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](#_Toc184812452)

[1.1. Σκοπός 4](#_Toc184812453)

[1.2. Πεδίο εφαρμογής 4](#_Toc184812454)

[2. Αντιμετωπίζοντας τα θέματα ασφάλειας πληροφοριών των συνεργατών 4](#_Toc184812455)

[3. Σχέσεις με τρίτα μέρη και προμηθευτές – Συμβάσεις 5](#_Toc184812456)

[3.1. Διατήρηση Μητρώου/Λίστας εξωτερικών συνεργατών 5](#_Toc184812457)

[3.2. Συμβάσεις με τους εξωτερικούς συνεργάτες 5](#_Toc184812458)

[3.3. Άλλες συμβατικές Υποχρεώσεις 6](#_Toc184812459)

[4. Διαχείριση παρεχόμενων υπηρεσιών εξωτερικού συνεργάτη 7](#_Toc184812460)

[4.1. Παρεχόμενες υπηρεσίες 7](#_Toc184812461)

[4.2. Διαδικασία αξιολόγησης εξωτερικού συνεργάτη/προμηθευτή 7](#_Toc184812462)

[5. Έλεγχος προσωπικού 8](#_Toc184812463)

[6. Πρόσβαση στις πληροφορίες, τα συστήματα και τα Φυσικά σημεία του Οργανισμού 8](#_Toc184812464)

[6.1. Ηλεκτρονική πρόσβαση 8](#_Toc184812465)

[6.2. Περιορισμοί χρόνου πρόσβασης 9](#_Toc184812466)

[6.3. Απομακρυσμένη πρόσβασης στο δίκτυο του Οργανισμού 9](#_Toc184812467)

[6.4. Διαχείριση ιών 9](#_Toc184812468)

[7. Διαχείριση περιστατικών ασφάλειας πληροφοριών 10](#_Toc184812469)

[8. Απόρριψη μέσων με πληροφορίες του Οργανισμού 10](#_Toc184812470)

[9. Απομάκρυνση εξοπλισμού από τον Οργανισμό 10](#_Toc184812471)

[10. Αναθεώρηση 11](#_Toc184812472)

[11. Αναφορές 12](#_Toc184812473)

[Παράρτημα Α – Λίστα εξωτερικών συνεργατών 13](#_Toc184812474)

# Εισαγωγή

# Σκοπός

Αναγνωρίζοντας τους κινδύνους που υπάρχουν κατά τη διαχείριση πληροφοριών και συστημάτων πληροφορικής του Οργανισμού από τρίτους προμηθευτές και άλλους εξωτερικούς του συνεργάτες ο [Όνομα Οργανισμού] εφαρμόζει την παρούσα πολιτική με στόχο να εξασφαλίσει ότι αυτοί συμμορφώνονται με τις απαιτήσεις ασφαλείας πληροφοριών, διασφαλίζοντας την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών, των συστημάτων και των λειτουργιών του οργανισμού.

# Πεδίο εφαρμογής

Η παρούσα πολιτική διαχείρισης προμηθευτών εφαρμόζεται σε όλους τους τομείς και τα τμήματα του [Όνομα Οργανισμού] που συμμετέχουν στη διαδικασία επιλογής, αξιολόγησης, σύναψης συμβάσεων και διαχείρισης προμηθευτών. Περιλαμβάνει όλες τις κατηγορίες προμηθευτών, από προμηθευτές πρώτων υλών και εξοπλισμού μέχρι παρόχους υπηρεσιών και εξωτερικούς συνεργάτες.

Ισχύει για όλους τους υπαλλήλους των εξωτερικών συνεργατών και των υπεργολάβων τους, που έχουν πρόσβαση σε 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.

# 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.

# Σχέσεις με τρίτα μέρη και προμηθευτές – Συμβάσεις

# Διατήρηση Μητρώου/Λίστας εξωτερικών συνεργατών

Ο [Όνομα Οργανισμού] τηρεί λίστα καταγραφής των τρίτων μερών και προμηθευτών του στην οποία λίστα να αναγράφονται τουλάχιστο 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 πρόσβαση

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

# Συμβάσεις με τους εξωτερικούς συνεργάτες

Σε κάθε σύμβαση μεταξύ του [Όνομα Οργανισμού] και εξωτερικού συνεργάτη καταγράφονται οι απαιτήσεις ασφάλειας πληροφοριών ώστε να διασφαλιστεί το ελάχιστο απαιτούμενο επίπεδο συμμόρφωσης. Οι συμβάσεις αυτές θα πρέπει να περιέχουν κατ’ ελάχιστον τα πιο κάτω ανάλογα με το είδος της Σύμβασης:

