Σύστημα Προστασίας Προσωπικών Δεδομένων και Συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Θεσσαλονίκη | 18.11.2024

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. Σκοπός και αποδέκτες εγγράφου.

Σκοπός του παρόντος εγγράφου είναι ο καθορισμός του πεδίου εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ/ΠΔ) της ανώνυμης εταιρείας με την επωνυμία «EPSILON NET – Ανώνυμη Εταιρεία Πληροφορικής, Εκπαίδευσης και Προϊόντων Υψηλής Τεχνολογίας» και τον διακριτικό τίτλο «EPSILON NET A.E.» (εφεξής «EPSILON NET») και η περιγραφή των γενικών αρχών, στόχων και κατευθύνσεων για την ασφάλεια των πληροφοριών της.

Αποδέκτες του παρόντος εγγράφου είναι η Διοίκηση, το ανθρώπινο δυναμικό και οι συνεργάτες της εταιρείας που σχετίζονται με τους πληροφοριακούς πόρους της εταιρείας που εντάσσονται στο πεδίο εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

2. Σύντομη περιγραφή της Epsilon Net.

Η EPSILON NET δραστηριοποιείται στους τομείς της πληροφορικής, της ανάπτυξης ψηφιακού περιεχομένου και της εκπαίδευσης. Επενδύει σε τεχνολογίες αιχμής και ακολουθεί με συνέπεια το δρόμο της συνεχούς ανάπτυξης, ενισχύοντας το μοντέλο των κινήσεων συνεργασίας στη βάση της τεχνολογικής σύμπραξης.

Η EPSILON NET δεν πραγματοποιεί καμία διάκριση σε βάρος οποιουδήποτε προσώπου με βάση τη φυλή, το χρώμα, την εθνική ή εθνοτική καταγωγή, τον σεξουαλικό προσανατολισμό, την αναπηρία, την ηλικία ή οποιοδήποτε άλλο χαρακτηριστικό, και εφαρμόζει τον νόμο 4443/2016.

Η EPSILON NET εδρεύει στην Πυλαία Θεσσαλονίκης (Πάροδος 17ης Νοέμβρη 87, Ζώνη ΕΜΟ, Τ.Κ. 55534), σε ένα σύγχρονο κτίριο, με όλες τις προδιαγραφές που προβλέπονται από τον Ν.Ο.Κ. και με σύστημα πυροπροστασίας.

3. Ενδιαφερόμενα μέρη.

Η EPSILON NET αναγνωρίζει τα κάτωθι ενδιαφερόμενα μέρη, καθώς και τις σχετικές ανάγκες και προσδοκίες τους όσον αφορά στο Σύστημα Διαχείρισης Ασφάλειας των Πληροφοριών της.

Ενδιαφερόμενα μέρη (Interested parties)	**Ανάγκες και προσδοκίες (Needs and expectations)**
Μέτοχοι και Διοίκηση της εταιρείας	• Καλή εξωτερική εικόνα της εταιρείας / Φήμη • Ανταγωνιστικό πλεονέκτημα • Κέρδη
Εργαζόμενοι και Εξωτερικοί συνεργάτες	• Εμπιστοσύνη σχετικά με τον ασφαλή χειρισμό των προσωπικών πληροφοριών τους στις σχέσεις τους με την εταιρεία

	• Δυνατότητα εξέλιξης της επαγγελματικής τους σταδιοδρομίας • Δυνατότητα λήψης πρωτοβουλιών
Πελάτες	• Εμπιστοσύνη σχετικά με τον ασφαλή χειρισμό των πληροφοριών τους στις σχέσεις τους με την εταιρεία • Αίσθηση ότι διασφαλίζουν συνεργασία με μια εταιρεία που έχει ανταγωνιστικό πλεονέκτημα • Παροχή υπηρεσιών υψηλών προδιαγραφών • Ικανοποίηση των αναγκών τους
Προμηθευτές	• Επίτευξη αμοιβαίου οφέλους • Αίσθηση ότι διασφαλίζουν συνεργασία με μια εταιρεία που έχει ανταγωνιστικό πλεονέκτημα
Πολιτεία	• Συμμόρφωση με την ισχύουσα νομοθεσία (προσωπικά δεδομένα, απόρρητο επικοινωνιών, πνευματική ιδιοκτησία κλπ)

4. Πολιτική ασφάλειας πληροφοριών.

4.1 Δομή της πολιτικής ασφάλειας.

Η πολιτική ασφάλειας της EPSILON NET, η οποία συνοπτικά παρουσιάζεται στο Παράρτημα Α' του παρόντος εγγράφου, αποτελείται από (α) την παρούσα γενική πολιτική ασφάλειας, η οποία περιλαμβάνει τους στόχους της εταιρείας για την προστασία των πληροφοριών της, τη δέσμευση της Διοίκησης για την εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών / Προσωπικών Δεδομένων, καθώς και τις βασικές αρχές και πρόνοιες της πολιτικής ασφάλειας, και (β) μία σειρά επιμέρους πολιτικών ασφάλειας, στόχος των οποίων είναι ο καθορισμός λεπτομερών πολιτικών ασφάλειας σε διάφορα πεδία της ασφάλειας πληροφοριών.

Η εφαρμογή της πολιτικής ασφάλειας υποστηρίζεται από επιμέρους διαδικασίες και αρχεία, όπου απαιτείται.

Η παρούσα πολιτική ασφάλειας έχει εγκριθεί από τη Διοίκηση της EPSILON NET (A.5.1.1).

4.2 Στόχοι ασφάλειας πληροφοριών.

Ως Ασφάλεια της Πληροφορίας (Information Security) ορίζεται από τη διεθνή βιβλιογραφία η διασφάλιση των παρακάτω ιδιοτήτων:

- Εμπιστευτικότητα (Confidentiality): Διασφάλιση ότι πρόσβαση στην πληροφορία έχουν μόνο όσοι έχουν κατάλληλη εξουσιοδότηση.
- Ακεραιότητα (Integrity): Διασφάλιση ότι η πληροφορία είναι πλήρης, ακριβής και έγκυρη.
- Διαθεσιμότητα (Availability): Διασφάλιση ότι η πληροφορία είναι διαθέσιμη κάθε στιγμή που ένας εξουσιοδοτημένος χρήστης επιχειρεί να αποκτήσει πρόσβαση σε αυτή.

Πέραν των παραπάνω τριών βασικών στόχων ασφάλειας, ως συμπληρωματικοί στόχοι της ασφάλειας των πληροφοριών θεωρούνται:

- Ταυτοποίηση και αυθεντικοποίηση χρηστών: Διασφάλιση ότι ο χρήστης που επιχειρεί να αποκτήσει πρόσβαση σε πληροφορία / σύστημα / εφαρμογή είναι αυτός που ισχυρίζεται ότι είναι. Πρόκειται ουσιαστικά για τη διαδικασία εξακρίβωσης της ταυτότητας του χρήστη.
- Έλεγχος πρόσβασης: Διασφάλιση ότι ο χρήστης που επιχειρεί να αποκτήσει πρόσβαση σε πληροφορία / σύστημα / εφαρμογή είναι εξουσιοδοτημένος για αυτήν την ενέργεια.
- Έλεγχος και παρακολούθηση (audit & monitoring): Παρακολούθηση και καταγραφή των ενεργειών των χρηστών.
- Προστασία προσωπικών δεδομένων: Προστασία των δεδομένων προσωπικού χαρακτήρα από μη εξουσιοδοτημένη επεξεργασία, σύμφωνα με την κείμενη νομοθεσία.
- Μη αποποίηση ευθύνης: Διασφάλιση ότι ένας χρήστης δεν μπορεί να αρνηθεί ότι εκτέλεσε μία ενέργεια σχετική με πρόσβαση / επεξεργασία σε πληροφορία / σύστημα / εφαρμογή.

Η επίτευξη του συνόλου των παραπάνω στόχων ασφάλειας (βασικών και συμπληρωματικών) οδηγεί στη μέγιστη δυνατή προστασία της πληροφορίας, των συστημάτων και εφαρμογών.

4.3 Δέσμευση της Διοίκησης για την ασφάλεια των πληροφοριών.

Η Διοίκηση της EPSILON NET αναγνωρίζει πλήρως τους στόχους του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών / Προσωπικών Δεδομένων, υποστηρίζει την υλοποίηση αυτών σύμφωνα με την παρούσα πολιτική ασφάλειας και μεριμνά για τη συνεχή βελτίωση του Συστήματος.

Ειδικότερα, η Διοίκηση της εταιρείας είναι υπεύθυνη για:

- Τον καθορισμό των στρατηγικών στόχων της εταιρείας για την ασφάλεια των πληροφοριών της.
- Τον καθορισμό των ρόλων και αρμοδιοτήτων για τη διαχείριση της ασφάλειας των πληροφοριών.
- Τον καθορισμό του αποδεκτού επιπέδου επικινδυνότητας.

- Την έγκριση της πολιτικής ασφάλειας της εταιρείας και τυχόν αλλαγών σε αυτή.
- Την έγκριση των σχεδίων αντιμετώπισης των κινδύνων.
- Τη διάθεση των απαραίτητων πόρων (οικονομικών και ανθρώπινων) για την εφαρμογή, την παρακολούθηση της εφαρμογής και τη συνεχή βελτίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών της εταιρείας.
- Τη διάδοση και την αποδοχή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών από το σύνολο του προσωπικού και τους συνεργάτες της εταιρείας.
- Τη λήψη πειθαρχικών ή / και άλλων μέτρων σε περιπτώσεις μη συμμόρφωσης με όσα σαφώς ορίζονται στην Πολιτική Ασφάλειας της εταιρείας.

4.4 Γενική καθοδήγηση.

Τα πληροφοριακά συστήματα της εταιρείας παρέχονται για επαγγελματική χρήση. Η χρήση οποιουδήποτε συστήματος πληροφοριών της εταιρείας για προσωπικούς λόγους (συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου και του ιστού) επιτρέπεται μόνο σύμφωνα με τις οδηγίες αυτής της πολιτικής.

Η εταιρεία διατηρεί το δικαίωμα να παρακολουθεί κάθε πτυχή των πληροφοριακών συστημάτων της, προκειμένου να προστατεύει τα νόμιμα επιχειρηματικά της συμφέροντα. Οι πληροφορίες που συλλέγονται από την παρακολούθηση αυτή μπορούν να χρησιμοποιηούν για την εκκίνηση ή υποστήριξη πειθαρχικών διαδικασιών και ενεργειών ενώπιον των αρμόδιων δικαστηρίων.

Περιστατικά που σχετίζονται με την ασφάλεια πρέπει να αναφέρονται από το προσωπικό στον διευθυντή του εκάστοτε τμήματος ή στο γραφείο υπηρεσιών πληροφορικής (A.7.2.1).

Αυτή η Πολιτική περιλαμβάνει σε διάφορα σημεία τη φράση «άλλοι μπορεί να θεωρούν προσβλητικό». Με τη φράση αυτή εννοείται ιδίως υλικό πορνογραφικό ή σεξουαλικό, ρατσιστικό, σεξιστικό ή ομοφοβικό, και ακατάλληλο (όπως απεικόνιση τραυματισμού ή βία κατά ζώων).

4.5 Οργάνωση της ασφάλειας πληροφοριών.

Η EPSILON NET έχει καθορίσει τις οργανωτικές δομές και τους ρόλους όσων είναι υπεύθυνοι ή σχετίζονται με τη διαχείριση της ασφάλειας των πληροφοριών της. Μέσω των συγκεκριμένων δομών και ρόλων, η εταιρεία στοχεύει στην προστασία των πληροφοριών της από μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, αλλοίωση ή καταστροφή.

4.5.1 Εσωτερική οργάνωση της εταιρείας για την ασφάλεια.

Η οργάνωση της εταιρείας για την ασφάλεια των πληροφοριών έχει επικοινωνηθεί από τη Διοίκηση της εταιρείας στο προσωπικό και στους συνεργάτες της εταιρείας, και περιλαμβάνει τους παρακάτω ρόλους:

i. Διοίκηση.

Στα τυπικά καθήκοντα της Διοίκησης της εταιρείας όσον αφορά στην ασφάλεια των πληροφοριών εμπίπτουν:

- Ο έλεγχος και η έγκριση της πολιτικής ασφάλειας, τόσο της αρχικής έκδοσης όσο και κάθε αναθεώρησης αυτής.
- Ο έλεγχος και η έγκριση των ρόλων και αρμοδιοτήτων σχετικά με τη διαχείριση του ΣΔΑΠ/ΠΔ.
- Η παρακολούθηση σημαντικών αλλαγών στην οργάνωση ή τις υποδομές της εταιρείας που δημιουργούν την ανάγκη αναθεώρησης του ΣΔΑΠ/ΠΔ.
- Η παρακολούθηση συμβάντων που σχετίζονται με την ασφάλεια.
- Η ανάληψη πρωτοβουλιών για την ενίσχυση της ασφάλειας των πληροφοριακών πόρων της εταιρείας με την υιοθέτηση πρόσθετων μέτρων.

ii. Υπεύθυνος Ασφάλειας Πληροφοριών.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών / Προσωπικών Δεδομένων (ΥΑΠ/ΠΔ) είναι υπεύθυνος για την καθημερινή διαχείριση και έλεγχο εφαρμογής του ΣΔΑΠ/ΠΔ.

