάθεια απενεργοποίησης ή απόδειξης ευπαθειών στα διοικητικά ή τεχνικά μέτρα ασφάλειας που εφαρμόζει ο [Όνομα Οργανισμού].

Περιστατικό ασφάλειας πληροφοριών που προήλθε από ιό ή κακόβουλο λογισμικό, χρειάζεται να κοινοποιηθεί αμέσως στον Προϊστάμενο του Τμήματος Πληροφορικής και ακολούθως στον Προϊστάμενο Ασφάλειας Πληροφοριών.

Οποιοσδήποτε εξοπλισμός μολύνθηκε με ιό ή με κακόβουλο λογισμικό χρειάζεται αμέσως να αποσυνδεθεί από το δίκτυο του [Όνομα Οργανισμού] και να μην συνδεθεί ξανά εκτός εάν δοθεί η απαραίτητη έγκριση.

# Διαχείριση περιστατικών ασφάλειας πληροφοριών

Οι εξωτερικοί συνεργάτες υποχρεούνται όπως αναφέρουν αμέσως οποιοδήποτε πιθανό ή πραγματικό περιστατικό ασφάλειας που σχετίζεται με πληροφορικά συστήματα ή πληροφορίες του [Όνομα Οργανισμού], στο συντονιστή της σύμβασης ή στη Λειτουργό Ασφάλειας Πληροφοριών. Παραβίαση της ασφάλειας είναι η μη εξουσιοδοτημένη πρόσβαση σε κτήριο, πληροφορικά συστήματα συνδεδεμένα με τον [Όνομα Οργανισμού] ή σε πληροφορίες του. Άλλα παραδείγματα είναι η απώλεια ή η κλοπή υπολογιστή, η μόλυνση από ιό ή κακόβουλο λογισμικό κ.α.

Ο [Όνομα Οργανισμού] θα διερευνήσει όλα τα πιθανά ή πραγματικά περιστατικά ασφάλειας και θα συγκεντρώσει τα απαραίτητα στοιχεία ώστε αναλύοντας την τάση, όπου απαιτείται, να εφαρμόσει τα κατάλληλα μέτρα ασφάλειας.

# Κατηγοριοποίηση πληροφοριών

Απαιτείται όπως οι εξωτερικοί συνεργάτες χειρίζονται τις πληροφορίες του Οργανισμού σύμφωνα με τα απαιτούμενα μέτρα ασφάλειας της κάθε κατηγορίας. Οι κατηγορίες πληροφοριών του Οργανισμού είναι οι ακόλουθες:

* **Κατηγορία 1**
* **Κατηγορία 2**
* **Κατηγορία 3**

Γενικά, απαγορεύεται η κοινοποίηση ή η συζήτηση πληροφοριών του Οργανισμού με άτομα που δεν είναι υπάλληλοι του ή ενδεδειγμένοι υπάλληλοι του εξωτερικού συνεργάτη. Εφαρμόζεται η αρχή της ανάγκης γνώσης σε όλες τις περιπτώσεις. Όλες οι πληροφορίες οι οποίες παράχθηκαν από ή για τον Οργανισμό είναι ιδιοκτησία του [Όνομα Οργανισμού] και σε καμία περίπτωση δεν μπορούν να πωληθούν, να αντιγραφούν ή να χρησιμοποιηθούν με άλλο τρόπο εκτός από τον εγκριμένο στη βάση της σύμβασης.

# Διαχείριση μέσων με πληροφορίες του Οργανισμού

Με στόχο την προστασία από απώλεια, μη εξουσιοδοτημένη πρόσβαση και την προστασία της ακεραιότητας της πληροφορίας, ο εξωτερικός συνεργάτης χρειάζεται να συντάσσει τα απαραίτητα έγγραφα με έλεγχο της έκδοσης τους και εφαρμόζοντας την πολιτική ‘άδειου γραφείου’ και ‘καθαρής οθόνης’. Όπου κρίνεται απαραίτητο, στα έγγραφα θα καταγράφεται η κατηγοριοποίηση τους π.χ. ‘εσωτερικής χρήσης -ειδικό’.

Για τη διαχείριση πληροφοριών κατηγοριοποίησης εσωτερικής χρήσης ειδικό και άνω, χρειάζεται να εφαρμόζονται κατά περίπτωση οι αντίστοιχες διαδικασίες φύλαξης και μεταφοράς τους. Σχετικά μπορείτε να ανατρέξετε στην πολιτική κρυπτογράφησης, στη διαδικασία χρήσης κινητών μέσων φύλαξης πληροφοριών και στην πολιτική κατηγοριοποίησης και διαχείρισης πληροφοριών.

# Απόρριψη μέσων με πληροφορίες του Οργανισμού

Τα μέσα που περιέχουν πληροφορίες του Οργανισμού θα πρέπει να απορρίπτονται με ασφάλεια, με φυσική καταστροφή του χαρτιού ή του πολυμέσου μεσω χαρτοκοπτικού μηχανήματος ή με ασφαλή διαγραφή των αποθηκευμένων πληροφοριών.

# Απομάκρυνση εξοπλισμού από τον Οργανισμό

Δεν επιτρέπεται από τον εξωτερικό συνεργάτη η οποιαδήποτε μετακίνηση εξοπλισμού από τα γραφεία του [Όνομα Οργανισμού], χωρίς την εκ των προτέρων σχετική έγκριση από τον αρμόδιο Προϊστάμενο.

# Πολιτική ‘άδειου γραφείου’ και ‘καθαρής οθόνης

Οι εξωτερικοί συνεργάτες είναι απαραίτητο να υιοθετήσουν πολιτική ‘άδειου γραφείου’ (clear desk) ενόσω διαχειρίζονται πληροφορίες του [Όνομα Οργανισμού]. Ως εκ τούτου, εάν ο χώρος εργασίας παραμείνει ανεπιτήρητος χρειάζεται όπως τα έγγραφα με διαβαθμισμένες ή ευαίσθητες πληροφορίες ή προσωπικά δεδομένα ή τα πολυμέσα φύλαξης πληροφοριών να φυλαχθούν ώστε να έχει πρόσβαση μόνο εξουσιοδοτημένος χρήστης. Παρόμοια, η οθόνη του ηλεκτρονικού υπολογιστή δεν πρέπει να βρίσκεται σε θέση που να μπορεί οποιοσδήποτε μη εξουσιοδοτημένος να λάβει γνώση για ευαίσθητη για τον Οργανισμό πληροφόρηση. Σε περίπτωση απουσίας από τον χώρο εργασίας, ο χρήστης χρειάζεται να αποσυνδεθεί από τον υπολογιστή.

# Χρήση ηλεκτρονικού ταχυδρομείου και διαδικτύου

Τα εισερχόμενα ή τα εξερχόμενα μηνύματα μέσω του ηλεκτρονικού ταχυδρομείου του Οργανισμού είναι ιδιοκτησία του [Όνομα Οργανισμού].

Υλικό το οποίο θεωρείται προσβλητικό (φυλετικό, σεξουαλικό, θρησκευτικό), δυσφημιστικό, άσεμνο, πορνογραφικό, απειλητικό, καταχρηστικό ή με οποιοδήποτε άλλο τρόπο ακατάλληλο δεν πρέπει να προβάλλεται, να ανεβάζεται, να αντιγράφεται, να αποθηκεύεται, να εκτυπώνεται ή να μεταδίδεται με τη χρήση των συστημάτων πληροφορικής του Οργανισμού.

Τα συστήματα του Οργανισμού πρέπει να χρησιμοποιούνται κυρίως για επιχειρηματικούς σκοπούς. Οποιαδήποτε προσωπική χρήση δεν πρέπει να παρεμποδίζει τις συνήθεις επιχειρηματικές δραστηριότητες του [Όνομα Οργανισμού], δεν θα πρέπει να συνεπάγεται προσωπικό κέρδος ή να θέσει τον [Όνομα Οργανισμού] σε προβληματικές καταστάσεις π.χ. νομικές.

Για περαιτέρω πληροφόρηση μπορείτε να ανατρέξετε στην ‘Πολιτική Αποδεκτής Χρήσης’ του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

# Έλεγχος αλλαγών σε λογισμικά και υλισμικά

Ο Προϊστάμενος του Τμήματος Πληροφορικής εγκρίνει τις τροποποιήσεις, τις αναβαθμίσεις και τις νέες εγκαταστάσεις υλισμικού και λογισμικού από τους εξωτερικούς συνεργάτες. Οι αλλαγές σε ρυθμίσεις εξυπηρετητών χρειάζεται να καταγράφονται και ως μέρος του σχεδίου ανάκαμψης από καταστροφή.

Λογισμικά και υλισμικά επιτρέπεται να εγκατασταθούν στην υποδομή / δίκτυο του Οργανισμού μόνο από τους αρμόδιους υπάλληλους του Τμήματος Πληροφορικής ή σε περίπτωση εξωτερικού συνεργάτη, κατόπιν επίβλεψης από αυτούς.

# Παράρτημα Α – Λίστα εξωτερικών συνεργατών

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Όνομα Οργανισμού | Άτομο επικοινωνίας | Στοιχεία επικοινωνίας | Υπηρεσίες | Προσβάσεις σε συστήματα | Είδος Διαχειριζόμενης Πληροφορίας | Διάρκεια προσβάσεων | Σύμβαση | Υπεύθυνος σύμβασης | Τοποθεσία Σύμβασης(link) |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |