Τελική Εργασία Ερώτημα 1β

Πολιτική Ασφάλειας Πληροφοριών ΧΑΝΙΣΤ Α.Ε

Έγγραφο

Αυτή είναι η πολιτική ασφάλειας πληροφοριών για την ΧΑΝΙΣΤ Α.Ε.

Εγκριτής

Αυτή η πολιτική έχει εγκριθεί από την επιτροπή διαχείρισης ασφάλειας πληροφοριών της ΧΑΝΙΣΤ Α.Ε. Οι αλλαγές πραγματοποιούνται από τον διαχειριστή ασφάλειας πληροφοριών, ο οποίος έχει εξουσιοδοτήσει την επιτροπή να ενημερώνει αυτό το έγγραφο.

Ιστορικό έκδοσης

2023-01-16

Σχετικά με

Αυτή είναι η πολιτική ασφάλειας πληροφοριών για την ΧΑΝΙΣΤ Α.Ε. Ισχύει για όλες τις επιχειρηματικές μονάδες και όλο το προσωπικό.

Αυτό το έγγραφο συντάχθηκε από την ομάδα ασφάλειας στον κυβερνοχώρο ΧΑΝΙΣΤ Α.Ε. Είναι διαθέσιμο σε όλο το προσωπικό και τρίτα μέρη που πρέπει να γνωρίζουν την πολιτική.

Οι παραβιάσεις αυτής της πολιτικής πρέπει να αναφέρονται στη διεύθυνση ασφαλείας.

Πολιτική

Πεδίο εφαρμογής

Αυτή η πολιτική ισχύει για την ΧΑΝΙΣΤ Α.Ε σε όλες τις τοποθεσίες και όλες τις επιχειρηματικές μονάδες. Ισχύει για όλο το προσωπικό, συμπεριλαμβανομένων του προσωπικού της εταιρείας, των συμβούλων και του έκτακτου προσωπικού. Η πολιτική ισχύει για όλες τις πληροφορίες, συμπεριλαμβανομένων των άυλων περιουσιακών στοιχείων και των φυσικών περιουσιακών στοιχείων, των συστημάτων υπολογιστών και των δεδομένων. Ισχύει οπουδήποτε υποβάλλονται σε επεξεργασία τα δεδομένα της ΧΑΝΙΣΤ Α.Ε.

Στόχοι

Οι στόχοι της πολιτικής είναι να διασφαλίσει ότι οι πληροφορίες της ΧΑΝΙΣΤ Α.Ε προστατεύονται κατάλληλα. Αναλυτικότερα:

1. Διασφάλιση της κατάλληλης διαχείρισης των κινδύνων για τις πληροφορίες.
2. Βεβαίωση ότι οι χρήστες έχουν πρόσβαση σε ακριβή και αξιόπιστα δεδομένα.
3. Βεβαίωση ότι η πρόσβαση στα δεδομένα παρέχεται σε άτομα που έχουν νόμιμη ανάγκη να γνωρίζουν.
4. Βεβαίωση ότι η πρόσβαση στα δεδομένα παρέχεται σε άτομα με βάση τις αρχές των ελάχιστων προνομίων.
5. Βεβαίωση ότι το προσωπικό έχει τις γνώσεις για να εργάζεται με ασφάλεια.
6. Βεβαίωση ότι ορίζονται και εφαρμόζονται διορθωτικές ενέργειες.

Ορισμοί

Εμπιστευτικότητα
Η ιδιότητα ότι οι πληροφορίες δεν διατίθενται ή αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες.
Ακεραιότητα
Η ιδιότητα της διασφάλισης της ακρίβειας και της πληρότητας των περιουσιακών στοιχείων.
Διαθεσιμότητα
Το πληροφοριακό σύστημα να είναι προσβάσιμο και χρησιμοποιήσιμο κατόπιν αιτήματος από εξουσιοδοτημένο φορέα.
Αυθεντικότητα
Η ιδιοκτησία μιας οντότητας να είναι αυτό που ισχυρίζεται ότι είναι.

Ευθύνη
Η ανάθεση ενεργειών και αποφάσεων σε μια οντότητα.
Μη αποκήρυξη
Η ικανότητα να αποδεικνύεται η εμφάνιση ενός γεγονότος ή μιας ενέργειας και των οντοτήτων που προέρχονται από αυτή.
Αξιοπιστία
Η ιδιότητα της συνεπούς επιδιωκόμενης συμπεριφοράς και αποτελεσμάτων.

Συμφραζόμενα

Η ΧΑΝΙΣΤ Α.Ε είναι μια πολυεθνική εταιρεία που προσφέρει ένα λογισμικό εξυπηρέτησης ασθενών και ιατρών σε πληθώρα νοσοκομείων ανά τον κόσμο. Λειτουργεί με έδρα της το Πανεπιστήμιο Πειραιώς (Καραολή κ. Δημητρίου, Πειραιάς 185 34)

Εσωτερικά και εξωτερικά θέματα

Το εξωτερικό πλαίσιο περιλαμβάνει:

- Κανονισμοί και νόμοι που αφορούν την πώληση και χρήση του λογισμικού.
- Συναγωνιστές
- Το γενικό κοινό
- Εταιρείες που παρέχουν το λογισμικό

Το εσωτερικό πλαίσιο περιλαμβάνει:

- Εσωτερικός λογιστικός έλεγχος
- Οι ανάγκες του προσωπικού
- Οι επιχειρηματικοί στόχοι της ΧΑΝΙΣΤ Α.Ε

Ενδιαφερόμενες ομάδες

- Άτομα που αγοράζουν το λογισμικό
- Προσωπικό

Δέσμευση διοίκησης και ηγεσίας

Η ηγεσία της εταιρείας Χ δεσμεύεται να διασφαλίσει ότι η ασφάλεια των πληροφοριών είναι ενσωματωμένη στον οργανισμό. Είναι υπεύθυνοι για τη διασφάλιση της τήρησης της πολιτικής και ότι:

- Οι πρακτικές ενσωματώνονται στον οργανισμό
- Διατίθενται πόροι
- Οι πληροφορίες μεταδίδονται αποτελεσματικά
- Τα επιδιωκόμενα αποτελέσματα επιτυγχάνονται
- Η ασφάλεια των πληροφοριών βελτιώνεται συνεχώς

Πολιτική

Πολιτική αξιολόγησης κινδύνου

Η πολιτική της ΧΑΝΙΣΤ Α.Ε σχετικά με τις εκτιμήσεις κινδύνου είναι, ότι όλα τα συστήματα πληροφοριών πρέπει να αξιολογούνται για κινδύνους μετά την εγκεκριμένη διαδικασία. Η εγκεκριμένη διαδικασία πρέπει:

- Να είναι τεκμηριωμένη
- Να είναι προβλεπόμενη για όλα τα συστήματα
- Συμπεριλάβετε μια αξιολόγηση επιχειρηματικού αντίκτυπου
- Συμπεριλάβετε μια εκτίμηση επιπτώσεων στο απόρρητο
- Συμπεριλάβετε τυχόν νομικές, κανονιστικές ή απαιτήσεις τρίτων
- Να επανεξετάζεται περιοδικά, συνήθως κάθε δύο χρόνια ή όταν υπάρχει σημαντική αλλαγή
- Να καθορίζει τα κριτήρια αποδοχής κινδύνου
- Να καθορίζει τα κριτήρια για τις αξιολογήσεις κινδύνου
- Να Βεβαιωθεί ότι τα αποτελέσματα των αξιολογήσεων είναι συνεπή
- Να προσδιορίσει τους κινδύνους
- Να αξιολογήσει την πιθανότητα κινδύνου
- Να αξιολογήσει το αντίκτυπο
- Να Προσδιορίσει ένα σχέδιο ανάκαμψης κινδύνου

Πολιτική Ανοχής Κινδύνου

Η ΧΑΝΙΣΤ Α.Ε έχει μέτρια ανοχή για ρίσκο.

Πολιτική Οργανισμού Ασφάλειας Πληροφοριών

Η πολιτική του ΧΑΝΙΣΤ Α.Ε για την οργάνωση της ασφάλειας είναι ότι πρέπει να επιβάλλονται οι αρχές των ελάχιστων προνομίων και του διαχωρισμού των καθηκόντων. Πρέπει να υπάρχει επαφή με αρχές και οργανισμούς ειδικών συμφερόντων όπου αυτό είναι σημαντικό και εφικτό, η ασφάλεια των πληροφοριών πρέπει να αντιμετωπίζεται σε όλα τα έργα.

Πολιτική φορητών συσκευών

Η πολιτική για φορητές συσκευές ΧΑΝΙΣΤ Α.Ε είναι ότι όλες οι πολιτικές ισχύουν για όλες τις συσκευές, συμπεριλαμβανομένων των φορητών συσκευών.

Πολιτική τηλεργασίας

Η πολιτική τηλεργασίας ΧΑΝΙΣΤ Α.Ε είναι ότι όλες οι πολιτικές ισχύουν για όλες τις τοποθεσίες όπου υποβάλλονται σε επεξεργασία πληροφορίες, συμπεριλαμβανομένων των τοποθεσιών τηλεργασίας.

Πολιτική Ασφάλειας Ανθρώπινου Δυναμικού

Η πολιτική ασφαλείας της ΧΑΝΙΣΤ Α.Ε για το ανθρώπινο δυναμικό(Human Resource ή HR) είναι ότι όλο το προσωπικό ελέγχεται κατάλληλα σύμφωνα με την τοπική νομοθεσία. Η ΧΑΝΙΣΤ Α.Ε αναγνωρίζει ότι ενδέχεται να απαιτούνται έλεγχοι προσωπικού ιστορικού για την επιβεβαίωση της καταλληλότητας για εργασία στα όρια μιας συγκεκριμένης δικαιοδοσίας και ότι οι παρελθοντικές συμπεριφορές μπορεί να μην είναι σχετικές. Όλες οι συμβάσεις εργασίας πρέπει να περιλαμβάνουν την απαίτηση του προσωπικού να συμμορφώνεται με όλες τις πολιτικές, συμπεριλαμβανομένων των πολιτικών ασφάλειας πληροφοριών.
Η διοίκηση πρέπει να διασφαλίσει ότι το προσωπικό εφαρμόζει όλες τις πολιτικές και ότι αναφέρονται όλες οι παραβιάσεις της ασφάλειας των πληροφοριών.
Κατά την αποχώρηση από την εργασία, η διοίκηση πρέπει να διασφαλίσει ότι τα αναγνωριστικά χρηστών αναστέλλονται και ότι όλα τα εταιρικά δεδομένα επιστρέφονται στην εταιρεία.

Πολιτική διαχείρισης περιουσιακών στοιχείων

Όλα τα πληροφοριακά συστήματα πρέπει να ταυτοποιούνται και να καταγράφονται με τα στοιχεία του ιδιοκτήτη. Ο προεπιλεγμένος κάτοχος για όλα τα συστήματα πληροφορικής είναι το τμήμα πληροφορικής. Τα περιουσιακά στοιχεία πρέπει να καταγράφονται στο κατάλληλο επίπεδο αφαίρεσης, αυτό είναι συνήθως το σύστημα ή η επιχείρηση ή το σύνολο περιουσιακών στοιχείων.

Παράδειγμα:

- Περιουσιακό στοιχείο 1. Σύστημα μισθοδοσίας γνωστό ως "ΧΑΝΙΣΤ Α.Ε Payroll"
- Περιουσιακό στοιχείο 2. Ιστότοπος στο Διαδίκτυο γνωστός ως "Ιστότοπος ΧΑΝΙΣΤ Α.Ε" με διεύθυνσηhttp://Medical-Appointment.com
- Στοιχείο 3. Όλοι οι επιτραπέζιοι υπολογιστές
- Περιουσιακό στοιχείο 4. Όλοι οι διακομιστές
- Περιουσιακό στοιχείο 5. Όλοι οι Servers
- Περιουσιακό στοιχείο 6. Προσωπικό

Πολιτική διάθεσης περιουσιακών στοιχείων

Η πολιτική διάθεσης περιουσιακών στοιχείων της ΧΑΝΙΣΤ Α.Ε είναι ότι χρησιμοποιείται μια κατάλληλη μέθοδος καταστροφής δεδομένων. Τα χάρτινα έγγραφα θα πρέπει να τεμαχίζονται εάν αυτό είναι δυνατό. Όπου δεν υπάρχουν εγκαταστάσεις για τον τεμαχισμό εμπιστευτικών εγγράφων, τότε αυτά πρέπει να σχιστούν με το χέρι σε τουλάχιστον τέσσερα κομμάτια. Τα μαγνητικά μέσα πρέπει να διαγράφονται με χρήση αντικατάστασης. Μπορούν να

χρησιμοποιηθούν δωρεάν εργαλεία και εργαλεία ανοιχτού κώδικα. Μπορούν να χρησιμοποιηθούν και άλλες μέθοδοι όπως η απομάκρυνση και η φυσική καταστροφή.

Πολιτική ταξινόμησης πληροφοριών

Η πολιτική ταξινόμησης πληροφοριών της ΧΑΝΙΣΤ Α.Ε είναι ότι όλα τα έγγραφα ταξινομούνται αυτόματα μόνο ως εσωτερική χρήση. Όπου τα έγγραφα προορίζονται για δημόσια χρήση, ο κάτοχος του εγγράφου δεν χρειάζεται να εφαρμόζει πρόσθετους ελέγχους. Ο κάτοχος του εγγράφου δεν χρειάζεται να επισημαίνει έγγραφα, ωστόσο, εάν το επιλέξει, τότε τα έγγραφα θα πρέπει να φέρουν την ετικέτα "Μόνο εσωτερική χρήση".

Ταξινόμηση	**Επιγραφή**
Μόνο για εσωτερική χρήση	Δεν είναι υποχρεωτικό, χρησιμοποιήστε μόνο εσωτερική χρήση
Δημόσιο	Κανένας

Πολιτική ελέγχου πρόσβασης

Η πολιτική ελέγχου πρόσβασης της ΧΑΝΙΣΤ Α.Ε είναι ότι το προσωπικό και τα τρίτα μέρη πρέπει να έχουν πρόσβαση μόνο σε συστήματα που βασίζονται στις αρχές του ελάχιστου προνομίου και πρέπει να γνωρίζουν. Όλη η πρόσβαση πρέπει να γίνεται μέσω μοναδικού αναγνωριστικού χρήστη που δεν είναι κοινόχρηστο με άλλους χρήστες. Όλοι οι λογαριασμοί πρόσβασης πρέπει να αναστέλλονται όταν το προσωπικό αποχωρεί ή όταν κάποιος τρίτος δεν απαιτεί πρόσβαση.

Κρυπτογραφική Πολιτική

Η πολιτική κρυπτογράφησης της ΧΑΝΙΣΤ Α.Ε είναι ότι χρησιμοποιείται κατάλληλη κρυπτογράφηση για την προστασία των περιουσιακών στοιχείων. Οι έλεγχοι πρέπει να χρησιμοποιούνται σε συμμόρφωση με τη νομοθεσία και την αδειοδότηση λογισμικού.

Πολιτική διαχείρισης κλειδιών

Η πολιτική διαχείρισης κρυπτογραφικού κλειδιού της ΧΑΝΙΣΤ Α.Ε είναι ότι υπάρχουν κατάλληλα στοιχεία ελέγχου για την προστασία των κρυπτογραφικών κλειδιών.

Πολιτική Φυσικής Ασφάλειας

Η πολιτική φυσικής ασφάλειας της ΧΑΝΙΣΤ Α.Ε είναι ότι οι τοποθεσίες στις οποίες γίνεται επεξεργασία πληροφοριών πρέπει να είναι προσβάσιμες μόνο σε εξουσιοδοτημένα άτομα. Το προσωπικό και οι επισκέπτες πρέπει να ελέγχονται. Η φυσική τοποθεσία των τοποθεσιών πρέπει

να λαμβάνει υπόψη τις περιβαλλοντικές απειλές. Ο εξοπλισμός δεν πρέπει να αφαιρείται εκτός των γραφείων εκτός εάν είναι επαγγελματική ανάγκη.

Πολιτική Ασφάλειας Επιχειρήσεων

Η πολιτική ασφάλειας λειτουργιών της ΧΑΝΙΣΤ Α.Ε είναι ότι η ασφάλεια πληροφοριών πρέπει να περιλαμβάνεται στις επιχειρηματικές δραστηριότητες. Οι διαδικασίες λειτουργίας πρέπει να είναι διαθέσιμες σε όλο το προσωπικό που χρειάζεται να έχει πρόσβαση σε αυτές. Τα συστήματα ανάπτυξης, δοκιμής και λειτουργίας πρέπει να διαχωριστούν. Οι έλεγχοι πρέπει να σχεδιάζονται για να ελαχιστοποιούνται οι διαταραχές.

Πολιτική προστασίας από κακόβουλο λογισμικό

Η πολιτική προστασίας της ΧΑΝΙΣΤ Α.Ε από κακόβουλο λογισμικό είναι ότι όλοι οι σταθμοί εργασίας και οι διακομιστές πρέπει να διαθέτουν κατάλληλο anti-malware. Εξαιρέσεις θα γίνονται όταν το anti-malware προκαλεί επιχειρησιακά ζητήματα της επιχείρησης ή όπου απαιτούνται συγκεκριμένοι σταθμοί εργασίας και δίκτυα για να μην έχουν τέτοιους ελέγχους. Σε αυτή την περίπτωση θα πρέπει να ληφθούν υπόψη αντισταθμιστικοί έλεγχοι ασφαλείας.

Πολιτική δημιουργίας αντιγράφων ασφαλείας

Η πολιτική δημιουργίας αντιγράφων ασφαλείας της ΧΑΝΙΣΤ Α.Ε είναι ότι πρέπει να λαμβάνονται αντίγραφα ασφαλείας των δεδομένων.

Πολιτική καταγραφής και παρακολούθησης

Η πολιτική καταγραφής της ΧΑΝΙΣΤ Α.Ε είναι ότι όλα τα συστήματα πρέπει να δημιουργούν αρχεία καταγραφής όπως επιτρέπεται από το σύστημα πληροφορικής. Τα αρχεία καταγραφής θα πρέπει να διατηρούνται για τουλάχιστον έξι μήνες όπου αυτό είναι δυνατό. Τα ρολόγια του συστήματος θα πρέπει να συγχρονίζονται όπου αυτό είναι δυνατό. Η προνομιακή πρόσβαση χρήστη θα πρέπει να καταγράφεται, εάν είναι δυνατόν αυτό το αρχείο καταγραφής θα πρέπει να είναι αμετάβλητο.

Πολιτική ελέγχου λειτουργικού λογισμικού

Η πολιτική ελέγχου του λειτουργικού λογισμικού της ΧΑΝΙΣΤ Α.Ε είναι ότι οι χρήστες δεν πρέπει να εγκαθιστούν απαγορευμένο λογισμικό.

Πολιτική πρόσβασης τρίτων

Η πολιτική πρόσβασης τρίτων του της ΧΑΝΙΣΤ Α.Ε είναι ότι οι πολιτικές ασφάλειας πληροφοριών ισχύουν για τρίτα μέρη. Η απομακρυσμένη πρόσβαση τρίτων πρέπει να αξιολογείται ως προς τον κίνδυνο και η πρόσβαση πρέπει να εφαρμόζεται με το λιγότερο προνόμιο και την ανάγκη να γνώσης ότι επιβάλλονται οι παραπάνω αρχές. Η απομακρυσμένη πρόσβαση θα πρέπει να είναι απενεργοποιημένη από προεπιλογή και να ενεργοποιείται υπό τον έλεγχο αλλαγής.

