Τέρμα Καραμέλα & Φράγμα Μυός, 57001, Αθήνα,
Τηλ.: +30 2310 272462
Ηλεκτρονικό ταχυδρομείο: info@digas.gr

ΠΟΛΙΤΙΚΗ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

1 Πολιτική ISMS

1.1 Απαιτήσεις ασφάλειας πληροφοριών

Θα συμφωνηθεί και θα διατηρηθεί με την επιχείρηση σαφής ορισμός των απαιτήσεων για την ασφάλεια των πληροφοριών, έτσι ώστε όλες οι δραστηριότητες ΣΔΑΠ να επικεντρώνονται στην εκπλήρωση αυτών των απαιτήσεων. Οι κανονιστικές, κανονιστικές και συμβατικές απαιτήσεις θα τεκμηριώνονται επίσης και θα συμβάλλουν στη διαδικασία σχεδιασμού. Ειδικές απαιτήσεις όσον αφορά την ασφάλεια νέων ή τροποποιημένων συστημάτων ή υπηρεσιών θα αποτυπώνονται στο πλαίσιο της φάσης σχεδιασμού κάθε έργου.

Είναι μια θεμελιώδης αρχή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ότι οι έλεγχοι που εφαρμόζονται καθοδηγούνται από τις επιχειρηματικές ανάγκες και αυτό θα κοινοποιείται τακτικά σε όλο το προσωπικό μέσω συνεδριάσεων της ομάδας και ενημερωτικών εγγράφων.

1.2 Κορυφαία ηγετική θέση και αφοσίωση στη διοίκηση

Η δέσμευση για την ασφάλεια των πληροφοριών επεκτείνεται σε ανώτερα επίπεδα του οργανισμού και θα αποδειχθεί μέσω αυτής της πολιτικής ΣΔΑΠ και της παροχής των κατάλληλων πόρων για την παροχή και την ανάπτυξη του ΣΔΑΠ και των σχετικών ελέγχων.

Η ανώτατη διοίκηση θα εξασφαλίσει επίσης ότι θα διεξάγεται σε τακτική βάση συστηματική ανασκόπηση των επιδόσεων του προγράμματος, ώστε να διασφαλίζεται ότι επιτυγχάνονται οι ποιοτικοί στόχοι και ότι εντοπίζονται τα σχετικά ζητήματα μέσω του προγράμματος ελέγχου και των διαδικασιών διαχείρισης. Ο έλεγχος της διαχείρισης μπορεί να λάβει διάφορες μορφές, συμπεριλαμβανομένων των συνεδριάσεων του τμήματος και άλλων συνεδριάσεων της διοίκησης.

Ο διαχειριστής ασφάλειας πληροφοριών έχει γενική εξουσία και ευθύνη για την εφαρμογή και τη διαχείριση του συστήματος διαχείρισης ασφάλειας πληροφοριών, και συγκεκριμένα:

- Τον προσδιορισμό, την τεκμηρίωση και την εκπλήρωση των απαιτήσεων ασφάλειας πληροφοριών
- Εφαρμογή, διαχείριση και βελτίωση των διαδικασιών διαχείρισης κινδύνου
- Ολοκλήρωση επιχειρησιακών διαδικασιών, διαδικασιών και ελέγχων
- Συμμόρφωση με τις κανονιστικές, κανονιστικές και συμβατικές απαιτήσεις
- Αναφορά στην ανώτατη διοίκηση σχετικά με την απόδοση και τη βελτίωση

1.3 Πλαίσιο για τον καθορισμό των στόχων

Θα χρησιμοποιηθεί τακτικός κύκλος για τον καθορισμό στόχων για την ασφάλεια των πληροφοριών, ο οποίος θα συμπίπτει με τον κύκλο προγραμματισμού του προϋπολογισμού. Με τον τρόπο αυτό εξασφαλίζεται η επαρκής χρηματοδότηση των

Τέρμα Καραμέλα & Φράγμα Μυός, 57001, Αθήνα,
Τηλ.: +30 2310 272462
Ηλεκτρονικό ταχυδρομείο: info@digas.gr

ΠΟΛΙΤΙΚΗ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

δραστηριοτήτων βελτίωσης που εντοπίζονται. Οι στόχοι αυτοί θα βασίζονται σε μια σαφή κατανόηση των επιχειρηματικών απαιτήσεων, η οποία θα ενημερώνεται από τη διαδικασία επανεξέτασης της διοίκησης κατά την οποία μπορούν να ληφθούν οι απόψεις των σχετικών ενδιαφερόμενων μερών.

Οι στόχοι ΣΔΜ θα τεκμηριώνονται για συμφωνημένο χρονικό διάστημα, μαζί με λεπτομέρειες για τον τρόπο επίτευξής τους. Οι αξιολογήσεις και η παρακολούθησή τους θα γίνονται στο πλαίσιο των ανασκοπήσεων της διαχείρισης, ώστε να διασφαλίζεται ότι εξακολουθούν να ισχύουν. Αν απαιτούνται τροποποιήσεις, αυτές θα διαχειρίζονται μέσω της διαδικασίας διαχείρισης αλλαγών.

Σύμφωνα με το πρότυπο ISO/IEC 27001:2013, οι έλεγχοι αναφοράς που περιγράφονται λεπτομερώς στο παράρτημα Α του προτύπου θα εγκριθούν, κατά περίπτωση, από την Digas g. Οι εν λόγω αξιολογήσεις θα επανεξετάζονται σε τακτική βάση με βάση τα αποτελέσματα των αξιολογήσεων κινδύνου και σύμφωνα με τα σχέδια αντιμετώπισης κινδύνων ασφάλειας πληροφοριών. Για λεπτομέρειες σχετικά με τους ελέγχους του παραρτήματος Α που έχουν τεθεί σε εφαρμογή και οι οποίοι έχουν εξαιρεθεί, βλ. δήλωση εφαρμογής.

1.4 Ρόλοι και ευθύνες

Στον τομέα της ασφάλειας των πληροφοριών, υπάρχουν διάφοροι ρόλοι διαχείρισης που αντιστοιχούν στους τομείς που ορίζονται στο πεδίο εφαρμογής που αναφέρεται παραπάνω. Σε έναν μεγαλύτερο οργανισμό, αυτοί οι ρόλοι συχνά θα καλυφθούν από ένα άτομο σε κάθε περιοχή. Σε έναν μικρότερο οργανισμό αυτοί οι ρόλοι και οι ευθύνες πρέπει να κατανέμονται μεταξύ των μελών της ομάδας.

Πλήρεις λεπτομέρειες των αρμοδιοτήτων που σχετίζονται με κάθε έναν από τους ρόλους και τον τρόπο με τον οποίο κατανέμονται στο πλαίσιο του Digas g. δίνονται σε ξεχωριστό έγγραφο Ρόλοι ασφάλειας πληροφοριών, Αρμοδιότητες και Αρχές.

Είναι ευθύνη του Υπεύθυνου Ασφάλειας Πληροφοριών να διασφαλίζει ότι οι εργαζόμενοι και οι εργολάβοι κατανοούν τους ρόλους που εκπληρώνουν και ότι διαθέτουν τις κατάλληλες δεξιότητες και ικανότητες για να το πράξουν.

1.5 Συνεχής βελτίωση των ΣΔΑΠ

Digas g. πολιτική όσον αφορά τη συνεχή βελτίωση είναι:

- Συνεχής βελτίωση της αποτελεσματικότητας των ΣΔΑΠ
- Ενίσχυση των τρεχουσών διεργασιών ώστε να ευθυγραμμιστούν με την ορθή πρακτική όπως ορίζεται στο ISO/IEC 27001
- Επίτευξη της πιστοποίησης ISO/IEC 27001 και διατήρησή της σε συνεχή βάση
- Αύξηση του επιπέδου της προορατικότητας (και της αντίληψης των ενδιαφερόμενων μερών για την προορατικότητα) όσον αφορά την ασφάλεια των πληροφοριών
- Να καταστούν οι διαδικασίες και οι έλεγχοι ασφάλειας πληροφοριών πιο μετρήσιμοι προκειμένου να παρέχουν μια υγιή βάση για τεκμηριωμένες αποφάσεις