Τα καθήκοντα του Υπεύθυνου Ασφάλειας Πληροφοριών / Προσωπικών Δεδομένων περιλαμβάνουν:

- Τον προσδιορισμό των ρόλων και καθηκόντων σχετικά με την ασφάλεια των πληροφοριακών πόρων της εταιρείας.
- Τη συμμετοχή και υποστήριξη σημαντικών πρωτοβουλιών σχετικά με την ασφάλεια (π.χ. πρόγραμμα επιμόρφωσης στελεχών σε θέματα ασφάλειας, πρόγραμμα προώθησης του ΣΔΑΠ/ΠΔ).
- Τη μέριμνα για τη συμπερίληψη των κατάλληλων μέτρων ασφάλειας στον σχεδιασμό επεκτάσεων / αναβαθμίσεων των πληροφοριακών συστημάτων και υποδομών της εταιρείας.
- Τη μέριμνα για τη λήψη όλων των κατάλληλων μέτρων για τη διασφάλιση της φυσικής και περιβαλλοντικής ασφάλειας των κτιριακών υποδομών της εταιρείας.

- Την αποτίμηση της καταλληλότητας και τον συντονισμό της εφαρμογής μέτρων ασφάλειας κατά την υλοποίηση επεκτάσεων / αναβαθμίσεων των πληροφοριακών συστημάτων και υποδομών της εταιρίας.
- Τη διατήρηση της δέσμευσης της Διοίκησης της εταιρείας στην εφαρμογή του ΣΔΑΠ/ΠΔ.
- Την υποβολή προτάσεων στη Διοίκηση για τη λήψη πρόσθετων μέτρων ασφάλειας.
- Τον έλεγχο και έγκριση νέων πολιτικών και διαδικασιών ασφάλειας ή τροποποιήσεων σε ήδη υπάρχουσες.
- Τον ακριβή προσδιορισμό των πληροφοριακών πόρων της εταιρείας.
- Τον προσδιορισμό των διαδικασιών χορήγησης πρόσβασης στους πληροφοριακούς πόρους.
- Την έγκριση / άρνηση χορήγησης πρόσβασης στους πληροφοριακούς πόρους.
- Την επισκόπηση και αναθεώρηση, εάν κριθεί απαραίτητο, των δικαιωμάτων πρόσβασης στους πληροφοριακούς πόρους.
- Την παρακολούθηση και έλεγχο των σχετικών περιστατικών ασφάλειας.

Επίσης, στα τυπικά καθήκοντα του ΥΑΠ/ΠΔ εντάσσονται:

- Η μέριμνα για συνεχή συμμόρφωση προς τις πολιτικές ασφάλειας και η υποστήριξη της εφαρμογής τους.
- Η ανάπτυξη και συνεχής επικαιροποίηση του προγράμματος αντιμετώπισης περιστατικών ασφάλειας και συνέχισης της επιχειρησιακής λειτουργίας.
- Η συμβολή και ενεργός συμμετοχή σε όλα τα θέματα ή προβλήματα που αφορούν στην ασφάλεια των πληροφοριακών πόρων της εταιρείας.

iii. Διαχειριστές συστημάτων.

Οι διαχειριστές των συστημάτων είναι τα άτομα εκείνα που είναι επιφορτισμένα με τις εργασίες καθημερινής διαχείρισης των πληροφοριακών συστημάτων και έχουν την ευθύνη καλής λειτουργίας τους. Στα καθήκοντά τους εμπίπτουν:

- Η χορήγηση πρόσβασης σε πληροφοριακούς πόρους (απόδοση επιπλέον δικαιωμάτων ή δημιουργία νέου λογαριασμού χρήστη).
- Η διατήρηση του φυσικού ελέγχου των δεδομένων.
- Η εφαρμογή των προβλεπόμενων μέτρων ασφάλειας κατά την πρόσβαση, επεξεργασία, αποθήκευση και μετάδοση πληροφορίας.
- Η διαχείριση των λογαριασμών χρηστών σύμφωνα με την πολιτική και τα πρότυπα ασφάλειας.

- Η παροχή υποστήριξης στον ΥΑΠ για θέματα λειτουργίας και συντήρησης των συστημάτων.
- Ο έλεγχος τήρησης των πολιτικών ασφάλειας από τους χρήστες (π.χ. χρήση των σταθμών εργασίας, χρήση του διαδικτύου κλπ).
- Η τακτική ή έκτακτη αναφορά στον ΥΑΠ για την εκδήλωση περιστατικών ασφάλειας
- Η εισήγηση στον ΥΑΠ για τη λήψη πρόσθετων μέτρων ασφάλειας.

iv. Χρήστες συστημάτων.

Ως χρήστες των συστημάτων της εταιρείας θεωρούνται όλα τα στελέχη της που χρησιμοποιούν τα συστήματα -που εμπίπτουν στο πεδίο εφαρμογής του ΣΔΑΠ- για την εκτέλεση των καθηκόντων εργασίας τους. Οι χρήστες των συστημάτων οφείλουν να συμμορφώνονται με όσα προβλέπονται στο ΣΔΑΠ.

4.5.2 Διαχωρισμός καθηκόντων και αρμοδιοτήτων.

Η εταιρεία έχει μεριμνήσει ώστε να υπάρχει σαφής διαχωρισμός καθηκόντων και αρμοδιοτήτων ανάμεσα στους διάφορους ρόλους. Ειδικότερα, η πρόσβαση ενός ατόμου σε πληροφοριακούς πόρους της εταιρείας επιτρέπεται κατόπιν κατάλληλης εξουσιοδότησης από άλλον ρόλο, σύμφωνα με σαφώς τεκμηριωμένη διαδικασία.

4.5.3 Σημεία επικοινωνίας με τις Αρχές.

Η επικοινωνία με τις Αρχές σε περίπτωση εκδήλωσης κάποιου περιστατικού παραβίασης της ασφάλειας γίνεται με προκαθορισμένο τρόπο. Υπεύθυνος από την πλευρά της εταιρείας για την αναφορά των περιστατικών ασφάλειας στην κατάλληλη Αρχή, καθώς και για τη γενικότερη επικοινωνία με τις Αρχές, είναι ο ΥΑΠ/ΠΔ. Ανάλογα με το είδος των περιστατικών ασφάλειας, ο ΥΑΠ/ΠΔ είναι πιθανό να χρειαστεί να επικοινωνήσει με τις παρακάτω Αρχές:

- Ελληνική Αστυνομία
- Πυροσβεστική Υπηρεσία
- Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
- Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Υπηρεσία δίωξης ηλεκτρονικού εγκλήματος

Ο ΥΑΠ/ΠΔ διατηρεί κατάλογο με τα στοιχεία επικοινωνίας των ανωτέρω Αρχών (τηλέφωνο, email, ονοματεπώνυμα σημείων επαφής).

4.5.4 Επικοινωνία με ειδικές ομάδες σχετικά με την ασφάλεια πληροφοριών.

Η διατήρηση επαφών με ειδικούς εμπειρογνώμονες σε θέματα ασφάλειας, η συμμετοχή σε ειδικές ομάδες εργασίας και επαγγελματικές ενώσεις και η πρόσβαση σε εξειδικευμένες ηλεκτρονικές βιβλιοθήκες πληροφοριών διασφαλίζουν ότι η εταιρεία, και συγκεκριμένα τα στελέχη της που είναι υπεύθυνα για τη διαχείριση της ασφάλειας των πληροφοριών της, παρακολουθεί στενά τις εξελίξεις στον τομέα της ασφάλειας πληροφοριών και διαθέτει συνεχώς επίκαιρη γνώση σχετικά με τις σύγχρονες απειλές και μέτρα προστασίας.

Ο ΥΑΠ/ΠΔ είναι υπεύθυνος για να αποφασίσει εάν κάποια από τις παραπάνω ενέργειες είναι αναγκαία. Στην περίπτωση αυτή, ο ΥΑΠ/ΠΔ αποτελεί το σημείο επαφής της εταιρείας με τους ειδικούς εμπειρογνώμονες / ειδικές ομάδες / επαγγελματικές ενώσεις σχετικά με την ασφάλεια των πληροφοριών.

Ενδεικτικές πηγές πληροφόρησης που παρακολουθεί ο ΥΑΠ/ΠΔ είναι οι εξής:

- European Union Agency for Network and Information Security (ENISA), http://www.enisa.europa.eu
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, http://www.nist.gov
- Information Systems Audit and Control Association (ISACA), http://www.isaca.org
- Information Systems Security Certification Consortium (ISC2), https://www.isc2.org/

4.5.5 Ασφάλεια πληροφοριών κατά τη διαχείριση έργων.

Κατά τη διαχείριση έργων που εμπίπτουν στο πεδίο εφαρμογής του ΣΔΑΠ, σε όλο τον κύκλο ζωής τους, η εταιρεία μεριμνά για τη συμμόρφωσή τους με τις απαιτήσεις ασφάλειας της εταιρείας. Ειδικότερα, κατά την ανάλυση απαιτήσεων και τον καθορισμό προδιαγραφών των έργων, η εταιρεία καθορίζει τις απαιτήσεις και προδιαγραφές ασφάλειας που πρέπει να πληρούνται.

4.6 Ασφάλεια ανθρωπίνων πόρων.

Όλα τα στελέχη της εταιρείας έχουν υποχρέωση εφαρμογής της πολιτικής ασφάλειας της εταιρείας, εφόσον διαχειρίζονται ή σχετίζονται με πληροφοριακούς πόρους που εμπίπτουν στο πεδίο εφαρμογής του ΣΔΑΠ/ΠΔ, ανάλογα με τον ρόλο τους. Αντίστοιχη υποχρέωση έχουν και οι συνεργάτες της εταιρείας που δεν ανήκουν στο στελεχιακό δυναμικό της.

Τα στελέχη (προσωπικό ή συνεργάτες) που έχουν υποχρέωση συμμόρφωσης με την πολιτική ασφάλειας της εταιρείας οφείλουν κατ’ ελάχιστον:

- Να είναι ενήμερα σχετικά με τους στόχους και τις πολιτικές ασφάλειας της εταιρείας.
- Να εφαρμόζουν το ΣΔΑΠ/ΠΔ και τις προβλεπόμενες διαδικασίες ασφάλειας.

- Να χρησιμοποιούν τους πληροφοριακούς πόρους της εταιρείας σύμφωνα με τις αντίστοιχες πολιτικές ορθής χρήσης, όπου υπάρχουν.
- Να βρίσκονται διαρκώς σε ετοιμότητα για την αναγνώριση και αναφορά περιστατικών ασφάλειας.

4.6.1 Έλεγχοι ασφάλειας πριν την πρόσληψη.

Η EPSILON NET δίνει ιδιαίτερη σημασία στην καταλληλότητα του προσωπικού που προσλαμβάνει σε σχέση με τον ρόλο και τα καθήκοντα που πρόκειται να του αναθέσει. Για τον λόγο αυτό εφαρμόζει κατάλληλες διαδικασίες ελέγχων και εξακρίβωσης στοιχείων πριν προβεί στην πρόσληψη ενός στελέχους.

Στο πλαίσιο των ελέγχων που εντάσσονται στις διαδικασίες πρόσληψης, περιλαμβάνονται οι εξής έλεγχοι (ανάλογα με τη θέση για την οποία προορίζεται ο υποψήφιος προς πρόσληψη):

- Επιβεβαίωση των προσωπικών στοιχείων και της διεύθυνσης του υποψηφίου.
- Επιβεβαίωση των τίτλων σπουδών και τυχόν επαγγελματικών τίτλων του υποψηφίου.
- Επιβεβαίωση της προϋπηρεσίας του υποψηφίου.

Επιπλέον, ανάλογα με τις δυνατότητες που παρέχει η νομοθεσία, για σημαντικές θέσεις στο σχήμα διαχείρισης της ασφάλειας της εταιρείας, η εταιρεία δύναται να προβαίνει σε έλεγχο πρόσθετων στοιχείων των υποψήφιων στελεχών για τις συγκεκριμένες θέσεις.

Οι ακριβείς όροι και προϋποθέσεις για την απασχόληση ενός στελέχους στην εταιρεία αποτυπώνονται σε σχετική συμφωνία συνεργασίας, η οποία υπογράφεται από την εταιρεία και το στέλεχος και περιγράφει επαρκώς τη μεταξύ τους συνεργασία. Στη συμφωνία αυτή, αποτυπώνονται και οι ευθύνες που έχει ο εργαζόμενος απέναντι στην επιχείρηση σχετικά με την ασφάλεια των πληροφοριών (π.χ. θέματα εμπιστευτικότητας - εχεμύθειας).

Στις συμφωνίες συνεργασίας που συνάπτουν εξωτερικοί συνεργάτες με την εταιρεία, γίνεται ρητή μνεία στα θέματα ασφάλειας πληροφοριών που τους αφορούν.

Τα συμφωνητικά συνεργασίας της εταιρείας τόσο με τους υπαλλήλους όσο και με τους εξωτερικούς συνεργάτες περιλαμβάνουν επιπλέον τις υποχρεώσεις, τα δικαιώματα και την ευθύνη των στελεχών ως προς την ασφάλεια (ιδιαίτερα την εμπιστευτικότητα) των πληροφοριών της εταιρείας.

Όλα τα παραπάνω στοιχεία δύναται να περιλαμβάνονται και σε ειδικές συμφωνίες εμπιστευτικότητας - εχεμύθειας (non disclosure agreements) που υπογράφουν με την εταιρεία.

4.6.2 Ασφάλεια κατά τη διάρκεια της απασχόλησης.

4.6.2.1 Ευθύνη της Διοίκησης.

Όλα τα στελέχη της εταιρείας έχουν υποχρέωση εφαρμογής της πολιτικής ασφάλειας της εταιρείας, ανάλογα με τον ρόλο τους. Η διοίκηση μεριμνά ώστε το προσωπικό της εταιρείας να είναι πλήρως ενημερωμένο για την πολιτική ασφάλειας και να την τηρεί κατά γράμμα. Παράλληλα ελέγχει την τήρηση της πολιτικής ασφάλειας της εταιρείας σε καθημερινή βάση.

4.6.2.2 Ενημέρωση, εκπαίδευση και κατάρτιση σε θέματα ασφάλειας πληροφοριών.

Η εταιρεία μεριμνά διαρκώς για την ενημέρωση, εκπαίδευση και πληροφόρηση του ανθρώπινου δυναμικού της για θέματα, κινδύνους και διαδικασίες ασφάλειας. Ειδικότερα:

- Κατά την πρόσληψη ενός νέου στελέχους στην εταιρεία, ο προϊστάμενος της Διεύθυνσης ή του Τμήματος στο οποίο εντάσσεται ενημερώνει το στέλεχος αυτό για την πολιτική ασφάλειας της εταιρείας, ιδιαίτερα σε ό,τι αφορά στις σχετικές υποχρεώσεις που απορρέουν από τον ρόλο και τη θέση του.
- Η Πολιτική Ασφάλειας (ή μέρος αυτής) είναι συνεχώς διαθέσιμη, σε ηλεκτρονική μορφή, σε συγκεκριμένο σημείο του εσωτερικού δικτύου της εταιρείας, το οποίο είναι γνωστό σε όλο το ανθρώπινο δυναμικό της εταιρείας.
- Η εταιρεία οργανώνει ειδικά σεμινάρια ασφάλειας πληροφοριών, όποτε αυτό κρίνεται απαραίτητο.
- Τα στελέχη της εταιρείας με αυξημένες αρμοδιότητες και ευθύνες σχετικά με τη διαχείριση της ασφάλειας των πληροφοριακών πόρων της εταιρείας συμμετέχουν σε ειδικά σεμινάρια ασφάλειας, κατόπιν έγκρισης των διοικητικών υπηρεσιών της εταιρείας. Το πλήθος και το είδος των σεμιναρίων που επιλέγονται, αποφασίζονται σε ετήσια βάση και σχετίζονται με τις εξελίξεις στον τομέα της ασφάλειας, τα περιστατικά ασφάλειας που έχουν παρουσιαστεί, καθώς και τα διαθέσιμα κονδύλια της εταιρείας.
- Η Διοίκηση της εταιρείας παρέχει συνεχή και έμπρακτη υποστήριξη στην εφαρμογή της Πολιτικής Ασφάλειας.
- Η εταιρεία τηρεί αρχείο για τις δράσεις ενημέρωσης / εκπαίδευσης του προσωπικού της σε σχέση με την πολιτική ασφάλειας της εταιρείας ή γενικότερα για θέματα ασφάλειας πληροφοριών.

4.6.2.3 Κυρώσεις.

Η Διοίκηση της εταιρείας δύναται να προχωρήσει στην επιβολή ποινών σε όσους δεν συμμορφώνονται με την πολιτική ασφάλειας, ανάλογα με το είδος και τη σοβαρότητα της περίπτωσης, και μόνο εφόσον υπάρχουν επαρκείς αποδείξεις για την παραβίαση της πολιτικής ασφάλειας.

Οι κυρώσεις / ποινές μπορεί να περιλαμβάνουν, στην περίπτωση των εργαζομένων, απλή επίπληξη για ήσσονος σημασίας παραβάσεις / μη συμμορφώσεις μέχρι και άμεση απόλυση (ή ακόμα και άσκηση ένδικων βοηθημάτων) για εκούσιες ενέργειες με ιδιαίτερα σοβαρές επιπτώσεις στην εικόνα και τη λειτουργία της εταιρείας. Ανάλογα με το είδος και τη σημασία της παράβασης, η εταιρεία προβαίνει αρχικά σε προφορική επίπληξη του εργαζομένου, εν συνεχεία σε έγγραφη επίπληξη και, σε περίπτωση συνεχιζόμενης μη συμμόρφωσης, δύναται να προβεί στην απόλυσή του.

Αντίστοιχα, στην περίπτωση των εξωτερικών συνεργατών / προμηθευτών, οι κυρώσεις / ποινές που μπορούν να επιβληθούν εξαρτώνται από τους όρους των αντίστοιχων συμφωνιών / συμβάσεων της εταιρείας με τα τρίτα αυτά μέρη και, ενδεικτικά, μπορεί να περιλαμβάνουν απλή έγγραφη διαμαρτυρία, εξώδικη όχληση - διαμαρτυρία, καταγγελία της σύμβασης ή ακόμα και άσκηση ένδικων βοηθημάτων.

Σε κάθε περίπτωση, οι κυρώσεις / ποινές που δύνανται να επιβληθούν πρέπει να είναι σύμφωνες με την ισχύουσα νομοθεσία.

4.6.3 Τερματισμός και αλλαγή απασχόλησης.

Κάθε στέλεχος της εταιρείας, με το οποίο διακόπτεται η συνεργασία, πρέπει να επιστρέφει όλους τους πληροφοριακούς πόρους της εταιρείας που έχει στη διάθεσή του. Ομοίως, τα δικαιώματα χρήσης που είχε το στέλεχος αυτό κατά την απασχόλησή του στην εταιρεία, ακυρώνονται από τους διαχειριστές των συστημάτων της εταιρείας, αμέσως μετά τη λήξη της συνεργασίας του στελέχους με την εταιρεία.

4.7 Διαχείριση πληροφοριακών πόρων.

Η EPSILON NET τηρεί αρχείο με όλους τους πόρους της εταιρείας που προστατεύονται από την πολιτική ασφάλειας.

Κάθε πληροφοριακός πόρος τίθεται υπό την ευθύνη συγκεκριμένου στελέχους της εταιρείας.

4.7.1 Αποδεκτή χρήση (acceptable use) σταθμών εργασίας και πληροφοριακών συστημάτων.

Οι σταθμοί εργασίας και τα πληροφοριακά συστήματα της εταιρείας θα πρέπει να χρησιμοποιούνται μόνο για επιχειρησιακούς σκοπούς της εταιρείας. Όλα τα δεδομένα που είναι αποθηκευμένα, επεξεργάζονται ή μεταδίδονται μέσω σταθμών εργασίας ή πληροφοριακών συστημάτων πρέπει να προστατεύονται αποτελεσματικά από μη εξουσιοδοτημένη τροποποίηση, καταστροφή ή αποκάλυψη.

Οι χρήστες των σταθμών εργασίας και των πληροφοριακών συστημάτων της εταιρείας πρέπει να συμμορφώνονται με τις εξής οδηγίες:

- Να μην αποκαλύπτουν τα στοιχεία πρόσβασής τους (username / password) στα συστήματα.
- Να αλλάζουν τακτικά το συνθηματικό πρόσβασης (password) στα συστήματα.
- Να μην αποθηκεύουν σε αποσπώμενα μέσα (CD/DVD, flash disks κλπ.) δεδομένα της εταιρείας με σκοπό να τα μεταφέρουν εκτός των εγκαταστάσεων της εταιρείας χωρίς κατάλληλη εξουσιοδότηση.
- Να μην εγκαθιστούν στα συστήματα προϊόντα λογισμικού, τα οποία δεν φέρουν τη νόμιμη άδεια χρήσης. Στην περίπτωση ελεύθερου λογισμικού, το οποίο θα χρησιμοποιηθεί για επιχειρησιακούς σκοπούς της εταιρείας, η απόκτηση και εγκατάσταση πρέπει να γίνεται μόνο από κατάλληλο τεχνικό προσωπικό, αφού πρώτα ελεγχθούν διεξοδικά οι όροι χρήσης του.
- Να μην χρησιμοποιούν αλόγιστα τους σταθμούς εργασίας και τα πληροφοριακά συστήματα της εταιρείας για προσωπικούς τους σκοπούς.
- Να έχουν ενεργοποιημένη την επιλογή προστασίας (κλειδώματος) οθόνης, σε περίπτωση αδράνειας του συστήματος. Η απενεργοποίηση του κλειδώματος πρέπει να απαιτεί την εισαγωγή του συνθηματικού πρόσβασης του χρήστη.

4.7.2 Αποδεκτή χρήση (acceptable use) του ηλεκτρονικού ταχυδρομείου.

Το ηλεκτρονικό ταχυδρομείο θα πρέπει να χρησιμοποιείται μόνο για επιχειρησιακούς σκοπούς της εταιρείας. Τα δεδομένα που διακινούνται μέσω ηλεκτρονικού ταχυδρομείου θα πρέπει να προστατεύονται αποτελεσματικά.

Το προσωπικό της εταιρείας πρέπει να συμμορφώνεται με τις εξής οδηγίες:

- Η επίσημη ηλεκτρονική αλληλογραφία της εταιρείας θα πρέπει να διακινείται αποκλειστικά μέσω της προβλεπόμενης υποδομής (name@epsilonnet.gr). Οι λογαριασμοί ηλεκτρονικού ταχυδρομείου είναι εταιρικοί και όχι προσωπικοί, συνεπώς,

το προσωπικό της εταιρείας δεν πρέπει να χρησιμοποιεί τον εταιρικό λογαριασμό για την εγγραφή σε ηλεκτρονικές υπηρεσίες εξωτερικών παρόχων ή να τον γνωστοποιεί σε μέσα κοινωνικής δικτύωσης.

- Τα δεδομένα που λαμβάνονται μέσω ηλεκτρονικού ταχυδρομείου, ειδικά τα επισυναπτόμενα αρχεία των μηνυμάτων, θα πρέπει να ελέγχονται για ιούς πριν από τη χρήση τους.
- Απαγορεύεται η μετάδοση εμπιστευτικών δεδομένων της εταιρείας μέσω ηλεκτρονικού ταχυδρομείου.
- Ο Υπεύθυνος Ασφάλειας θα πρέπει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τον περιορισμό της άσκοπης χρήσης του ηλεκτρονικού ταχυδρομείου (π.χ. για λήψη και αποστολή chain mails), της λήψης εμπορικών μηνυμάτων, spam κλπ.
- Το προσωπικό της εταιρείας δεν επιτρέπεται να ανοίγει συνημμένα αρχεία, να επιλέγει συνδέσμους (links) που περιλαμβάνονται σε μηνύματα ηλεκτρονικού ταχυδρομείου ή να απαντά σε μήνυμα ηλεκτρονικού ταχυδρομείου όταν:
    - ο αποστολέας είναι άγνωστος
    - το όνομα του αποστολέα διαφέρει από την ηλεκτρονική του διεύθυνση
    - το email προέρχεται φαινομενικά από παρόχους οικονομικών, τραπεζικών ή άλλων υπηρεσιών και ζητούνται αναγνωριστικά, οικονομικά ή άλλα προσωπικά στοιχεία των χρηστών
    - το μήνυμα ηλεκτρονικού ταχυδρομείου έχει αποσταλεί σε πολλαπλούς μη φανερούς παραλήπτες (undisclosed recipients).

4.8 Έλεγχος πρόσβασης.

Η χορήγηση δικαιωμάτων στα στελέχη και τους συνεργάτες της εταιρείας για πρόσβαση σε πληροφοριακούς πόρους ακολουθεί σαφή και τεκμηριωμένη διαδικασία εγκεκριμένη από τη Διοίκηση της εταιρείας. Η πρόσβαση στους πληροφοριακούς πόρους ελέγχεται με κατάλληλα μέσα και μηχανισμούς αναγνώρισης της ταυτότητας των χρηστών. Οι χρήστες είναι υπεύθυνοι για την προστασία των διακριτικών πρόσβασής τους στους πληροφοριακούς πόρους της εταιρείας.

4.8.1 IT Access - Γενικά.

Όλοι οι κωδικοί πρόσβασης παρέχονται έπειτα από εντολή των διευθυντών ή προϊσταμένων των τμημάτων.

Όλοι οι κωδικοί πρόσβασης, σε επίπεδο χρήστη, αλλάζουν λόγω Active Directory Policy κάθε ενενήντα (90) ημέρες ή κάθε φορά που ένα σύστημα προτρέπει τον χρήστη να τον αλλάξει (A.9.4.3).

Οι χρήστες δεν επαναχρησιμοποιούν τον ίδιο κωδικό πρόσβασης μέσα σε πέντε (5) αλλαγές κωδικού πρόσβασης.

Όλα τα συστήματα και οι διαδικασίες της EPSILON NET, εφαρμόζουν τα ακόλουθα: (α) Έλεγχος ταυτότητας μεμονωμένων χρηστών, όχι ομάδων χρηστών. Δηλαδή, δεν υπάρχουν γενικοί λογαριασμοί, εκτός από αυτούς που υπάρχουν για συγκεκριμένα projects, που με το τέλος κάθε project γίνεται αλλαγή των κωδικών. (β) Προστασία όσον αφορά στην ανάκτηση κωδικών πρόσβασης και στοιχείων ασφαλείας. (γ) Παρακολούθηση και καταγραφή πρόσβασης στο σύστημα (σε επίπεδο χρήστη). (δ) Διαχείριση ρόλων ώστε να είναι δυνατή η εκτέλεση λειτουργιών χωρίς να μοιράζονται κωδικοί πρόσβασης. (ε) Οι διαδικασίες διαχείρισης κωδικού πρόσβασης είναι ασφαλείς και ελέγχονται (A.9.1.1).

Οι τυπικές διαδικασίες ελέγχου πρόσβασης των χρηστών τεκμηριώνονται, εφαρμόζονται και ενημερώνονται για κάθε σύστημα εφαρμογής και πληροφοριών, ώστε να εξασφαλίζεται η εξουσιοδοτημένη πρόσβαση των χρηστών και να προλαμβάνεται η μη εξουσιοδοτημένη πρόσβαση. Οι εν λόγω διαδικασίες καλύπτουν όλα τα στάδια του κύκλου ζωής της πρόσβασης των χρηστών που δεν χρειάζονται πλέον πρόσβαση.