Πολιτική μεταφοράς πληροφοριών

Η πολιτική μεταφοράς πληροφοριών της ΧΑΝΙΣΤ Α.Ε είναι ότι συμφωνίες, όπως συμβάσεις, πρέπει να ισχύουν όταν τα δεδομένα μεταφέρονται εκτός ΧΑΝΙΣΤ Α.Ε.

Πολιτική Απόκτησης, Ανάπτυξης και Συντήρησης Συστημάτων

Η πολιτική απόκτησης, ανάπτυξης και συντήρησης συστημάτων της ΧΑΝΙΣΤ Α.Ε είναι:

- Οι απαιτήσεις για νέα συστήματα πληροφορικής πρέπει να περιλαμβάνουν απαιτήσεις ασφάλειας πληροφοριών.
- Όλο το λογισμικό που αναπτύσσεται από την ΧΑΝΙΣΤ Α.Ε ή τρίτα μέρη πρέπει να ακολουθεί έναν ασφαλή κύκλο ζωής ανάπτυξης λογισμικού.
- Τα συστήματα πρέπει να σχεδιάζονται σύμφωνα με αρχές ασφαλούς μηχανικής.
- Οι αλλαγές στα συστήματα πρέπει να ελέγχονται μετά τον έλεγχο των αλλαγών.
- Τα δεδομένα δοκιμής πρέπει να επιλέγονται προσεκτικά και να προστατεύονται.
- Τα συστήματα πρέπει να επιδιορθώνονται, ύστερα από εντοπισμό κάποιας βλάβης.

Πολιτική διαχείρισης περιστατικών ασφάλειας πληροφοριών

Η πολιτική διαχείρισης συμβάντων ασφάλειας πληροφοριών της ΧΑΝΙΣΤ Α.Ε είναι ότι:

- Όλα τα συμβάντα, συμπεριλαμβανομένων των πραγματικών και των ύποπτων συμβάντων, πρέπει να αναφέρονται στη διοίκηση.
- Για πραγματικά περιστατικά, θα πρέπει να καθοριστεί η βασική αιτία και να συνιστώνται και να εφαρμόζονται διορθωτικοί έλεγχοι όπου είναι δυνατόν.

Πολιτική επιχειρησιακής συνέχειας ασφάλειας πληροφοριών

Η πολιτική επιχειρησιακής συνέχειας ασφάλειας πληροφοριών της ΧΑΝΙΣΤ Α.Ε είναι ότι η πολιτική ασφάλειας πληροφοριών εφαρμόζεται σε περίπτωση συμβάντος επιχειρηματικής συνέχειας. Οι διαδικασίες επιχειρησιακής συνέχειας θα πρέπει να λαμβάνουν υπόψη την ασφάλεια των δεδομένων.

Πολιτική Συμμόρφωσης

Η πολιτική συμμόρφωσης ΧΑΝΙΣΤ Α.Ε είναι:

- Πρέπει να πληρούνται όλες οι σχετικές νομικές απαιτήσεις.
- Τα αρχεία πρέπει να προστατεύονται από απώλεια.
- Η προσέγγιση στη διαχείριση της ασφάλειας των πληροφοριών πρέπει να επανεξετάζεται περιοδικά.
- Τα αρχεία πρέπει να διατηρούνται για την περίοδο που απαιτείται από τη νομοθεσία ή τις επιχειρησιακές απαιτήσεις.

Πολιτική απαιτήσεων από τον χρήστη

Η πολιτική απαιτήσεων από τον χρήστη, για την εφαρμογή, της ΧΑΝΙΣΤ Α.Ε είναι:

- Ο χρήστης οφείλει να καταχωρεί όνομα χρήστη το οποίο αποτελείται μονάχα από αγγλικούς χαρακτήρες και νούμερα (12 χαρακτήρες ή νούμερα).
- Ο χρήστης οφείλει να καταχωρεί όνομα και επώνυμο τα οποία αποτελούνται μονάχα από χαρακτήρες.
- Ο χρήστης οφείλει να χρησιμοποιεί τις συναρτήσεις κρυπτογράφησης, που προσφέρονται, και να μην αποθηκεύει ‘’plain-text’’ στη βάση δεδομένων του συστήματος.