1. Συμμόρφωση με τη «Πολιτική Ασφάλειας Πληροφοριών» του [Όνομα Οργανισμού] η οποία θα πρέπει να κοινοποιείται σε όλους τους προμηθευτές και τρίτα μέρη.
2. Συμφωνία Εμπιστευτικότητας ή μη αποκάλυψης, σε περίπτωση που παρέχεται πρόσβαση σε εμπιστευτικές πληροφορίες.
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 από τη λήξη της σύμβασης, ανάλογα με το είδος της πληροφορίας / του εξοπλισμού.
7. Διαδικασίες διαχείρισης αλλαγών σε λογισμικά ή υλισμικά.
8. Περιγραφή του τρόπου με τον οποίο θα διασφαλίζουν ότι πληρούνται απαιτήσεις και διαδικασίες αναφοράς και διαχείρισης συμβάντων ασφάλειας πληροφοριών στον Υπεύθυνο 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. Νομικές και κανονιστικές απαιτήσεις, συμπεριλαμβανομένης της προστασίας δεδομένων, των δικαιωμάτων πνευματικής ιδιοκτησίας και των πνευματικών δικαιωμάτων.
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 Υπεύθυνο Ασφάλειας Πληροφοριών, θα καθορίζει τα πιο πάνω, λαμβάνοντας υπόψη και την κρισιμότητα ή / και την ευαισθησία των πληροφοριών που θα διαχειριστεί ο εξωτερικός συνεργάτης.

# Άλλες συμβατικές Υποχρεώσεις

* Τα τρίτα μέρη πρέπει να ενημερώνονται για σημαντικές αλλαγές σε κρίσιμα συστήματα που επηρεάζουν τις υπηρεσίες που προσφέρουν.
* Όπου εφαρμόζεται, η επιθεώρηση τρίτων μερών και προμηθευτών σε σχέση με την ασφάλεια πληροφοριών πρέπει να ανατίθεται σε ανεξάρτητο τρίτο μέρος.
* Σε περιπτώσεις που τα τρίτα μέρη αποθηκεύουν δεδομένα του[Όνομα Οργανισμού] πρέπει να δίνονται συγκεκριμένες δεσμεύσεις και τεκμηρίωση από την μεριά του τρίτου μέρους για την υλοποίηση των συγκεκριμένων μέτρων ασφάλειας.
* Η συμβατική συμφωνία πρέπει να περιέχει ενέργειες που πρέπει να γίνουν εάν ο εξωτερικός συνεργάτης αγνοήσει τις απαιτήσεις ασφάλειας του [Όνομα Οργανισμού].

# 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.

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.

# Διαδικασία αξιολόγησης εξωτερικού συνεργάτη/προμηθευτή

Ο [Όνομα Οργανισμού] δύναται να θεσπίσει διαδικασία για αξιολόγηση ενός συνεργάτη/προμηθευτή με ενσωμάτωση ολοκληρωμένων απαιτήσεων ασφάλειας πληροφοριών σε μορφή απαιτήσεων/κριτηρίων συμμόρφωσης όπου το κρίνει απαραίτητο. Τα κριτήρια αυτά τα οποία δύναται να κάνουν αναφορά σε σχετικά πρότυπα ασφαλείας και άλλες καλές πρακτικές, (π.χ. ISO 27001, NIST, Μοντέλο Ωριμότητας Κυβερνοασφάλειας της Αρχής, Πλαίσιο ΚΥΒΕΡΝΟ-ΥΓΙΕΙΝΗΣ και άλλα) , για τον καθορισμό βασικών προσδοκιών, και 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

# 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».

# Πρόσβαση στις πληροφορίες, τα συστήματα και τα Φυσικά σημεία του Οργανισμού

Πρόσβαση του εξωτερικού συνεργάτη σε συστήματα πληροφορικής ή σε φυσικά σημεία (π.χ κτήρια) του [Όνομα Οργανισμού] θα δίνεται κατόπιν εφαρμογής της σχετικής «Διαδικασίας Διαχείρισης Πρόσβασης Χρηστών» και των οδηγιών που εκδίδονται από τους διαχειριστές των συστημάτων φυσικής ασφαλείας των κτηρίων του [Όνομα Οργανισμού] (βλέπε Πολιτική Ελέγχου Πρόσβασης και Πολιτική Φυσικής Ασφάλειας).

Η φυσική πρόσβαση των εξωτερικών συνεργατών στα κτήρια του [Όνομα Οργανισμού] θα παρακολουθείται ανά τακτά χρονικά διαστήματα από το συντονιστή της σύμβασης, και θα πρέπει να απενεργοποιείται με την ολοκλήρωση των συμβατικών υποχρεώσεων του ανάδοχου.