Κάθε χρήστης διαθέτει δικαίωμα πρόσβασης και δικαιώματα σε συστήματα και δεδομένα υπολογιστών τα οποία: (α) Είναι ανάλογα με τις εργασίες που αναμένεται να εκτελεσθούν (A.9.2.2). (β) Έχουν ένα μοναδικό όνομα χρήστη, το οποίο δεν μοιράζεται ή αποκαλύπτεται σε κανέναν άλλον χρήστη. (γ) Έχουν ένα συνδεδεμένο μοναδικό κωδικό πρόσβασης που ζητείται σε κάθε νέα σύνδεση. (A.9.1.1)

Τα δικαιώματα πρόσβασης των χρηστών επανεξετάζονται κάθε έξι (6) μήνες σε συνεργασία με τον διευθυντή του τμήματος και το τμήμα IT, ώστε να εξασφαλίζεται ότι εξακολουθούν να χορηγούνται τα κατάλληλα δικαιώματα (A.9.2.1, A.9.2.5, A.9.1.1).

Οι λογαριασμοί διαχείρισης συστήματος παρέχονται μόνο σε χρήστες που είναι υποχρεωμένοι να εκτελούν εργασίες διαχείρισης του συτήματος (λ.χ. τα μέλη του τμήματος IT) και έπειτα από εξέταση του αιτήματος από τη Γενική Διεύθυνση (A.9.2.3).

Μια αίτηση πρόσβασης στα συστήματα ηλεκτρονικών υπολογιστών της εταιρείας πρέπει πρώτα να υποβληθεί στο σύστημα διαχείρισης ticket για δημιουργία (A.9.2.2).

Οι αιτήσεις πρόσβασης πρέπει να υποβάλλονται μόνον εάν έχει αποκτηθεί έγκριση από τον διευθυντή του χρήστη (A.9.2.2).

Οι προσωρινοί κωδικοί πρόσβασης δίνονται στον χρήστη είτε μέσω τηλεφώνου είτε μέσω email. Λόγω των ρυθμίσεων που έχουν γίνει σε εφαρμογές και λειτουργικά συστήματα (μέσω Active Directory Policy) ο χρήστης κατά την πρώτη είσοδό του πρέπει να αλλάξει τον κωδικό που του έχει δοθεί έτσι ώστε να διασφαλίζεαι ότι μόνον ο ίδιος τον γνωρίζει (A.9.2.4, A.9.4.3).

Όταν ένας εργαζόμενος εγκαταλείπει τηνεταιρεία, η πρόσβασή του σε όλα τα συστήματα πληροφορικής αλλά και τα access controls στις κτιριακές υποδομές αναστέλλονται κατά τη διάρκεια της τελευταίας ημέρας εργασίας του. Ο διευθυντής του τμήματος έχει ευθύνη να ζητήσει την αναστολή των δικαιωμάτων πρόσβασης του εργαζομένου από το τμήμα IT (A.9.2.1, A.9.2.6, A.9.1.1).

4.8.2 Έλεγχος πρόσβασης διακομιστή και εφαρμογών.

Η πρόσβαση στους διακομιστές γίνεται με την βοήθεια του Active Directory, αφότου έχει εγκριθεί από τον διευθυντή του εκάστοτε τμήματος η ένταξη του υπαλλήλου στο ανάλογο Security Group.

Η πρόσβαση στις εφαρμογές γίνεται είτε με τη βοήθεια του Active Directory είτε με μοναδικό λογαριασμό της εκάστοτε εφαρμογής (A.9.4.4).

Όλη η πρόσβαση στα λειτουργικά συστήματα γίνεται μέσω ενός μοναδικού ονόματος χρήστη, το οποίο θα ελεγχθεί και μπορεί να ανιχνευθεί πίσω σε κάθε μεμονωμένο χρήστη. Η διαδικασία σύνδεσης προστατεύεται, επίσης, με τους εξής τρόπους: (α) Δεν εμφανίζονται προηγούμενες πληροφορίες σύνδεσης, π.χ. όνομα χρήστη. (β) Περιορισμός του αριθμού ανεπιτυχών προσπαθειών (πέντε προσπάθειες) και κλείδωμα του λογαριασμού σε περίπτωση υπέρβασης για δέκα (10) λεπτά (A.9.4.3). (γ) Οι χαρακτήρες του κωδικού πρόσβασης είναι κρυμμένοι με σύμβολα (A.9.4.3). (δ) Η πολυπλοκότητα των κωδικών πρόσβασης ρυθμίζεται από το Active Directory. Οι κωδικοί περιέχουν γράμματα (κεφαλαία και μικρά), αριθμό και σύμβολο (A.9.4.3).

Οι διαχειριστές συστήματος έχουν μεμονωμένους λογαριασμούς διαχειριστή (ομάδα administrator) που καταγράφονται και ελέγχονται.

Η πρόσβαση σε εφαρμογές λογισμικού περιορίζεται χρησιμοποιώντας τα χαρακτηριστικά ασφαλείας που είναι ενσωματωμένα στο συγκεκριμένο προϊόν.

Ο CTO είναι υπεύθυνος για τη χορήγηση πρόσβασης στις πληροφορίες εντός του συστήματος.

Η πρόσβαση: (α) Χωρίζει σε σαφώς καθορισμένους ρόλους τους χρήστες (A.6.1.2), (β) Δίνει το κατάλληλο επίπεδο πρόσβασης που απαιτείται για τον ρόλο του χρήστη (A.6.1.2, A.9.2.2, A.9.4.1). (γ) Δεν επιτρέπει την αντικατάσταση (με αφαίρεση ή απόκρυψη των ρυθμίσεων διαχείρισης από τον χρήστη). (δ) Δεν επιτρέπει την τροποποίηση των δικαιωμάτων που έχουν κληρονομήσει από το λειτουργικό σύστημα που θα μπορούσαν να επιτρέψουν μη εξουσιοδοτημένα υψηλότερα επίπεδα πρόσβασης (A.6.1.2). (ε) Καταγράφεται και ελέγχεται.

Για την πρόσβαση σε πηγαίο κώδικα χρησιμοποιείται ξεχωριστός διακομιστής για διαχωρισμό της πρόσβασης. Συγκεκριμένη εφαρμογή διαχειρίζεται τον πηγαίο κώδικα και καταγράφει τις προσβάσεις και τις αλλαγές στον κώδικα. Ο κάθε χρήστης έχει συγκεκριμένα

δικαιώματα ανάγνωσης και επεξεργασίας ανάλογα με το project που ασχολείται η ομάδα του (A.9.4.5).

4.8.3 Απομακρυσμένη πρόσβαση υπαλλήλου.

Η απομακρυσμένη πρόσβαση στα συστήματα της εταιρείας από τους υπαλλήλους της γίνεται έπειτα από σχετική άδεια του τμήματος IT.

Το τμήμα IT αξιολογεί τον σκοπό της σύνδεσης και αν είναι αποδεκτός χορηγεί την ανάλογη πρόσβαση.

Η πρόσβαση υλοποιείται μέσα από την VPN εφαρμογή και πάντα μέσω του υπολογιστή του υπαλλήλου που ζητάει πρόσβαση για περισσότερη ασφάλεια. Με τη χρήση του VPN ισχύουν όλα τα μέτρα ασφαλείας που λαμβάνει η εταιρεία.

(A.6.2.2)

4.9 Φυσική και περιβαλλοντική ασφάλεια.

Η εκτίμηση της επικινδυνότητας προσδιορίζει το κατάλληλο επίπεδο προστασίας που εφαρμόζεται για τη διασφάλιση της αποθήκευσης των πληροφοριών.

Η φυσική ασφάλεια αρχίζει με το ίδιο το κτίριο της EPSILON NET και διεξάγεται αξιολόγηση της ευαισθησίας της περιμέτρου (A.11.1.1).

Η πρόσβαση στις εγκαταστάσεις της EPSILON NET επιτρέπεται μόνο σε άτομα με κατάλληλη εξουσιοδότηση και μόνο με τη χρήση των μέτρων που έχει ορίσει η εταιρεία.

Οι μηχανισμοί ελέγχου περιλαμβάνουν ιδίως:

- Συναγερμούς που είναι τοποθετημένοι σε όλα τα μέρη των εγκαταστάσεων και είναι ενεργοποιημένοι καθ’ όλη τη διάρκεια της ημέρας.
- Κλειδαριές παραθύρων και θυρών (A.11.1.1).
- Ράφια παραθύρων στα χαμηλότερα επίπεδα δαπέδου (A.11.1.1).
- Μηχανισμούς ελέγχου πρόσβασης που είναι εγκατεστημένοι σε όλες τις προσβάσιμες πόρτες. Όπου χρησιμοποιούνται κωδικοί, αλλάζονται τακτικά και είναι γνωστοί μόνο σε όσους έχουν άδεια πρόσβασης στην περιοχή / κτίριο.
- Κάμερες CCTN.
- Επανδρωμένο χώρο υποδοχής (A.11.1.1).
- Προστασία από βλάβες (λ.χ. πυρανίχνευση σε όλες τις εγκαταστάσεις και πυρασφάλεια στο Server Room) και από βανδαλισμούς με την κατάλληλη φρούρηση από άτομο ασφαλείας (A.11.1.4).

- Το προσωπικό που εργάζεται σε ασφαλείς περιοχές θα αμφισβητήσει όποιον δεν φέρει σήμα.
- Τα αναγνωριστικά και τα εργαλεία πρόσβασης / διέλευσης (π.χ. διακριτικά, κλειδιά, κωδικοί εισόδου κλπ) τηρούνται μόνο από το προσωπικό που έχει εξουσιοδοτηθεί να έχει πρόσβαση σε αυτές τις περιοχές και δεν επιτρέπεται να δανείζονται / παρέχονται σε οποιονδήποτε άλλον (Α.11.1.2).
- Οι επισκέπτες σε ασφαλείς περιοχές υποχρεούνται να συνδεθούν και να αποσυνδεθούν σύμφωνα με τους χρόνους άφιξης και αναχώρησης από τις εγκαταστάσεις της εταιρείας και υποχρεούνται να φέρουν αναγνωριστικό σήμα (καρτελάκι guest). Οι αφίξεις και αναχωρίσεις των επισκεπτών καταγράφονται σε βιβλίο επισκεπτών (Α.11.1.2).
- Όποιος επισκέπτεται τις εγκαταστάσεις της εταιρείας κατόπιν ραντεβού συνοδεύεται πάντα από το άτομο με το οποίο έχει προγραμματίσει το ραντεβού (Α.11.1.2).
- Ένας υπάλληλος του τμήματος πληροφορικής παρακολουθεί όλους τους επισκέπτες που επισκέπτονται ασφαλείς περιοχές πληροφορικής (Α.11.1.2).
- Τα κλειδιά όλων των ασφαλών περιοχών που στεγάζουν τον εξοπλισμό πληροφορικής και των ντουλαπιών IT που κλειδώνουν, φυλάσσονται σε χώρο που φρουρείται από φρουρό καθ' όλη διάρκεια της ημέρας. Σε όλες τις περιπτώσεις που υπάρχουν διαδικασίες ασφαλείας, εκδίδονται οδηγίες για την αντιμετώπιση της παράβασης ασφαλείας.
- Σε περίπτωση που υπάρχουν παραβιάσεις ή όταν ένα μέλος του προσωπικού αποχωρεί εκτός των κανονικών συνθηκών τερματισμού, όλα τα εργαλεία αναγνώρισης / πρόσβασης (π.χ. εμβλήματα, κλειδιά κλπ) ανακτώνται από άτομο του προσωπικού και οι κωδικοί θυρών / πρόσβασης αλλάζουν αμέσως.

Τέλος, όλοι οι χώροι διαθέτουν σύστημα κλιματισμό και σύστημα πυροπροστασίας.

4.10 Ασφάλεια λειτουργιών και επικοινωνιών.

Οι διαδικασίες λειτουργίας των πληροφοριακών συστημάτων της εταιρείας διαθέτουν κατάλληλη τεκμηρίωση, ενημερώνονται σε περίπτωση αλλαγών και είναι διαθέσιμες σε όλους τους χρήστες που τις χρειάζονται, μέσω των διαδικτυακών τόπων των αντίστοιχων κατασκευαστών. Η Διοίκηση της εταιρείας έχει μεριμνήσει για την επάρκεια των συστημάτων να καλύψουν τις επιχειρησιακές της ανάγκες, ενώ λαμβάνει κάθε πρόσφορο μέτρο για την προστασία από κακόβουλο λογισμικό, την αντιμετώπιση περιστατικών απώλειας δεδομένων και την πλήρη καταγραφή κάθε ενέργειας σε σχετικά αρχεία (logs) για σκοπούς παρακολούθησης και ελέγχου.

Επίσης, η εταιρεία έχει λάβει ένα σημαντικό αριθμό μέτρων για την προστασία του δικτύου της από μη εξουσιοδοτημένη πρόσβαση. Αντίστοιχα με την προστασία των πληροφοριών στο εσωτερικό της εταιρείας, έχουν ληφθεί κατάλληλα μέτρα για την προστασία εταιρικής πληροφορίας που διακινείται μέσω ηλεκτρονικού ταχυδρομείου, του διαδικτύου εν γένει ή άλλων μέσων επικοινωνίας.

4.10.1 Λειτουργικές διαδικασίες και ευθύνες.

Οι λειτουργικές διαδικασίες χρησιμοποιούνται σε όλη την καθημερινή συντήρηση των συστημάτων πληροφορικής και της υποδομής της εταιρείας, προκειμένου να διασφαλισθεί η μέγιστη δυνατή εξυπηρέτηση από αυτά τα στοιχεία ενεργητικού.

Οι αναβαθμίσεις στα λειτουργικά συστήματα της εταιρείας ελέγχονται μέσω κεντρικού εξυπηρετητή.

Τα περιβάλλοντα ανάπτυξης και δοκιμών είναι ξεχωριστά από το λειτουργικό περιβάλλον, ώστε να μειωθεί ο κίνδυνος τυχαίων αλλαγών ή μη εξουσιοδοτημένης πρόσβασης.

Υπάρχουν διαδικασίες χειρισμού εγγράφων σε κατάλληλο επίπεδο λεπτομέρειας για την ομάδα των τμημάτων που θα τα χρησιμοποιήσουν.

Όλες οι σημαντικές αλλαγές στην κύρια υποδομή (λ.χ. δίκτυο, κατάλογοι) αξιολογούνται για τον αντίκτυπό τους στην ασφάλεια των πληροφοριών ως μέρος της τυποποιημένης εκτίμησης κινδύνου.

Τα περιβάλλοντα ανάπτυξης και δοκιμής διαχωρίζονατι από τους καταλληλότερους ελέγχους, οι οποίοι περιλαμβάνουν ιδίως:

- Εκτέλεση σε ξεχωριστούς υπολογιστές, τομείς, παρουσίες και δίκτυα.
- Διαφορετικά ονόματα χρηστών και κωδικοί πρόσβασης.
- Καθήκοντα όσων μπορούν να έχουν πρόσβαση και να δοκιμάσουν λειτουργικά συστήματα.

Στους σταθμούς εργασίας εφαρμόζεται αυτόματο κλείδωμα έπειτα από πέντε (5) λεπτά αδράνειας μέσω Active Directory Policy (A.11.2.8).

4.10.2 Σχεδιασμός και αποδοχή συστήματος.

(A.12.1.3)

Όλες οι συνιστώσες ή οι εγκαταστάσεις υποδομής πληροφορικής της εταιρείας καλύπτονται από στρατηγικές σχεδιασμού και αντικατάστασης χωρητικότητας, για να διασφαλισθεί ότι οι αυξημένες απαιτήσεις για την περισσότερη δύναμη και αποθήκευση δεδομένων μπορούν να αντιμετωπισθούν και να εκπληρωθούν έγκαιρα.

Τα βασικά συστατικά στοιχεία υποδομής πληροφορικής περιλαμβάνουν ιδίως:

- Διακομιστές αρχείων
- Διακομιστές τομέα
- Διακομιστές ηλεκτρονικού ταχυδρομείου
- Web servers
- Εκτυπωτές
- Δίκτυα

Επίσης, πραγματοποιούνται περιβαλλοντικοί έλεγχοι, συμπεριλαμβανομένου του κλιματισμού.

Το τμήμα IT προγραμματίζει μία συνάντηση ετησίως με όλα τα τμήματα, κατά την οποία δέχεται ενημερώσεις για ενδεχόμενες νέες απαιτήσεις προϊόντων ή αναβαθμίσεις, service packs, patches, επιδιορθώσεις που απαιτούνται σε υπάρχοντα συστήματα, νέο ανθρώπινο δυναμικό ή νέα projects.

Όλα τα νέα προϊόντα αγοράζονται μέσω του IT manager ή του CTO.

Τα νέα συστήματα πληροφοριών, οι αναβαθμίσεις προϊόντων και οι ενημερώσεις κώδικα υποβάλλονται σε κατάλληλο επίπεδο ελέγχου πριν από την αποδοχή και την απελευθέρωση στο περιβάλλον. Αυτό αφορά και στα προϊόντα που αναπτύσσει η εταιρεία, καθώς και στα προϊόντα που χρησιμοποιεί για τη λειτουργία της (A.12.1.4, A.12.5.1).

Τα κριτήρια αποδοχής είναι σαφώς προσδιορισμένα, συμφωνούνται και τεκμηριώνονται, και περιλαμβάνουν την άδεια χρήσης.

Οι εφαρμογές τρίτου μέρους παρακολουθούνται για service pack και patches.

Οι σημαντικές αναβαθμίσεις του συστήματος δοκιμάζονται διεξοδικά παράλληλα με το υπάρχον σύστημα σε ένα ασφαλές περιβάλλον δοκιμών που αντιγράφει το λειτουργικό σύστημα (A.12.1.4, A.12.5.1).

4.10.3 Προστασία από κακόβουλο και κινητό κώδικα.

Λαμβάνονται τα κατάλληλα μέτρα για την προστασία όλων των πληροφοριακών συστημάτων, της υποδομής και των πληροφοριών της εταιρείας από τον κακόβουλο κώδικα.

Η εταιρεία διαθέτει πλήρως ενημερωμένο λογισμικό προστασίας από ιούς (antivirus), το οποίο -μέσω της κεντρικής κονσόλας διαχείρισης που διαθέτει το τμήμα IT- έχει τη δυνατότητα να παρακολουθεί ότι όλοι οι σταθμοί είναι ενημερωμένοι με τελευταίες εκδόσεις antivirus, καθώς επίσης δέχεται email alert σε περίπτωση που εντοπισθεί κάποιο πρόβλημα. Επίσης, όλα τα δεδομένα φιλτράρονται από το Cisco Firewall Firepower πριν εισέλθουν στο δίκτυο της εταιρείας (A.12.2.1, A.13.2.1).

Υπάρχουν κατάλληλοι έλεγχοι πρόσβασης (λ.χ. δικαιώματα διαχειριστή / χρήστη) προκειμένου να αποφευχθεί ο κακόβουλος και ο κινητός κώδικας, καθώς και η εγκατάσταση λογισμικού από τους χρήστες.

Ο κώδικας κινητής τηλεφωνίας αντιπροσωπεύει νεότερες τεχνολογίες που βρίσκονται συχνά σε ιστοσελίδες και ηλεκτρονικά ταχυδρομεία και περιλαμβάνει ιδίως:

- ActiveX
- Java
- JavaScript
- VBScript
- Macros
- HTTPs
- HTML

Οι κινητές συσκευές στις οποίες έχει εγκατασταθεί εταιρικό email έχουν κωδικό κλειδώματος στη συσκευή. Επίσης, στη συσκευή μπορεί να γίνει απομακρυσμένη διαγραφή των δεδομένων λόγω της υπηρεσίας Exchange.

Το προσωπικό της εταιρείας είναι υπεύθυνο να μην εισάγει κακόβουλο κώδικα στα συστήματα πληροφορικής της εταιρείας.

Σε περίπτωση ανίχνευσης ενός ιού σε σύστημα της εταιρείας, το προσωπικό ενημερώνει το τμήμα IT.

Όλοι οι διακομιστές εφαρμόζουν τις κατάλληλες κρίσιμες ενημερωμένες εκδόσεις ασφαλείας μόλις καταστούν διαθέσιμες και έχουν περάσει τη δοκιμή αποδοχής του συστήματος. Όλα τα άλλα patches εφαρμόζονται ανάλογα με την περίπτωση (A.12.2.1).

Τα ενημερωτικά δελτία εφαρμόζονται σε όλο το λογισμικό στο δίκτυο οργάνωσης που χρειάζεται.

Υπάρχει πλήρης καταγραφή των επιδιορθώσεων που έχουν εφαρμοσθεί και του χρόνου εφαρμογής τους.

Οι αιτήσεις εγκατάστασης λογισμικού γίνονται αποδεκτές μόνον εφόσον υπάρχει σαφής τεχνική επαλήθευση και κατόπιν αιτήσεως στο τμήμα IT.

Το λογισμικό κατά του κατάβουλου λογισμικού εγκαθίσταται σε κατάλληλα σημεία στο δίκτυο και στους υπολογιστές των πωλητών.

4.10.4 Δημιουργία αντιγράφων ασφαλείας.

(A.12.3.1)

Η εταιρεία λαμβάνει καθημερινώς αντίγραφα σημαντικών επιχειρηματικών πληροφοριών (μέσω ενός κατάλληλου κύκλου back-up, πλήρως τεκμηριωμένου), ώστε να διασφαλιστεί η δυνατότητα ανάκαμψης από καταστροφή, απόσπαση μέσων ή σφάλμα.

Εάν κριθεί απαραίτητο, επιπλέον των ημερήσιων back-ups, γίνονται εβδομαδιαία ή μηνιαία back-ups για συγκεκριμένα στοιχεία.

Αντίγραφα ασφαλείας πρέπει να δημιουργούνται και για πληροφορίες που τυχόν αποθηκεύονται από τρίτα μέρη.

Η απομακρυσμένη τοποθεσία είναι επαρκώς απομακρυσμένη ώστε να αποφεύγεται οποιαδήποτε καταστροφή τυχόν συμβεί στον κύριο χώρο.

Όπου απαιτείται, εκτελούνται τακτικές αποκαταστάσεις πληροφοριών από αντίγραφα ασφαλείας, ώστε να διασφαλίζεται η αξιοπιστία των μέσων δημιουργίας αντιγράφων και της διαδικασίας επαναφοράς.

Η εταιρεία λαμβάνει back-ups με τη χρήση ειδικών προγραμμάτων. Το τμήμα IT, χρησιμοποιώντας αυτά τα προγράμματα, αποθηκεύει τα back-ups σε εξωτερικούς HDD. Αυτοί οι δίσκοι αλλάζουν καθημερινά (εκτός Σαββάτου και Κυριακής) και μεταφέρονται σε ασφαλές μέρος, εκτός των εγκαταστάσεων της εταιρείας, μαζί με τις τεκμηριώσεις τους. Παράλληλα, δημιουργείται καθημερινό back-up, κατά το οποίο τα δεδομένα που υπάρχουν στο site της Θεσσαλονίκης μεταφέρονται μέσω ασφαλούς γραμμής VPN σε κεντρικό server στην Αθήνα και αντίστροφα τα δεδομένα της Αθήνας σε κεντρικό server της Θεσσαλονίκης. Έτσι εξασφαλίζεται ότι υπάρχει και γεωγραφικό back-up. Μαζί με αυτές τις τεκμηριώσεις γίνεται και μία πλήρης καταγραφή όσων έχουν δημιουργηθεί μαζί με τη διαδικασία της ανάκτησης. Όλες οι διαδικασίες επιβλέπονται καθημερινά από το τμήμα IT, το οποίο επικυρώνει το back-up των αρχείων. Αντίγραφο των τεκμηριώσεων τηρείται και στην κεντρική τοποθεσία.

4.10.5 Χειρισμός μέσων αποθήκευσης.

Τα μέσα αποθήκευσης περιλαμβάνουν ιδίως:

- Σκληρούς δίσκους υπολογιστών (εσωτερικούς και εξωτερικούς)
- DVD
- Οπτικούς δίσκους

Το τμήμα IT ή οποιοδήποτε άλλο τμήμα της εταιρείας δημιουργεί ειδική τεκμηρίωση ιδίως για εφαρμογές, μεθόδους, διαδικασίες, δομές δεδομένων και στοιχεία εξουσιοδότησης. Στην ειδική τεκμηρίωση δεν περιλαμβάνονται τυχόν γενικά εγχειρίδια που έχουν παρασχεθεί με το λογισμικό. Η τεκμηρίωση του συστήματος προστατεύεται από μη εξουσιοδοτημένη πρόσβαση.

Τα αποθηκευτικά μέσα που μεταφέρονται (εξωτερικοί δίσκοι για back-up) διατηρούνται σε ασφαλές περιβάλλον, στο οποίο πρόσβαση έχουν μόνο ο IT manager και ο CTO, ώστε να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση, κατάχρηση ή φθορά (A.6.1.5).

Γίνονται κατάλληλες ρυθμίσεις προκειμένου να εξασφαλισθεί η μελλοντική διαθεσιμότητα των δεδομένων (πέρα από τη διάρκεια ζωής των μέσων δημιουργίας αντιγράφων ασφαλείας).

Όπου απαιτούνται υπηρεσίες ταχυμεταφορών, υπάρχει συνεργασία με συγκεκριμένες έμπιστες και αξιόπιστες εταιρείες ταχυμεταφορών (couriers), που έχουν εγκριθεί από το αρμόδιο τμήμα της εταιρείας. Σε κάθε περίπτωση, διασφαλίζεται η τοποθέτηση του μέσου αποθήκευσης σε κατάλληλο πακέτο και η προστασία του από τη ζέστη και την υγρασία (A.8.3.3).

Όπου απαιτείται, εφαρμόζονται φυσικοί έλεγχοι, λ.χ. κρυπτογράφηση Bit Locker ή ειδικά κλειδωμένα δοχεία (A.6.1.5, A.8.3.1).

Τα μέσα αποθήκευσης που δεν χρειάζονται πλέον καταστρέφονται με low level format (αντικατάσταση δεδομένων με μηδενικά), προκειμένου να αποφευχθεί η διαρροή δεδομένων, ή καταστρέφονται με φυσικό τρόπο και μεταφέρονται στην ανακύκλωση από το τμήμα IT (A.8.3.2).

Αν η εταιρεία κρίνει ότι κάποια δεδομένα ενδέχεται να χρειάζονται για μελλοντική χρήση, τα αποθηκεύει σε συγκεκριμένο σημείο περιορισμένης πρόσβασης, ώστε να αποφευχθεί η αλλοίωσή τους λόγω μακροχρόνιας αδράνειας του μέσου ή κλοπής του (A.8.3.1).

Ο αποτελεσματικός έλεγχος της έκδοσης εφαρμόζεται σε όλη την τεκμηρίωση και αποθήκευση τεκμηρίωσης.

4.10.6 Καταγραφή ελέγχου.

Τα αρχεία καταγραφής ελάχιστων ελέγων περιέχουν τις εξής πληροφορίες (A.12.4.1):

- Ταυτότητα συστήματος
- Ταυτότητα χρήστη
- Επιτυχής / μη επιτυχής σύνδεση
- Επιτυχής / μη επιτυχής αποσύνδεση
- Μη εξουσιοδοτημένη πρόσβαση σε ερφαρμογές
- Αλλαγές στις διαμορφώσεις του συστήματος
- Χρήση προνομιούχων λογαριασμών (π.χ. διαχείριση λογαριασμού, αλλαγές πολιτικής, διαμόρφωση συσκευών).

Αρχεία καταγραφής ελέγχου, τα οποία καταγράφουν εξαιρέσεις και άλλα συμβάντα που σχετίζονται με την ασφάλεια, τηρούνται τουλάχιστον τρεις (3) μήνες (A.12.4.2).

Η πρόσβαση στα αρχεία καταγραφής προστατεύεται από μη εξουσιοδοτημένη πρόσβαση, ώστε να αποτρέπεται η αλλοίωση ή διαγραφή εγγραφών μέσω του περιορισμού των δικαιωμάτων

διαχειριστή. Αναφορικά με την εξωτερική απειλή, τα αρχεία καταγραφής προστατεύονται από λογισμικά προστασίας κατά των ιών και από το hardware firewall (A.12.4.2).

Οι διαχειριστές συστημάτων δεν διαγράφουν ή απενεργοποιούν τα αρχεία καταγραφής της δικής τους δραστηριότητας (A.12.4.3).

Το επιχειρησιακό προσωπικό και οι διαχειριστές συτσημάτων τηρούν αρχείο των δραστηριοτήτων τους.

Το αρχείο δραστηριοτήτων διαχειριστή περιλαμβάνει:

- Τον χρόνο έναρξης και λήξης συμβάντος συστήματος, καθώς και τον εμπλεκόμενο.
- Το είδος, την ημερομηνία και την ώρα των σφαλμάτων συστήματος, καθώς και τις διορθωτικές ενέργειες που λαμβάνουν χώρα.

Τα αρχεία καταγραφής ελέγχονται τακτικά, ώστε να εξασφαλίζεται η τήρηση των ορθών διαδικασιών.

Όλα τα ρολόγια υπολογιστή συγχρονίζονται με την πηγή ώρας GSI, για να διασφαλίζεται η ακρίβεια όλων των αρχείων καταγραφής ελέγχου συστημάτων, καθώς μπορεί να χρειαστούν για την έρευνα περιστατικών (A.12.4.4).

4.10.7 Διαχείριση δικτύου.

(A.9.1.2)

Η διαχείριση δικτύου είναι κρίσιμη για την παροχή υπηρεσιών οργάνωσης.

Οι συνδέσεις με την υποδομή δικτύου της εταιρείας πραγματοποιούνται με ελεγχόμενο τρόπο.

Υπάρχουν δύο (2) ασύρματα δίκτυα WiFi στην εταιρεία. Ένα ξεχωριστό δίκτυο για τους επισκέπτες και συνεργάτες και ένα για το προσωπικό. Και τα δύο (2) δίκτυα ελέγχονται ως προς τη ροή των δεδομένων του δικτύου και αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση (A.13.1.3).

Όπου είναι δυνατόν, υπάρχει ξεχωριστή επιχειρησιακή ευθύνη για τα δίκτυα από δραστηριότητες ηλεκτρονικών υπολογιστών (A.13.1.1).

Υπάρχουν σαφείς ευθύνες και διαδικασίες για τη διαχείριση απομακρυσμένου εξοπλισμού και χρηστών.

Όπου ενδείκνυται, τοποθετούνται έλεγχοι για να προστατεύονται τα δεδομένα που περνούν μέσω του δικτύου (π.χ. κρυπτογράφηση) (A.13.1.1).

Η αρχιτεκτονική του δικτύου καταγράφεται και αποθηκεύεται, μαζί με τις ρυθμίσεις διαμόρφωσης όλων των στοιχείων υλικού και λογισμικού που αποτελούν το δίκτυο, σε ένα μητρώο στοιχείων μέσω της εφαρμογής Asset Management.

Όλοι οι κεντρικοί υπολογιστές έχουν αυξήσει την ασφάλεια σε κατάλληλο επίπεδο.

Οι υπηρεσίες δικτύου των λειτουργικών συστημάτων έχουν απενεργοποιήσει τις υπηρεσίες που δεν απαιτούνται.

Στα ασύρματα δίκτυα εφαρμόζεται κρυπτογράφηση WPA2, ώστε να αποφεύγεται η παρακράτηση πληροφοριών (A.13.1.1).

4.11 Ασφάλεια χαρτιού και εξοπλισμού.

Στις πληροφορίες που βρίσκονται σε χαρτί (φυσική μορφή) καθώς και σε παρόμοιες μη ηλεκτρονικές πληφορίες υπάρχει ένας κάτοχος και μια ταξινόμηση. Εάν χαρακτηρίζονται ως ευαίσθητες, τίθενται σε εφαρμογή οι έλεγχοι ασφαλείας της πληροφορίας για την προστασία τους.

Τα έγγραφα σε ένα ανοικτό γραφείο προστατεύονται από τους ελέγχους που προβλέπονται για το κτίριο και μέσω κατάλληλων μέτρων, που περιλαμβάνουν ιδίως:

- Ντουλάπια αρχειοθέτησης που κλειδώνονται με κλειδιά, τα οποία αποθηκεύοται μακριά από το ντουλάπια.
- Κλειδωμένα χρηματοκιβώτια.
- Αποθήκευση σε ασφαλή περιοχή που προστατεύεται από τα στοιχεία ελέγχου πρόσβασης.

Όλος ο γενικός εξοπλισμός πληροφορικής βρίσκεται σε κατάλληλες φυσικές τοποθεσίες (A.11.2.1) που:

- Είναι περιορισμένες από περιβαλλοντικούς κινδύνους, π.χ. θερμότητα, πυρκαγιά, καπνό, νερό, σκόνη και δονήσεις.
- Περιορίζεται ο κίνδυνος κλοπής, π.χ. όλοι οι φορητοί υπολογιστές είναι κλειδωμένοι με Bit Locker.
- Οι σταθμοί εργασίας που χειρίζονται ευαίσθητα δεδομένα διαχωρίζονται, ώστε να αποφεύγεται ο κίνδυνος της προβολής της πληροφορίας σε μη εξουσιοδοτημένα άτομα.

Τα δεδομένα αποθηκεύονται στους διακομιστές αρχείων δικτύου, όπου χρειάζεται. Επίσης, τα έγγραφα της διοίκησης αποθηκεύονται στο λογιστήριο ή στο χρηματοκιβώτιο, αναλόγως της περίπτωσης. Αυτό διασφαλίζει ότι οι πληροφορίες που έχουν χαθεί, κλαπεί ή καταστραφεί μέσω μη εξουσιοδοτημένης πρόσβασης μπορούν να ανακτηθούν, με την ακεραιότητά τους να διατηρείται.

Όλοι οι servers που βρίσκονται εκτός του κέντρου δεδομένων βρίσκονται σε φυσικό ασφαλές περιβάλλον ή σε προστατευμένους servers Azure της Microsoft.

Τα κρίσιμα για την επιχείρηση συστήματα προστατεύονται από ένα μη διακοπτόμενο τροφοδοτικό (UPS), προκειμένου να μειωθεί το λειτουργικό σύστημα και ο κίνδυνος απώλειας ή φθοράς δεδομένων από αποτυχίες της τροφοδοσίας ρεύματος (A.11.2.2).

Όλα τα είδη εξοπλισμού καταγράφονται σε κατάλογο, τόσο στο τμήμα IT (μέσω του IT Asset Management System) (A.8.1.2), όσο και στο τμήμα Οικονομικών (πάγια περιουσιακά στοιχεία).

Όταν η εταιρεία αποκτά ένα νέο περιουσιακό στοιχείο ή επιθυμεί να αφαιρέσει ένα παλιό, ο προϊστάμενος του συγκεκριμένου τμήματος του στοιχείου ενημερώνει το τμήμα IT και το τμήμα Οικονομικών, προκειμένου να ενημερώσουν τα σχετικά αρχεία τους. (A.11.1.6).

Υπάρχουν διαδικασίες για την ενημέρωση των αποθεμάτων, μόλις ληφθούν ή διατεθούν τα περιουσιακά στοιχεία (A.11.1.6).

Όλος ο εξοπλισμός φέρει ασφάλεια και έχει έναν μοναδικό αριθμό ενεργητικού, ο οποίος αντιστοιχεί στον σειριακό αριθμό (serial number) του εκάστοτε προϊόντος. Αυτός ο αριθμός του ενεργητικού καταγράφεται στο IT Asset Management System.

Τα καλώδια που μεταφέρουν δεδομένα ή υποστηρίζουν βασικές υπηρεσίες πληροφοριών προστατεύονται από την υποκλοπή ή τη ζημία.

Τα καλώδια τροφοδοσίας διαχωρίζονται από τα καλώδια δικτύου, προκειμένου να αποφεύγονται παρεμβολές (A.11.2.3).

Τα καλώδια δικτύου προστατεύονται με αγωγούς και, όπου είναι δυνατόν, αποφεύγονται διαδρομές μέσω δημόσιων χώρων (A.11.2.3).

4.12 Διαχείριση του κύκλου ζωής του εξοπλισμού.

(A.11.2.4)

Το τμήμα IT και οι τρίτοι προμηθευτές διασφαλίζουν ότι όλος ο εξοπλισμός πληροφορικής της EPSILON NET συντηρείται σύμφωνα με τις οδηγίες του κατασκευαστή και με τυχόν τεκμηριωμένες εσωτερικές διαδικασίες, ώστε να διασφαλισθεί ότι παραμένει σε κατάσταση λειτουργίας.

Το προσωπικό που ασχολείται με τη συντήρηση:

- Διατηρεί όλα τα αντίγραφα των οδηγιών του κατασκευαστή.
- Προσδιορίζει τα συνιστώμενα διαστήματα και τις προδιαγρές συντήρησης.
- Ενεργοποιεί μια διαδικασία κλήσης σε περίπτωση αποτυχίας.
- Διασφαλίζει ότι μόνον οι εξουσιοδοτημένοι τεχνικοί ολοκληρώνουν οποιαδήποτε εργασία στον εξοπλισμό.
- Καταγράφει τις λεπτομέρειες όλων των διορθωτικώνεργασιών που πραγματοποιήθηκαν.
- Προσδιορίζει τυχόν ασφαλιστικές απαιτήσεις.
- Καταγράφει τις λεπτομέρειες των ελαττωμάτων και των απαιτούμενων ενεργειών και τηρείται αρχείο.

Τηρείται αρχείο ιστορικού συντήρησης (service) του εξοπλισμού, ώστε όταν ο εξοπλισμός τείνει να γίνει παλαιότερος, λαμβάνονται αποφάσεις σχετικά με τον κατάλληλο χρόνο αντικατάστασής του.

Η συντήρηση του εξοπλισμού είναι σύμφωνη με τις οδηγίες του κατασκευαστή, οι οποίες είναι τεκμηριωμένες και διαθέσιμες για να χρησιμοποιηθούν από το προσωπικό υποστήριξης κατά την οργάνωση των επισκευών.

Η χρήση του εξοπλισμού εκτός του χώρου πρέπει να εγκριθεί επίσημα από τον διευθυντή του χρήστη (A.11.2.6).

Στον εξοπλισμό που πρόκειται να επαναχρησιμοποιηθεί ή να απορριφθεί έχουν διαγραφεί / καταστραφεί όλα τα δεδομένα και το λογισμικό του (A.11.2.6, A.11.2.7).

Εάν ο εξοπλισμός αφορά φορητούς υπολογιστές γίνεται πλήρης κρυπτογράφηση δίσκου με την υπηρεσία Bit Locker πριν από τη χρήση τους εκτός της εταιρείας (A.11.2.7).

Εάν ο εξοπλισμός πρόκειται να μεταβιβασθεί σε έναν άλλο οργανσιμό (λ.χ. για την εκπόνηση σεμιναρίων), η απομάκρυνση των δεδομένων και των εφαρμογών με άδεια χρήσης επιτυγχάνεται χρησιμοποιώντας επαγγελματικό λογισμικό για αφαίρεση δεδομένων ή πραγμτοποιώντας πλήρη διαγραφή του λειτουργικού (computer format) (A.11.2.6, A.11.2.7).

Τα μέσα ή οι υπηρεσίες λογισμικού καταστρέφονται για να αποφευχθεί η πιθανότητα ακατάλληλης χρήσης που θα μπορούσε να παραβιάσει τους όρους και τις προϋποθέσεις των αδειών που τηρούνται.

Προκειμένου να επιβεβωθεί η ακρίβεια και η καταάσταση των παραδόσεων και να αποφευχθεί η απώλεια ή κλοπή αποθηκευμένου εοπλισμού, εφαρμόζονται τα εξής:

- Οι παραδόσεις εξοπλισμού υπογράφονται από εξουσιοδοτημένο άτομο χρησιμοποιώντας μια ελεγχόμενη τυπική διαδικασία. Η διαδικασία αυτή επιβεβαιώνει ότι τα παραλαμβανόμενα αντικείμενα αντιστοιχούν πλήρως στον κατάλογο του δελτίου παράδοσης (A.11.1.6).
- Οι χώροι φόρτωσης και οι χώροι αποθήκευσης είναι επαρκώς ασφαλισμένοι με την επίβλεψη του φρουρού ασφαλείας έναντι μη εξουσιοδοτημένης πρόσβασης και κάθε πρόσβαση είναι ελεγχόμενη (A.11.1.6).
- Η μεταγενέστερη κατάργηση του εξοπλισμού γίνεται μέσω επίσημης και ελεγχόμενης διαδικασίας.

Υπάρχει υποχρέωση ελέγχου των ρυθμίσεων για την ασφάλεια των πληροφοριών σε τακτική βάση, ώστε να απρέχεται ανεξάρτητη εκτίμηση και να προτείνονται βελτιώσεις ασφαλείας, όπου χρειάζεται.

Για κάθε εξοπλισμό υπάρχει ο κάτοχος (Owner of asset). Ο κάτοχος είναι υπεύθυνος ενημερώσει το τμήμα IT σε περίπτωση που διαπιστώσει κάποιο πρόβλημα στον εξοπλισμό ή επιθυμεί να αλλάξει κάτι στη λειτουργία του (A.8.1.2).

4.13 Προμήθεια, ανάπτυξη και συντήρηση συστημάτων.

Κατά την προμήθεια ή ανάπτυξη νέων συστημάτων ή την επέκταση / αναβάθμιση υφιστάμενων συστημάτων, η εταιρεία μεριμνά για τη διατήρηση του επιπέδου ασφάλειας των πληροφοριακών της πόρων συμπεριλαμβάνοντας, μεταξύ άλλων:

- Τις σχετικές απαιτήσεις ασφάλειας στις προδιαγραφές των συστημάτων.
- Όρους σχετικά με την ασφάλεια στις συμβάσεις με τους προμηθευτές των συστημάτων.
- Σενάρια ελέγχου σχετικά με την ασφάλεια των συστημάτων στις δοκιμές των συστημάτων, πριν αυτά τεθούν σε παραγωγική λειτουργία.

Εάν χρησιμοποιούνται προσωπικές πληροφορίες κατά την ανάπτυξη και τη δοκιμή της προετοιμασίας του λογισμικού εφαρμογών, αυτές προστατεύονται σύμφωνα με τη νομοθεσία περί προστασίας προσωπικών δεδομένων και, όπου είναι δυνατόν, ανωνυμοποιούνται.

Εάν χρησιμοποιούνται λειτουργικά δεδομένα, πραγματοποιούνται έλεγχοι που περιλαμβάνουν, μεταξύ άλλων, τα ακόλουθα:

- Διαδικασία εξουσιοδότησης
- Αφαίρεση όλων των λειτουργικών δεδομένων από το σύστημα δοκιμής μετά τη χρήση
- Πλήρης διαδρομή ελέγχου σχετικών δραστηριοτήτων.

4.14 Λογισμικό.

Η εταιρεία χρησιμοποιεί λογισμικό σε όλες τις πτυχές των δραστηριοτήτων της, προκειμένου να υποστηρίξει το έργο που επιτελούν οι υπάλληλοί της.

Σε κάθε περίπτωση, το λογισμικό απαιτείται να έχει άδεια και να έχει αποκτηθεί από γνωστούς και αξιόπιστους προμηθευτές για να διασφαλισθεί η νομιμότητα του προϊόντος (A.18.1.2).

Όλες οι άδειες, δίσκοι εγκατάστασης ή ηλεκτρονικά αρχεία εγκατάστασης και οι οδηγίες χρήσης αποθηκεύονται σε συγκεκριμένο αποθηκευτικό χώρο ή ηλεκτρονικό φάκελο και η πρόσβαση σε αυτά περιορίζεται μόνο στο τμήμα IT ή τη Διοίκηση (A.18.1.2).

Οι τρόποι απόκτησης λογισμικού περιορίζονται για να εξασφαλίσουν ότι η εταιρεία έχει πλήρη καταγραφή όλων των λογισμικών που έχουν αγορασθεί για τους υπολογιστές της και μπορεί να καταχωρίσει, υποστηρίξει και αναβαθμίσει το λογισμικό ανάλογα.

Αυτό περιλαμβάνει λογισμικό που μπορεί να μεταφορτωθεί ή/και να αγορασθεί από το διαδίκτυο (A.12.6.2).

Αυτό το λογισμικό ανήκει στην εταιρεία λογισμικού και η αντιγραφή αυτού του λογισμικού αποτελεί αδίκημα σύμφωνα με τον νόμο περί δικαιωμάτων πνευματικής ιδιοκτησίας, σχεδίων και διπλωμάτων ευρεσιτεχνίας του 1988, εκτός εάν εξουσιοδοτηθεί από τον κατασκευαστή του λογισμικού (A.12.6.2, A.18.1.2).

Το λογισμικό κοινής χρήσης λογισμικού, το δωρεάν λογισμικό και το δημόσιο Domain δεσμεύονται από τις ίδιες πολιτικές και διαδικασίες, όπως και το υπόλοιπο λογισμικό.

Όλα τα λογισμικά που έχουν αποκτηθεί από την εταιρεία αγοράζονται μέσω του IT Manager ή του CTO.

Το τμήμα IT διατηρεί μητρώο όλων των λογισμικών και των στοιχείων της εταιρείας, όπως και βιβλιοθήκη αδειών λογισμικού. Το μητρώο περιέχει: (α) Τον τίτλο και τον εκδότη του λογισμικού. (β) Την ημερομηνία και την πηγή απόκτησης του λογισμικού. (γ) Τη θέση κάθε εγκατάστασης καθώς και τον σειριακό αριθμό του υλικού στο οποίο είναι εγκατεστημένο κάθε αντίγραφο του λογισμικού. (δ) Τον σειριακό αριθμό του προϊόντος λογισμικού, όπου υπάρχει. (ε) Λεπτομέρειες και διάρκεια των ρυθμίσεων υποστήριξης για αναβαθμίσεις λογισμικού.

Το λογισμικό σε τοπικά δίκτυα ή σε πολλαπλά μηχανήματα χρησιμοποιείται μόνο σύμφωνα με τη σύμβαση της άδειας χρήσης (A.18.1.2).

Το λογισμικό εγκαθίσταται μόνο από το τμήμα IT μόλις πληρούνται οι απαιτήσεις εγγραφής (A.12.6.2).

Όλες οι αλλαγές στο λογισμικό εγκρίνονται μόνον από τον IT Manager ή τον CTO πριν από την εφαρμογή της αλλαγής (A.12.6.2).

Η εταιρεία, μέσω των Active Directory Policies, δεν επιτρέπει την εγκατάσταση προσωπικού λογισμικού στους υπολογιστές των τμημάτων. Επίσης, δεν επιτρέπει συγκεκριμένες ρυθμίσεις που αφορούν στην ασφάλεια των σταθμών εργασίας (χρόνος screen saver, αλλαγή κωδικών) (A.12.6.2).

Σε περίπτωση που ένας σταθμός εργασίας έχει δικαίωμα τοπικού διαχειριστή (local admin rights), ο χρήστης ενημερώνει το τμήμα IT για το λογισμικό που επιθυμεί να εγκαταστήσει (A.12.6.2).

Λόγω του κύκλου εργασιών του προσωπικού, το λογισμικό δεν καταχωρίζεται ποτέ στο όνομα του μεμονωμένου χρήστη. Το λογισμικό καταχωρίζεται στην εταιρεία (A.18.1.2).

Το λογισμικό δεν αλλάζει ή μεταβάλλεται από οποιονδήποτε χρήστη, εκτός αν υπάρχει σαφής επιχειρησιακή ανάγκη και μετά από έγκριση του IT Manager ή του CTO.

Οποισδήποτε χρήστης λογισμικού της εταιρείας δημιουργεί, αποκτά ή χρησιμοποιεί μη εξουσιοδοτημένα αντίγραφα λογισμικού, θα υφίσταται ανάλογες κυρώσεις. Η εταιρεία δεν εγκρίνει την παράνομη αλληλοεπικάλυψη λογισμικού και προβαίνει σε κυρώσεις ανάλογα με τη σοβαρότητα της αλληλοεπικάλυψης (A.7.2.3, A.18.1.2).

4.15 Ετήσιος διαγνωστικός έλεγχος.

Ετησίως δημιουργείται ένας έλεγχος υγείας όλων των συστημάτων και εγκαταστάσεων υποδομής πληροφορικής (Α.12.6.1). Αυτός ο έλεγχος υγείας περιλαμβάνει. Μεταξύ άλλων, τα ακόλουθα:

- Πλήρη δοκιμή διείσδυσης (Α.18.2.1, Α.18.2.3).
- Περίληψη δικτύου με εντοπισμό όλων των συσκευών που έχουν διεύθυνση IP.
- Ανάλυση δικτύου, συμπεριλαμβανομένων των εκμεταλλεύσιμων δικοπτών και πυλών.
- Ανάλυση ευπάθειας, συμπεριλαμβανομένων των επιπέδων των επιδιορθώσεων, των κακών κωδικών πρόσβασης και των χρησιμοποιούμενων υπηρεσιών (Α.18.2.3).
- Ανάλυση αξιοποίησης.
- Συνοπτική έκθεση με συστάσεις για βελτίωση (Α.18.2.3).

4.16 Σχέσεις με προμηθευτές.

Στις περιπτώσεις που προμηθευτές της εταιρείας αποκτούν πρόσβαση σε πόρους της εταιρείας, η πρόσβαση αυτή διέπεται από συγκεκριμένους όρους και μόνο για τους προβλεπόμενους από τη συνεργασία σκοπούς.

Η εταιρεία ενημερώνει τους προμηθευτές της για τις υποχρεώσεις τους όσον αφορά στην προστασία των πληροφοριακών της πόρων. Αντίστοιχα, οι προμηθευτές οφείλουν να συμμορφώνονται με τις σχετικές προβλέψεις της πολιτικής ασφάλειας της εταιρείας.

4.17 Διαχείριση περιστατικών ασφάλειας πληροφοριών.

Όλα τα στελέχη της EPSILON NET, ανεξάρτητα από τη θέση τους στην ιεραρχία και του ρόλου τους στην εταιρεία, οφείλουν να αναφέρουν κάθε περιστατικό που σχετίζεται με υποψία παραβίασης καθ’ οιονδήποτε τρόπο της ασφάλειας των πληροφοριακών πόρων της εταιρείας. Αντίστοιχη υποχρέωση έχουν και τρίτα μέρη (συνεργάτες και προμηθευτές).

Για τον σκοπό αυτό, η Διοίκηση της EPSILON NET έχει θεσπίσει κατάλληλη διαδικασία αναφοράς περιστατικών ασφάλειας, την οποία έχει γνωστοποιήσει σε όλους τους εμπλεκόμενους. Επίσης, η διερεύνηση των περιστατικών ασφάλειας γίνεται από κατάλληλο προσωπικό της εταιρείας μέσω σχετικής διαδικασίας, από την οποία καθορίζονται, όπου απαιτείται, τα μέτρα ασφάλειας που πρέπει να ληφθούν.

4.17.1 Σημείο αναφοράς περιστατικών ασφαλείας.

Ως αρμόδιο σημείο επαφής για την αναφορά περιστατικών διακύβευσης της ασφάλειας των πληροφοριακών πόρων της εταιρείας έχει οριστεί από τη Διοίκηση της εταιρείας ο Υπεύθυνος

Ασφάλειας Πληροφοριών / Προσωπικών Δεδομένων. Τα στοιχεία επικοινωνίας (τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου) του ΥΑΠ/ΠΔ έχουν γνωστοποιηθεί στο προσωπικό και τους συνεργάτες της εταιρείας.

4.17.2 Τρόπος αναφοράς περιστατικών ασφαλείας.

Τα περιστατικά διακύβευσης της ασφάλειας των πληροφοριακών πόρων της εταιρείας αναφέρονται στον ΥΑΠ/ΠΔ: (α) ηλεκτρονικά, μέσω αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου, (β) έντυπα ή (γ) τηλεφωνικά, σε εξαιρετικές περιπτώσεις (π.χ. ιδιαίτερα σοβαρά συμβάντα).

4.17.3 Αναφορά και αντιμετώπιση περιστατικών και αδυναμιών ασφαλείας πληροφοριών.

Όλα τα στελέχη της εταιρείας, ανεξάρτητα από τη θέση τους στην ιεραρχία και του ρόλου τους στην εταιρεία, καθώς και οι συνεργάτες της εταιρείας, οφείλουν να αναφέρουν στον ΥΑΠ/ΠΔ κάθε περιστατικό που σχετίζεται με υποψία παραβίασης, καθ' οιονδήποτε τρόπο, της ασφάλειας των πληροφοριακών πόρων της εταιρείας. Η διαδικασία που ακολουθείται για τον σκοπό αυτό περιλαμβάνει τα παρακάτω βήματα:

I. Κάθε στέλεχος (διοίκηση, διαχειριστής, προσωπικό, τεχνικός ή χρήστης, συνεργάτης) της εταιρείας που εντοπίζει -ή έχει υποψία για- ένα συμβάν ασφάλειας οφείλει να ενημερώσει αμέσως τον ΥΑΠ/ΠΔ. Οι αναφορές ενός συμβάντος από το στέλεχος που το εντόπισε στον ΥΑΠ/ΠΔ πρέπει να είναι κατά το δυνατό τεκμηριωμένες και να περιλαμβάνουν στοιχεία όπως ημερομηνία, ώρα, περιγραφή κλπ.
II. Ο ΥΑΠ/ΠΔ εξετάζει και αξιολογεί τις αναφορές συμβάντων ασφάλειας σε συνεργασία με τα κατάλληλα στελέχη (π.χ. διαχειριστές συστημάτων).
III. Τα περιστατικά ασφάλειας χαρακτηρίζονται από τον ΥΑΠ/ΠΔ, ανάλογα με τις επιπτώσεις τους στην εταιρεία, ως εξής:
    a. Σοβαρά, εάν στις επιπτώσεις τους περιλαμβάνονται:
        i. Η απώλεια ιδιαίτερα υψηλής αξίας στοιχείων της υλικοτεχνικής και τεχνολογικής υποδομής ή άλλων σημαντικών άυλων πόρων της εταιρείας.
        ii. Η επίτευξη καίριου πλήγματος στο κύρος και τη δημόσια εικόνα της εταιρείας.
        iii. Η απώλεια ανθρώπινων ζωών ή η πρόκληση σοβαρών τραυματισμών.
    b. Σημαντικά, εάν στις επιπτώσεις τους περιλαμβάνονται:

i. Η απώλεια υψηλής αξίας στοιχείων της υλικοτεχνικής και τεχνολογικής υποδομής ή άλλων σημαντικών άυλων πόρων της εταιρείας.

ii. Η επίτευξη σημαντικού πλήγματος στο κύρος και τη δημόσια εικόνα της εταιρείας.

iii. Η πρόκληση τραυματισμών του ανθρωπίνου δυναμικού.

c. Χαμηλής σπουδαιότητας, εάν στις επιπτώσεις τους περιλαμβάνονται:

i. Η απώλεια χαμηλής αξίας στοιχείων της υλικοτεχνικής και τεχνολογικής υποδομής ή άλλων άυλων πόρων της εταιρείας.

ii. Η επίτευξη μικρού πλήγματος στο κύρος και τη δημόσια εικόνα της εταιρείας.

d. Ασήμαντα, εάν είχαν ελάχιστες ή καμία επίπτωση στους πληροφοριακούς πόρους της εταιρείας.