Τέρμα Καραμέλα & Φράγμα Μυός, 57001, Αθήνα,
Τηλ.: +30 2310 272462
Ηλεκτρονικό ταχυδρομείο: info@digas.gr

ΠΟΛΙΤΙΚΗ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

- Επανεξετάζει τις σχετικές μετρήσεις σε ετήσια βάση για να εκτιμήσει αν είναι σκόπιμο να τις αλλάξει, με βάση τα συλλεγόμενα ιστορικά δεδομένα
- Αποκτήστε ιδέες για βελτίωση μέσω τακτικών συναντήσεων με τα ενδιαφερόμενα μέρη και τεκμηριώστε τις σε ένα συνεχές σχέδιο βελτίωσης
- Να επανεξετάζει το σχέδιο συνεχούς βελτίωσης σε τακτικές συνεδριάσεις διαχείρισης, προκειμένου να δίνει προτεραιότητα και να αξιολογεί τα χρονοδιαγράμματα και τα οφέλη

Ιδέες για βελτιώσεις μπορούν να ληφθούν από οποιαδήποτε πηγή, συμπεριλαμβανομένων των υπαλλήλων, των πελατών, των προμηθευτών, του προσωπικού τεχνολογίας πληροφορικής, των αξιολογήσεων κινδύνου και των αναφορών εξυπηρέτησης. Μόλις προσδιοριστούν, θα προστεθούν στο σχέδιο συνεχούς βελτίωσης και θα αξιολογηθούν από τον υπάλληλο που είναι υπεύθυνος για τη συνεχή βελτίωση των υπηρεσιών.

Στο πλαίσιο της αξιολόγησης των προτεινόμενων βελτιώσεων, θα χρησιμοποιηθούν τα ακόλουθα κριτήρια:

- Κόστος
- Επιχειρηματικό όφελος
- Κίνδυνος
- Χρονική κλίμακα υλοποίησης
- Απαίτηση πόρου

Αν γίνει δεκτή, η πρόταση βελτίωσης θα έχει προτεραιότητα, προκειμένου να επιτραπεί πιο αποτελεσματικός σχεδιασμός.

1.6 Προσέγγιση στη Διαχείριση Κινδύνων

Η διαχείριση των κινδύνων θα πραγματοποιηθεί σε διάφορα επίπεδα στο πλαίσιο του ΣΔΑΠ, μεταξύ των οποίων:

- Διαχειριστικός σχεδιασμός - οι κίνδυνοι για την επίτευξη των στόχων της ασφάλειας των πληροφοριών θα αξιολογούνται και θα επανεξετάζονται σε τακτική βάση
- Αξιολογήσεις κινδύνου ασφάλειας πληροφοριών και συνέχισης υπηρεσιών ΤΠ
- Αξιολόγηση του κινδύνου αλλαγών μέσω της διαδικασίας διαχείρισης αλλαγών
- Ως μέρος των μεγάλων έργων για την επίτευξη επιχειρηματικής αλλαγής, π.χ. νέα συστήματα υπολογιστών

Οι αξιολογήσεις υψηλού επιπέδου κινδύνου θα επανεξετάζονται σε ετήσια βάση ή μετά από σημαντική αλλαγή στην παροχή επιχειρήσεων ή υπηρεσιών.

Θα χρησιμοποιηθεί διαδικασία αξιολόγησης κινδύνου που συνάδει με τις απαιτήσεις και τις συστάσεις του ISO/IEC 27001, του διεθνούς προτύπου για την ασφάλεια των πληροφοριών. Αυτό τεκμηριώνεται στην Αξιολόγηση Κινδύνου και στη Διαδικασία Θεραπείας.

Τέρμα Καραμέλα & Φράγμα Μυός, 57001, Αθήνα,
Τηλ.: +30 2310 272462
Ηλεκτρονικό ταχυδρομείο: info@digas.gr

ΠΟΛΙΤΙΚΗ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Από την ανάλυση αυτή, θα συνταχθεί έκθεση εκτίμησης κινδύνου ακολουθούμενη από σχέδιο αντιμετώπισης κινδύνου στο οποίο θα επιλέγονται οι κατάλληλοι έλεγχοι από τον κατάλογο αναφοράς του παραρτήματος Α του προτύπου ISO/IEC 27001, μαζί με τυχόν πρόσθετους ελέγχους που κρίνονται αναγκαίοι.

1.7 Ανθρώπινο δυναμικό

Το Digas g. θα εξασφαλίσει ότι όλο το προσωπικό που ασχολείται με την ασφάλεια των πληροφοριών είναι ικανό με βάση την κατάλληλη εκπαίδευση, κατάρτιση, δεξιότητες και εμπειρία.

Οι δεξιότητες που απαιτούνται θα καθορίζονται και θα αναθεωρούνται σε τακτική βάση, μαζί με μια αξιολόγηση των υφιστάμενων επιπέδων δεξιοτήτων εντός του Digas g. Θα προσδιοριστούν οι ανάγκες κατάρτισης και θα διατηρηθεί ένα σχέδιο για να εξασφαλιστεί ότι υπάρχουν οι απαραίτητες ικανότητες.

Η κατάρτιση, η εκπαίδευση και άλλα σχετικά αρχεία θα τηρούνται από το Τμήμα Ανθρώπινου Δυναμικού για την τεκμηρίωση των ατομικών επιπέδων δεξιοτήτων που επιτυγχάνονται.

1.8 Έλεγχος και αναθεώρηση

Μόλις τεθεί σε εφαρμογή, είναι ζωτικής σημασίας να πραγματοποιούνται τακτικές ανασκοπήσεις σχετικά με το πόσο καλά τηρούνται οι διαδικασίες και οι διαδικασίες ασφάλειας των πληροφοριών. Αυτό θα συμβεί σε τρία επίπεδα:

1. Δομημένη τακτική επανεξέταση της συμμόρφωσης της διαχείρισης με πολιτικές και διαδικασίες
2. Ανασκοπήσεις εσωτερικού ελέγχου σε σχέση με το πρότυπο ISO/IEC 27001 από την ομάδα ποιότητας Digas.
3. Εξωτερικός έλεγχος βάσει του προτύπου από εγγεγραμμένο φορέα πιστοποίησης (RCB) με σκοπό την απόκτηση και διατήρηση πιστοποίησης

Λεπτομέρειες σχετικά με τον τρόπο διενέργειας των εσωτερικών ελέγχων περιλαμβάνονται στη διαδικασία για τους ελέγχους ΣΔΜ.

1.9 Δομή και πολιτική τεκμηρίωσης

Όλες οι πολιτικές και τα σχέδια ασφάλειας πληροφοριών πρέπει να τεκμηριώνονται. Λεπτομέρειες σχετικά με τις συμβάσεις και τα πρότυπα τεκμηρίωσης παρέχονται στη διαδικασία ελέγχου των τεκμηριωμένων πληροφοριών.

Ορισμένα βασικά έγγραφα θα διατηρηθούν ως μέρος του ΣΔΑΠ. Είναι μοναδικά αριθμημένες και οι τρέχουσες εκδόσεις παρακολουθούνται στο αρχείο καταγραφής τεκμηρίωσης ISMS.

1.10 Έλεγχος εγγραφών

Η τήρηση αρχείων αποτελεί θεμελιώδες μέρος του ΣΔΑΠ. Τα αρχεία είναι βασικοί πόροι πληροφοριών και αποτελούν απόδειξη ότι οι διαδικασίες διεξάγονται αποτελεσματικά.

Τέρμα Καραμέλα & Φράγμα Μυός, 57001, Αθήνα,
Τηλ.: +30 2310 272462
Ηλεκτρονικό ταχυδρομείο: info@digas.gr

ΠΟΛΙΤΙΚΗ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Οι έλεγχοι που εφαρμόζονται για τη διαχείριση εγγραφών ορίζονται στη Διαδικασία Ελέγχου Τεκμηριωμένων Πληροφοριών του εγγράφου.