# Ηλεκτρονική πρόσβαση

Για να παρασχεθεί ηλεκτρονική πρόσβαση στα συστήματα του [Όνομα Οργανισμού] , είναι απαραίτητο όπως:

1. Ο εξωτερικός συνεργάτης υπογράψει συμφωνία εμπιστευτικότητας.
2. Του δοθεί πρόσβαση για διεκπεραίωση των καθηκόντων του στη βάση της αρχής της ανάγκης γνώσης και εφόσον κριθεί απαραίτητο από τον ιδιοκτήτη του εκάστοτε συστήματος για τη σχετική ανάγκη.
3. Η πρόσβαση περιορίζεται στα συμφωνημένα, μέθοδο, δικαιώματα και επίπεδο λειτουργικότητας.
4. Η πρόσβαση γίνεται μέσω μοναδικού ονόματος χρήστη(named user) 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 ώστε να απενεργοποιούνται άμεσα.

Το Τμήμα Πληροφορικής [Όνομα Οργανισμού] είναι υπεύθυνο να αναθεωρεί τις προσβάσεις των εξωτερικών συνεργατών σε τακτικά χρονικά διαστήματα (όχι πέραν των τεσσάρων μηνών) σε συνεργασία με το συντονιστή της σύμβασης 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 εξ ορισμού απενεργοποιημένη και να ενεργοποιείται από τα αρμόδια άτομα του Τμήματος Πληροφορικής του [Όνομα Οργανισμού] μετά την ολοκλήρωση της ταυτοποίηση των χρηστών. Οποιαδήποτε ύποπτη ενέργεια χρειάζεται ανάλογα να αναφέρεται στο συντονιστή της σύμβασης ή στον Υπεύθυνο Ασφάλειας Πληροφοριών για περεταίρω διερεύνηση.

# Απομακρυσμένη πρόσβασης στο δίκτυο του Οργανισμού

Όλες οι εξ’ αποστάσεως προσβάσεις στα συστήματα πληροφορικής του [Όνομα Οργανισμού] χρειάζεται να έχουν την εκ των προτέρων έγκριση του Προϊσταμένου του Τμήματος Πληροφορικής του [Όνομα Οργανισμού]. 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 εξ’ αποστάσεως προσβάσεις θα πρέπει απαραίτητα να προστατεύονται με τη χρήση επαλήθευσης μέσω πολλών παραγόντων (Multi-Factor Authentication - MFA).

# Διαχείριση ιών

Το κατάλληλο ενεργό και ενημερωμένο λογισμικό κατά των ιών είναι απαραίτητο να εγκατασταθεί σε όλους τους υπολογιστές και τους εξυπηρετητές στους οποίους δίδεται πρόσβαση στο δίκτυο του [Όνομα Οργανισμού]. 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 του [Όνομα Οργανισμού] και στον Υπεύθυνο Ασφάλειας Πληροφοριών του [Όνομα Οργανισμού].

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/και στο Υπεύθυνο 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 και αναλύσει όλα τα απαραίτητα στοιχεία, όπου απαιτείται, και να εφαρμόσει τα κατάλληλα μέτρα αντιμετώπισης τους.

# Απόρριψη μέσων με πληροφορίες του Οργανισμού

Τα μέσα που χρησιμοποίησε ο ανάδοχος στα πλαίσια της σύμβασης με τον [Όνομα Οργανισμού] και περιέχουν πληροφορίες του Οργανισμού, θα πρέπει να απορρίπτονται με ασφάλεια, με φυσική καταστροφή του χαρτιού ή του πολυμέσου μέσω 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.

# Αναθεώρηση

Τα έγγραφα σχετικά με τη Διαχείρισης Προμηθευτών θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] π.χ. υπογραφή σύμβασης με νέο Προμηθευτή.

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Διαχείριση Τρίτων Μερών Και Προμηθευτών | TPS1 | Δέουσα επιμέλεια για τρίτα μέρη και προμηθευτές | Να επιδεικνύει τη δέουσα επιμέλεια σχετικά με τρίτα μέρη και προμηθευτές. |
| Διαχείριση Τρίτων Μερών Και Προμηθευτών | TPS2 | Σχέσεις με τρίτα μέρη και προμηθευτές | Να διασφαλιστεί η ενσωμάτωση συμβατικών ρητρών ασφάλειας πληροφοριών στις σχέσεις με τρίτα μέρη και προμηθευτές. |
| Διαχείριση Αλλαγών | CM1 | Διαχείριση Αλλαγών | Να διασφαλιστεί ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών. |
| Ασφάλεια Δεδομένων | DS1 | Διαχείριση του κύκλου ζωής των πληροφοριών | Να εξασφαλιστεί η προστασία δεδομένων καθ’ όλο τον κύκλο ζωής των πληροφοριών, συμπεριλαμβανομένης της συλλογής, καταχώρησης, οργάνωσης, δομής, αποθήκευσης, προσαρμογής ή μεταβολής, ανάκτησης, αναζήτησης, χρήσης, κοινοποίησης με διαβίβαση, διάδοσης ή κάθε άλλη μορφή διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής. |
| Ασφάλεια Ανθρωπίνων Πόρων | HRS4 | Εξωτερικού συνεργάτες | Να εξασφαλιστεί ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών. και τους στόχους ασφάλειας του οργανισμού. |

# 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) |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |