****

Πίνακας περιεχομένων

[1. Σκοπός - 2 -](#_Toc125238591)

[2. Πεδίο εφαρμογής - 2 -](#_Toc125238592)

[3. Απαιτήσεις Ενδιαφερόμενων μερών - 3 -](#_Toc125238593)

[4. Στόχος Συστήματος Ασφάλειας Πληροφοριών - 3 -](#_Toc125238594)

[5. Πεδίο Εφαρμογής Συστήματος Ασφάλειας Πληροφοριών - 4 -](#_Toc125238595)

[6. Υπεύθυνος Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών - 4 -](#_Toc125238596)

[7. Λειτουργικές Ευθύνες - 5 -](#_Toc125238597)

[7.1. Εκτελεστική Διοίκηση - 5 -](#_Toc125238598)

[7.2. Διοίκηση Πληροφορικής - 5 -](#_Toc125238599)

[7.3. Εργατικό Δυναμικό - 6 -](#_Toc125238600)

[8. Κατηγοριοποίηση και χειρισμός πληροφοριών - 6 -](#_Toc125238601)

[9. Διαχείριση περιουσιακών στοιχείων πληροφορικής - 6 -](#_Toc125238602)

[10. Ασφάλεια προσωπικού - 7 -](#_Toc125238603)

[11. Διαχείριση περιστατικού κυβερνοασφάλειας - 7 -](#_Toc125238604)

[12. Φυσική και περιβαλλοντική ασφάλεια - 8 -](#_Toc125238605)

[13. Διαχείριση λογαριασμών και έλεγχος πρόσβασης - 8 -](#_Toc125238606)

[14. Ασφάλεια συστημάτων - 9 -](#_Toc125238607)

[15. Διαχείριση ευπαθειών - 9 -](#_Toc125238608)

[16. Ασφάλεια διαδικασιών - 10 -](#_Toc125238609)

[17. Συμμόρφωση - 11 -](#_Toc125238610)

[18. Ιστορικό αναθεωρήσεων - 11 -](#_Toc125238611)

**Διαγνωστικό Κέντρο**

**ΠΑΠ.01**

**Εκδ. 1**

**10.01.2023**

**Πολιτική Ασφάλειας Πληροφοριών**

# 1. Σκοπός

Σκοπός της παρούσας Πολιτικής Ασφάλειας είναι η διασφάλιση των πληροφοριών που ανήκουν στο Διαγνωστικό Κέντρο και στα ενδιαφερόμενα μέρη του (προσωπικό, ασθενείς), μέσα σε ένα ασφαλές περιβάλλον, αλλά και η ενημέρωση των τελευταίων για τις αρχές που διέπουν την κατοχή, χρήση και διάθεση πληροφοριών.

Οι στόχοι του Συστήματος Ασφάλειας Πληροφοριών του Διαγνωστικού Κέντρου είναι:

* Η προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση ή κακή χρήση.
* Η διασφάλιση της εμπιστευτικότητας των πληροφοριών.
* Η διασφάλιση της ακεραιότητας των πληροφοριών.
* Η διατήρηση της διαθεσιμότητας των πληροφοριών και των πληροφοριακών συστημάτων παροχής υπηρεσιών.
* Η διατήρηση των διαδικασιών σχεδιασμού επιχειρησιακής συνέχειας.
* Η τήρηση των κανονιστικών, συμβατικών και νομικών απαιτήσεων.
* Η διατήρηση της φυσικής, λογικής, περιβαλλοντικής και επικοινωνιακής ασφάλειας.
* Η κατάλληλη απόρριψη των πληροφοριών, όταν αυτές δεν είναι πλέον χρήσιμες.
* Η πειθαρχική ή ποινική δίωξη σε περίπτωση παραβίασης της παρούσας Πολιτικής Ασφάλειας.

# 2. Πεδίο εφαρμογής

Η παρούσα Πολιτική Ασφάλειας περιλαμβάνει όλα τα συστήματα, αυτοματοποιημένα και χειροκίνητα, για τα οποία το Διαγνωστικό Κέντρο έχει διοικητική ευθύνη, συμπεριλαμβανομένων των δεδομένων που διαχειρίζεται. Απευθύνεται σε όλες τις πληροφορίες, ανεξαρτήτως δομής ή μορφής, που δημιουργούνται ή χρησιμοποιούνται για την υποστήριξη επιχειρηματικών δραστηριοτήτων. Η παρούσα Πολιτική Ασφάλειας αναπτύχθηκε και εφαρμόζεται εντός των πλαισίων λειτουργίας του Διαγνωστικού Κέντρου και σύμφωνα με το πρότυπο ISO 27001:2013.

# 3. Απαιτήσεις Ενδιαφερόμενων μερών

|  |  |
| --- | --- |
| **Ενδιαφερόμενα μέρη** | **Απαιτήσεις** |
| **Προσωπικό** | * Να μη διαρρεύσουν τα προσωπικά τους δεδομένα. * Να τους παρέχονται σωστές πληροφορίες. * Να μη διαρρεύσει μέρος της σύμβασης που αναγράφει προσωπικά ή οικονομικά δεδομένα |
| **Ασθενείς** | * Να μη διαρρεύσουν τα προσωπικά τους δεδομένα. * Να μη διαρρεύσουν τα ιατρικά τους δεδομένα. * Να τους παρέχονται ιατρικές πληροφορίες με ακεραιότητα και εμπιστευτικότητα. * Να διατηρούνται τα δεδομένα τους στους διακομιστές του Διαγνωστικού Κέντρου με ασφάλεια. |
| **Ιδιοκτήτες** | * Να μη διαρρεύσουν οικονομικά στοιχεία. * Να μη διαρρεύσουν προσωπικά δεδομένα υπαλλήλων ή ασθενών. * Να συμμορφώνεται το Διαγνωστικό Κέντρο με τη νομοθεσία. * Να μη διαρρεύσουν διαβαθμισμένες πληροφορίες. |
| **Προμηθευτές** | * Να μη διαρρεύσουν οι συμβάσεις συνεργασίας. * Να μη διαρρεύσει τεχνογνωσία. * Να μη διαρρεύσουν οικονομικές συμφωνίες. |
| **Κυβέρνηση** | * Να συμμορφώνεται το Διαγνωστικό Κέντρο με τη νομοθεσία. |

# 4. Στόχος Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

Στόχος του Συστήματος Ασφάλειας Πληροφοριών είναι να προστατέψει τα πληροφοριακά περιουσιακά στοιχεία του Διαγνωστικού Κέντρου, του προσωπικού και των ασθενών του από όλες τις εσωτερικές, εξωτερικές εκούσιες ή ακούσιες απειλές.

Οι επιμέρους στόχοι του Διαγνωστικού Κέντρου σχετικά με την ασφάλεια της πληροφορίας είναι:

* Η προστασία της ψηφιακής διαχείρισης και επεξεργασίας των ιατρικών πληροφοριών από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση.
* Η διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.
* Η διασφάλιση της τήρησης των νομοκανονιστικών απαιτήσεων.
* Η αυτοματοποίηση χειρωνακτικών εργασιών, με σκοπό την γρηγορότερη επεξεργασία δεδομένων και κατά συνέπεια, την καλύτερη οικονομική και διοικητική οργάνωση.

# 5. Πεδίο Εφαρμογής Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

Το Διαγνωστικό Κέντρο παρέχει σε δύο ειδών ιατρικές υπηρεσίες: την κλινική παθολογία (π.χ. μικροβιολογία) και την ανατομική παθολογία (π.χ. κυτταρολογία). Οι υπηρεσίες αυτές προσφέρονται τόσο σε εσωτερικούς και εξωτερικούς ασθενείς νοσοκομείων, όσο και σε κλινικούς και άλλους μη νοσοκομειακούς ασθενείς. Συνεπώς, σκοπός του είναι η διασφάλιση της ασφάλειας των αγαθών του, στα οποία περιλαμβάνονται τα προσωπικά δεδομένα των υπαλλήλων και των ασθενών, τα ιατρικά δεδομένα των ασθενών, τα ιατρικά μηχανήματα και όλες τις υποδομές πληροφορικής συμπεριλαμβανομένων των λογισμικών που εκτελούνται. Ως μία επιχείρηση που δραστηριοποιείται μόνο δια ζώσης, οποιεσδήποτε διαδικασίες «απομακρυσμένης φύσεως» εξαιρούνται από το πεδίο εφαρμογής.

# 6. Υπεύθυνος Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

Υπεύθυνος Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, εφαρμογής, επιμέλειας και αναθεώρησης της παρούσας Πολιτικής Ασφάλειας, καθώς και εκπαίδευσης του προσωπικού σε θέματα ασφαλείας ορίζεται ο κ. Κωνσταντίνος Γεωργίου.

# 7. Λειτουργικές Ευθύνες

## 7.1. Εκτελεστική Διοίκηση

* Διασφάλιση της εφαρμογής ενός κατάλληλου Προγράμματος Ασφάλειας Πληροφοριών βάσει κινδύνου για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας όλων των πληροφοριών που συλλέγονται ή διατηρούνται από το Διαγνωστικό Κέντρο.
* Διασφάλιση ότι οι διαδικασίες ασφάλειας πληροφοριών ενσωματώνονται σε διαδικασίες στρατηγικού και επιχειρησιακού σχεδιασμού για τη διασφάλιση της αποστολής του οργανισμού.
* Διασφάλιση ότι στη διαδικασία κατάρτισης προϋπολογισμού ή/και οικονομικού σχεδιασμού περιλαμβάνονται επαρκείς οικονομικοί πόροι για την ασφάλεια των πληροφοριών.
* Διασφάλιση ότι παρέχεται στους υπεύθυνους ασφαλείας η απαραίτητη εξουσιοδότηση για την ασφάλεια των πληροφοριών που βρίσκονται υπό τον έλεγχό τους εντός του πεδίου εφαρμογής του Προγράμματος Ασφάλειας Πληροφοριών του Διαγνωστικού Κέντρου.

## 7.2. Διοίκηση Πληροφορικής

* Υποστήριξη της ασφάλειας με την παροχή σαφούς κατεύθυνσης και εξέτασης των ελέγχων ασφαλείας στις υποδομές επεξεργασίας δεδομένων και στα δίκτυα υπολογιστών.
* Παροχή των πόρων που απαιτούνται για τη διατήρηση ενός επιπέδου ελέγχου της ασφάλειας των πληροφοριών σύμφωνα με την παρούσα Πολιτική Ασφάλειας.
* Προσδιορισμός και εφαρμογή όλων των διαδικασιών, πολιτικών και ελέγχων που σχετίζονται με τις απαιτήσεις ασφαλείας που ορίζονται από την επιχείρηση και την παρούσα Πολιτική Ασφάλειας.
* Ενθάρρυνση της συμμετοχής του τεχνικού προσωπικού και του προσωπικού ασφάλειας πληροφοριών στην προστασία των πληροφοριακών πόρων, καθώς και στον προσδιορισμό, την επιλογή και την εφαρμογή κατάλληλων και οικονομικά αποδοτικών ελέγχων και διαδικασιών ασφαλείας.

## 7.3. Εργατικό Δυναμικό

* Κατανόηση των βασικών ελέγχων ασφάλειας πληροφοριών που είναι αναγκαίοι για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.
* Προστασία πληροφοριών από μη εξουσιοδοτημένη χρήση ή αποκάλυψη.
* Προστασία προσωπικών, ιδιωτικών και ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη χρήση ή αποκάλυψη.
* Συναίνεση και συμμόρφωση με όλες τις ισχύουσες πολιτικές, πρότυπα και κατευθυντήριες γραμμές που έχουν θεσπιστεί.

# 8. Κατηγοριοποίηση και χειρισμός πληροφοριών

* Όλες οι πληροφορίες, οι οποίες δημιουργούνται, αποκτώνται ή χρησιμοποιούνται για την υποστήριξη επιχειρηματικών δραστηριοτήτων, πρέπει να χρησιμοποιούνται μόνο για τον επιδιωκόμενο επιχειρηματικό σκοπό.
* Η σωστή διαχείριση των πληροφοριών πρέπει να γίνεται, μέσω της εξουσιοδοτημένης χρήσης, από τη δημιουργία τους έως τη διάθεσή τους.
* Όλες οι πληροφορίες πρέπει να διαβαθμίζονται σε τακτικά με βάση τα χαρακτηριστικά εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητάς τους.
* Η συγχώνευση πληροφοριών που δημιουργεί ένα νέο πληροφοριακό στοιχείο ή καταστάσεων που παρουσιάζουν το ενδεχόμενο συγχώνευσης (π.χ. εφεδρική μαγνητική ταινία με πολλά αρχεία) πρέπει να αξιολογηθεί για να προσδιοριστεί εάν δικαιολογείται μια νέα ταξινόμηση των συγχωνευμένων δεδομένων.
* Το Διαγνωστικό Κέντρο πρέπει να κοινοποιεί τις απαιτήσεις ασφαλούς χειρισμού των πληροφοριών στο εργατικό δυναμικό του.
* Πρέπει να τηρείται γραπτή ή ηλεκτρονική απογραφή όλων των πληροφοριακών στοιχείων.

# 9. Διαχείριση περιουσιακών στοιχείων πληροφορικής

* Όλα τα περιουσιακά στοιχεία υλικού και λογισμικού πληροφορικής πρέπει να εκχωρηθούν σε μια καθορισμένη επιχειρηματική οντότητα.
* Οι οντότητες υποχρεούνται να διατηρούν κατάσταση περιουσιακών στοιχείων υλικού και λογισμικού, συμπεριλαμβανομένων όλων των στοιχείων του συστήματος (π.χ. διεύθυνση δικτύου, όνομα μηχανήματος, έκδοση λογισμικού) σε επίπεδο λεπτομέρειας που κρίνεται απαραίτητο για την παρακολούθηση και την υποβολή εκθέσεων. Ο κατάλογος αυτός πρέπει να αυτοματοποιείται όπου αυτό είναι τεχνικά εφικτό.
* Διαδικασίες, όπως η τακτική σάρωση, πρέπει να εφαρμόζονται για τον εντοπισμό μη εξουσιοδοτημένου υλικού ή / και λογισμικού και την ειδοποίηση του κατάλληλου προσωπικού όταν ανακαλύπτονται.

# 10. Ασφάλεια προσωπικού

* Το εργατικό δυναμικό πρέπει να λάβει γενική εκπαίδευση ευαισθητοποίησης για την ασφάλεια, συμπεριλαμβανομένης της αναγνώρισης και αναφοράς εσωτερικών απειλών, εντός 30 ημερών από την πρόσληψη. Πρέπει να ολοκληρώνεται πρόσθετη κατάρτιση σχετικά με ειδικές διαδικασίες ασφαλείας, εφόσον απαιτείται, προτού παρασχεθεί πρόσβαση σε ευαίσθητες πληροφορίες συγκεκριμένων οντοτήτων που δεν καλύπτονται από τη γενική εκπαίδευση ασφαλείας. Όλη η εκπαίδευση ασφαλείας πρέπει να επαναλαμβάνεται τουλάχιστον ετησίως και πρέπει να παρακολουθείται από το σύνολο του εργατικού δυναμικού.
* Όλες οι θέσεις εργασίας πρέπει να αξιολογούνται για να καθοριστεί εάν απαιτούν πρόσβαση σε ευαίσθητες πληροφορίες ή / και ευαίσθητα στοιχεία πληροφοριών.
* Πρέπει να οριστεί μια διαδικασία για την επανάληψη ή την αναθεώρηση των προσδιορισμών καταλληλότητας περιοδικά και κατά την αλλαγή των καθηκόντων ή της θέσης εργασίας.
* Οι οντότητες είναι υπεύθυνες για τη διασφάλιση ότι όλα τα εκδοθέντα περιουσιακά στοιχεία επιστρέφονται πριν από την αποχώριση ενός υπαλλήλου, την απενεργοποίηση των λογαριασμών και την αφαίρεση της πρόσβασης.

# 11. Διαχείριση περιστατικού κυβερνοασφάλειας

* Οι οντότητες πρέπει να διαθέτουν σχέδιο αντιμετώπισης συμβάντων και συνεπή πρότυπα για την αποτελεσματική αντιμετώπιση περιστατικών που θέτουν σε κίνδυνο την ασφάλεια των πληροφοριών και των συστημάτων.
* Όλα τα παρατηρούμενα ή εικαζόμενα συμβάντα ή αδυναμίες που αφορούν την ασφάλεια των πληροφοριών πρέπει να αναφέρονται στον Υπεύθυνο Συστήματος Ασφάλειας Πληροφοριών το συντομότερο δυνατόν.

# 12. Φυσική και περιβαλλοντική ασφάλεια

* Οι εγκαταστάσεις επεξεργασίας και αποθήκευσης πληροφοριών πρέπει να διαθέτουν καθορισμένη περίμετρο ασφαλείας και κατάλληλους φραγμούς ασφαλείας και ελέγχους πρόσβασης.
* Πρέπει να διενεργείται περιοδική αξιολόγηση κινδύνου για τις εγκαταστάσεις επεξεργασίας και αποθήκευσης πληροφοριών, προκειμένου να προσδιορίζεται κατά πόσον οι υφιστάμενοι έλεγχοι λειτουργούν σωστά και εάν απαιτούνται πρόσθετα μέτρα φυσικής ασφάλειας για τον μετριασμό των κινδύνων.
* Πρέπει να διενεργούνται τακτικοί ειδικοί έλεγχοι για την προστασία των υποστηρικτικών υποδομών και εγκαταστάσεων, όπως οι υποδομές παροχής ηλεκτρικής ενέργειας και καλωδίωσης.
* Όλος ο εξοπλισμός της τεχνολογίας των πληροφοριών και τα μέσα αποθήκευσης πληροφοριών πρέπει να ασφαλίζονται ώστε να αποφεύγεται η διαρροή της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας σύμφωνα με τη διαβάθμιση των πληροφοριών που περιέχονται σε αυτά.
* Το προσωπικό συντήρησης των εγκαταστάσεων επεξεργασίας και αποθήκευσης πληροφοριών πρέπει να συνοδεύεται ανά πάσα στιγμή.

# 13. Διαχείριση λογαριασμών και έλεγχος πρόσβασης

* Σε όλους τους τύπους λογαριασμών πρέπει να έχει ανατεθεί μία οντότητα που θα είναι υπεύθυνη για τη διαχείριση τους.
* Η πρόσβαση στα συστήματα πρέπει να παρέχεται μέσω της χρήσης ατομικά εκχωρημένων μοναδικών αναγνωριστικών κωδικών, γνωστών ως «αναγνωριστικά χρήστη» (user ID).
* Κάθε αναγνωριστικό χρήστη είναι συσχετισμένο με ένα διακριτικό ελέγχου ταυτότητας (π.χ. κωδικός πρόσβασης, βιομετρικό δεδομένο) που πρέπει την εξακρίβωση της ταυτότητας του ατόμου ή του συστήματος που ζητά πρόσβαση.
* Πρέπει να εφαρμόζονται αυτοματοποιημένες τεχνικές και έλεγχοι για το κλείδωμα μιας συνεδρίας και να απαιτείται έλεγχος ταυτότητας ή εκ νέου έλεγχος ταυτότητας μετά από μια περίοδο αδράνειας για οποιοδήποτε σύστημα όπου είναι απαραίτητη η ταυτοποίηση. Οι πληροφορίες στην οθόνη πρέπει να αντικατασταθούν με δημόσια ορατές πληροφορίες (π.χ. προφύλαξη οθόνης, κενή οθόνη, ρολόι) κατά τη διάρκεια του κλειδώματος της συνεδρίας.

# 14. Ασφάλεια συστημάτων

* Απαραίτητη ανάθεση ευθύνης στις οντότητες για τη συντήρηση και τη διαχείριση ενός συστήματος που χρησιμοποιείται για λογαριασμό του Διαγνωστικού Κέντρου. Πρέπει να διατηρείται ένας κατάλογος των εκχωρημένων οντοτήτων.
* Κάθε σύστημα πρέπει να διαθέτει ένα σύνολο ελέγχων ανάλογο με την κατηγοριοποίηση των δεδομένων που αποθηκεύονται στο σύστημα ή διέρχονται από αυτό.
* Όλα τα ρολόγια των συστημάτων πρέπει να συγχρονίζονται με μια κεντρική πηγή αναφοράς χρόνου που έχει οριστεί σε UTC (Συντονισμένη Παγκόσμια Ώρα), η οποία, με τη σειρά της, είναι συγχρονισμένη με τουλάχιστον τρεις συγχρονισμένες πηγές ώρας.
* Οι συνδέσεις μεταξύ των συστημάτων πρέπει να εγκρίνονται από την εκτελεστική διοίκηση όλων των σχετικών οντοτήτων και να προστατεύονται με τη διενέργεια κατάλληλων ελέγχων.
* Η διαχείριση του δικτύου πρέπει να πραγματοποιείται από ασφαλές, ειδικό δίκτυο.
* Ο έλεγχος ταυτότητας απαιτείται για όλους τους χρήστες που συνδέονται σε εσωτερικά συστήματα.
* Απαιτείται έλεγχος ταυτότητας δικτύου για όλες τις συσκευές που συνδέονται σε εσωτερικά δίκτυα.

# 15. Διαχείριση ευπαθειών

* Όλα τα συστήματα πρέπει να σαρωθούν για ευπάθειες πριν χρησιμοποιηθούν για πρώτη φορά και περιοδικά έκτοτε.
* Απαιτούνται περιοδικοί έλεγχοι διείσδυσης για όλα τα κρίσιμα περιβάλλοντα/συστήματα.
* Απαιτείται τακτική ενημέρωση του λογισμικών των συστημάτων, για την πρόληψη τυχόν ευπαθειών.

# 16. Ασφάλεια διαδικασιών

* Όλα τα συστήματα και οι φυσικές εγκαταστάσεις στις οποίες βρίσκονται πρέπει να έχουν τεκμηριωμένες οδηγίες λειτουργίας, διαδικασίες διαχείρισης και επίσημες διαδικασίες διαχείρισης συμβάντων που σχετίζονται με θέματα ασφάλειας πληροφοριών, οι οποίες καθορίζουν τους ρόλους και τις ευθύνες των επηρεαζόμενων οντοτήτων που τα χρησιμοποιούν.
* Οι διαμορφώσεις των συστημάτων πρέπει να ακολουθούν εγκεκριμένα πρότυπα διαμόρφωσης.
* Πρέπει να πραγματοποιείται εκ των προτέρων σχεδιασμός και προετοιμασία, ώστε να διασφαλίζεται η διαθεσιμότητα επαρκούς χωρητικότητας και πόρων. Η χωρητικότητα του συστήματος πρέπει να παρακολουθείται σε συνεχή βάση.
* Τα τείχη προστασίας που βασίζονται σε κεντρικό υπολογιστή πρέπει να είναι εγκατεστημένα και ενεργοποιημένα σε όλους τους σταθμούς εργασίας για προστασία από απειλές και περιορισμό της πρόσβασης μόνο σε ό,τι απαιτείται.
* Οι έλεγχοι (π.χ. προγράμματα προστασίας από ιούς, ελεγκτές ακεραιότητας λογισμικού, φιλτράρισμα ιστού) πρέπει να εφαρμόζονται σε όλα τα συστήματα, όπου αυτό είναι τεχνικά εφικτό, για την πρόληψη και τον εντοπισμό της εκτέλεσης κακόβουλου κώδικα ή άλλων απειλών.
* Πρέπει να εφαρμοστούν στοιχεία ελέγχου για την απενεργοποίηση της αυτόματης εκτέλεσης περιεχομένου από αφαιρούμενα μέσα.
* Πρέπει να εφαρμόζονται έλεγχοι για τον περιορισμό της αποθήκευσης πληροφοριών σε εξουσιοδοτημένες τοποθεσίες.
* Πρέπει να υπάρχουν στοιχεία ελέγχου που να επιτρέπουν την εκτέλεση μόνο εγκεκριμένου λογισμικού σε ένα σύστημα και να εμποδίζουν την εκτέλεση οποιουδήποτε άλλου λογισμικού.
* Όλα τα συστήματα πρέπει να συντηρούνται σε επίπεδο που υποστηρίζεται από τον προμηθευτή για να διασφαλιστεί η ακρίβεια και η ακεραιότητα.
* Όλες οι ενημερώσεις κώδικα ασφαλείας πρέπει να εξετάζονται, να αξιολογούνται και να εφαρμόζονται εγκαίρως. Η διαδικασία αυτή πρέπει να είναι αυτοματοποιημένη, όπου αυτό είναι τεχνικά εφικτό.
* Τα συστήματα-λογισμικά που δεν μπορούν πλέον να υποστηριχθούν ή να ενημερωθούν σε νεότερες εκδόσεις πρέπει να καταργηθούν.
* Αντίγραφα ασφαλείας των πληροφοριών των οντοτήτων, του λογισμικού και των ειδώλων συστήματος πρέπει να λαμβάνονται τακτικά.
* Τα αντίγραφα ασφαλείας και η διαδικασία αποκατάστασης πρέπει να ελέγχονται τακτικά.
* Πρέπει να θεσπιστούν διαδικασίες για τη διατήρηση της ασφάλειας των πληροφοριών κατά τη διάρκεια ενός ανεπιθύμητου συμβάντος.

# 17. Συμμόρφωση

Η παρούσα Πολιτική Ασφάλειας τίθεται σε ισχύ από τη δημοσίευσή της. Αναμένεται συμμόρφωση με όλες τις εταιρικές πολιτικές και πρότυπα. Οι πολιτικές και τα πρότυπα μπορούν να τροποποιηθούν ανά πάσα στιγμή. αναμένεται συμμόρφωση με τις τροποποιημένες πολιτικές και πρότυπα.

Εάν η συμμόρφωση με την παρούσα Πολιτική Ασφάλειας δεν είναι δυνατή ή τεχνικά εφικτή ή εάν η απόκλιση από την Πολιτική Ασφάλειας αυτή είναι απαραίτητη για την υποστήριξη μιας επιχειρηματικής λειτουργίας, είναι απαραίτητο το αίτημα εξαίρεσης μέσω της διαδικασίας εξαίρεσης που παρέχει ο Υπεύθυνος Συστήματος Ασφάλειας Πληροφοριών.

# 18. Ιστορικό αναθεωρήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Έκδοση** | **Ημ/νία Τροποποίησης** | **Ημ/νία Έγκρισης** | **Εγκρίθηκε από** | **Περιγραφή** |
| 1.0 | 10 Ιανουαρίου 2023 | 10 Ιανουαρίου 2023 | Κ. Γεωργίου | Αρχική Έκδοση σύμφωνα με απαιτήσεις ISO 27001:2013 |
|  |  |  |  |  |