IV. Εάν υπήρξαν παραβιάσεις της ασφάλειας, ο ΥΑΠ/ΠΔ αναζητά τις αιτίες και μεριμνά για την αποκατάσταση τυχόν προβλημάτων που δημιουργήθηκαν. Παράλληλα εξετάζει πιθανούς τρόπους και μέτρα προστασίας από αντίστοιχες μελλοντικές απόπειρες παραβίασης της ασφάλειας.

V. Τα περιστατικά ασφάλειας, σε συνδυασμό με τις ενέργειες επίλυσής τους, καθώς και προτάσεις για βελτίωση των μέτρων ασφάλειας (όπου έχει εφαρμογή) καταγράφονται.

Σε περίπτωση που κρίνεται σκόπιμο, ο ΥΑΠ/ΠΔ δύναται να αποφασίσει τη σύσταση μικρής ομάδας με στόχο τη διερεύνηση του περιστατικού ή να αναθέσει τη συγκεκριμένη εργασία σε κάποιο στέλεχος της εταιρείας. Αντίστοιχα, δύναται να απευθυνθεί στις αρμόδιες Αρχές ή να έρθει σε επικοινωνία με ειδικές ομάδες σχετικά με την ασφάλεια πληροφοριών, προκειμένου να λάβει υποστήριξη στη διερεύνηση του περιστατικού.

Με την ίδια ως άνω διαδικασία, αναφέρονται από όλα τα στελέχη και συνεργάτες της εταιρείας στον ΥΑΠ/ΠΔ πιθανές αδυναμίες ασφάλειας των πληροφοριακών πόρων της εταιρείας.

4.17.4 Επισκόπηση περιστατικών ασφαλείας.

Ο ΥΑΠ/ΠΔ εξετάζει σε τακτά χρονικά διαστήματα τα περιστατικά ασφάλειας που έχουν καταγραφεί από τα στελέχη ή τους συνεργάτες της εταιρείας. Σε περίπτωση που ο ΥΑΠ/ΠΔ διαπιστώσει την εμφάνιση πολλών αντίστοιχων ή ομοειδών περιστατικών ασφάλειας, καταγράφει το γεγονός αυτό σε σχετική αναφορά την οποία προωθεί στη Διοίκηση της εταιρείας, μαζί με τις προτάσεις του για τη λήψη πρόσθετων μέτρων ασφάλειας.

Η Διοίκηση της εταιρείας αξιολογεί τις προτάσεις του ΥΑΠ/ΠΔ, κατά την τακτική ή έκτακτη συνεδρίασή της για την ανασκόπηση της πολιτικής ασφάλειας της εταιρείας, και αποφασίζει για τα πρόσθετα μέτρα ασφάλειας που πρέπει να ληφθούν. Στη συνέχεια, ο ΥΑΠ/ΠΔ αναλαμβάνει την ευθύνη για την υλοποίηση των επιπλέον μέτρων ασφάλειας. Εννοείται ότι η λήψη πρόσθετων μέτρων ασφάλειας ξεκινά έναν νέο κύκλο αναθεώρησης της πολιτικής ασφάλειας της εταιρείας.

4.17.5 Κυρώσεις.

Σε περίπτωση που η Διοίκηση της εταιρείας αποφασίσει να κινηθεί νομικά ή να επιβάλει κάποιου είδους κυρώσεις στον υπεύθυνο για την εκδήλωση ενός περιστατικού ασφάλειας, η εταιρεία ακολουθεί τις παρακάτω αρχές:

- Η εταιρεία, μέσω της εσωτερικής της οργάνωσης για τη διαχείριση της ασφάλειας των πληροφοριακών της πόρων ή/και με τη συμβολή εξωτερικών συνεργατών, διερευνά τα αίτια εκδήλωσης του περιστατικού ασφάλειας και επιχειρεί να το τεκμηριώσει κατά το δυνατό πληρέστερα. Στην τεκμηρίωση του περιστατικού περιλαμβάνονται απαραίτητα και αποδεικτικά στοιχεία που αποδίδουν την ευθύνη για την εκδήλωσή του σε κάποιο φυσικό ή νομικό πρόσωπο.
- Η αναλυτική τεκμηρίωση του περιστατικού ασφάλειας, μαζί με τα αποδεικτικά στοιχεία, παραδίδονται στους νομικούς συμβούλους της εταιρείας.
- Οι νομικοί σύμβουλοι της εταιρείας αναλαμβάνουν να κινήσουν τις όποιες νομικές διαδικασίες επιβολής κυρώσεων στον υπεύθυνο εκδήλωσης του περιστατικού, απαιτώντας πιθανώς σχετική αποζημίωση για τη ζημία που προκλήθηκε στην εταιρεία. Όλες οι ενέργειες των νομικών συμβούλων της εταιρείας τελούν υπό την έγκριση της Διοίκησης της εταιρείας.

4.18 Διαχείριση παραβίασης προσωπικών δεδομένων.

Η Διοίκηση της EPSILON NET έχει θεσπίσει κατάλληλη διαδικασία προκειμένου να εξασφαλίσει ότι:

- Περιστατικά data breach ανιχνεύονται, αναφέρονται και παρακολουθούνται τακτικά.
- Τα περιστατικά αξιολογούνται και αντιμετωπίζονται κατάλληλα.
- Γίνονται ενέργειες για τη μείωση των επιπτώσεων μιας παραβίασης.
- Οι σχετικές παραβιάσεις αναφέρονται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εντός εβδομήντα δύο (72) ωρών.
- Πραγματοποιούνται βελτιώσεις για την αποφυγή επανάληψης όμοιων περιστατικών.

- Η εμπειρία αντιμετώπισης του εν λόγω περιστατικού παραβίασης που αποκτήθηκε διαχέεται ευρύτερα εντός της εταιρείας.

4.18.1 Αναγνώριση ή υποψία παραβίασης προσωπικών δεδομένων.

Η παραβίαση των προσωπικών δεδομένων μπορεί να συμβεί για πολλούς λόγους, όπως για παράδειγμα:

- Απώλεια ή κλοπή δεδομένων ή εξοπλισμού στον οποίο αποθηκεύονται δεδομένα, ή μέσω των οποίων είναι δυνατή η πρόσβαση σε αυτά.
- Απώλεια ή κλοπή φυσικού αρχείου.
- Διαδικτυακές επιθέσεις.
- Ακατάλληλοι έλεγχοι πρόσβασης που επιτρέπουν μη εξουσιοδοτημένη / άσκοπη πρόσβαση στα δεδομένα.
- Αστοχία εξοπλισμού.
- Λανθασμένος ανθρώπινος χειρισμός.
- Απρόβλεπτες συνθήκες, όπως πυρκαγιά ή πλημμύρα.

4.18.2 Αναφορά περιστατικού.

Είναι ζωτικής σημασίας, μόλις εντοπιστεί ή υπάρξει υποψία παραβίασης προσωπικών δεδομένων, η εταιρεία να αναφέρει το περιστατικό αυτό, χωρίς αδικαιολόγητη καθυστέρηση, εντός εβδομήντα δύο (72) ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Προκειμένου να βελτιώσει την κατανόηση των κινδύνων για τα δεδομένα και να τα αντιμετωπίσει πριν συμβεί κάποια παραβίαση, πρέπει επίσης η εταιρεία να ενθαρρύνει τα άτομα να αναφέρουν αποσοβηθείσες παραβιάσεις (π.χ. περιστατικά που έχουν σχεδόν οδηγήσει σε παραβίαση δεδομένων, και απετράπησαν είτε από επιτυχημένη παρέμβαση είτε κατά «τύχη»). Οι αποσοβηθείσες παραβιάσεις αναφέρονται, με την ίδια μορφή και διαδικασία που αναφέρονται και οι πραγματικές παραβιάσεις και να επισημαίνεται με σαφήνεια ότι το περιστατικό αποτελεί μία αποσοβηθείσα παραβίαση.

Η γνωστοποίηση κατ' ελάχιστο: α) περιγράφει τη φύση της παραβίασης προσωπικών δεδομένων, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων προσωπικών δεδομένων, β) ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες, γ)περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης των προσωπικών δεδομένων και δ) περιγράφει τα ληφθέντα

ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των προσωπικών δεδομένων, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.

Για τη γνωστοποίηση περιστατικού παραβίασης στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σε συμμόρφωση με τη σχετική υποχρέωση του άρθρου 33 του Κανονισμού (ΕΕ) 2016/679, ο υπεύθυνος επεξεργασίας πρέπει να συμπληρώσει ειδική φόρμα και να την υποβάλει στην Αρχή ηλεκτρονικά, με αποστολή στην ηλεκτρονική διεύθυνση: databreach@dpa.gr. Μόνο σε εξαιρετική περίπτωση μπορεί η φόρμα να υποβληθεί με άλλο τρόπο (π.χ. με φυσική υποβολή) και σε αυτήν την περίπτωση θα πρέπει να τεκμηριώνεται επαρκώς ο λόγος που δεν προτιμήθηκε η ηλεκτρονική υποβολή.

Διατίθενται δύο μορφές της φόρμας: η πρώτη διαθέτει αυτοματισμούς με σκοπό τη διευκόλυνση της συμπλήρωσής της, και κατά το «άνοιγμά» της, θα πρέπει να ενεργοποιούνται οι μακροεντολές. Η δεύτερη είναι η απλή μορφή, χωρίς μακροεντολές.

Η φόρμα υποβάλλεται στην ελληνική, ενώ είναι διαθέσιμη και αγγλική έκδοση, η οποία πρέπει να χρησιμοποιείται όταν το περιστατικό αφορά διασυνοριακή επεξεργασία.

Προτείνεται, για την ασφάλεια της ηλεκτρονικής αποστολής να αποστέλλεται η εν λόγω φόρμα κρυπτογραφημένη, με τρόπο τέτοιο ώστε να μπορεί να αναγνωσθεί (αποκρυπτογραφηθεί) μόνο από την Αρχή. Για να διασφαλιστεί αυτό, θα πρέπει να χρησιμοποιηθεί το λογισμικό GnuPG (GPG), το οποίο αποτελεί ελεύθερη διανομή του προτύπου OpenPGP. Θα πρέπει πρώτα να κρυπτογραφηθεί το αρχείο (συμπληρωμένη φόρμα γνωστοποίησης) τοπικά στο υπολογιστικό σύστημα της εταιρείας, ανεξάρτητα από το πρόγραμμα/υπηρεσία ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται, και ακολούθως να επισυναφθεί, ως κρυπτογραφημένο πλέον αρχείο, σε μήνυμα ηλεκτρονικού ταχυδρομείου. Το δημόσιο GPG κλειδί της Αρχής, με το οποίο θα πρέπει να κρυπτογραφηθεί η συμπληρωθείσα φόρμα γνωστοποίησης πριν επισυναφθεί στο μήνυμα ηλεκτρονικού ταχυδρομείου* που θα αποσταλεί στην Αρχή, είναι διαθέσιμο εδώ (Key ID:445EA68B). Με τον ίδιο τρόπο μπορεί να κρυπτογραφηθεί και όποιο άλλο τυχόν συνοδευτικό αρχείο της φόρμας.

4.18.3 Ανακοίνωση παραβίασης στο υποκείμενο των δεδομένων.

Όταν η παραβίαση προσωπικών δεδομένων ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των προσωπικών δεδομένων στο υποκείμενο των δεδομένων[1].

Στην ανακοίνωση στο υποκείμενο των δεδομένων περιγράφεται με σαφήνεια η φύση της παραβίασης των προσωπικών δεδομένων και περιέχονται τουλάχιστον οι ακόλουθες πληροφορίες και μέτρα:

α) ανακοίνωση του ονόματος και των στοιχείων επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες,

β) περιγραφή των ενδεχόμενων συνεπειών της παραβίασης των προσωπικών δεδομένων και

γ) περιγραφή των ληφθέντων ή των προτεινόμενων προς λήψη μέτρων από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των προσωπικών δεδομένων, καθώς και, όπου ενδείκνυται, μέτρων για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Η ανακοίνωση στο υποκείμενο των δεδομένων δεν απαιτείται, εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις:

α) Ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση προσωπικά δεδομένα, κυρίως μέτρα που καθιστούν μη κατανοητά τα προσωπικά δεδομένα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση.

β) Ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

γ) Προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

Εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των προσωπικών δεδομένων στο υποκείμενο των δεδομένων, η εποπτική αρχή μπορεί, έχοντας εξετάσει την πιθανότητα επέλευσης υψηλού κινδύνου από την παραβίαση των προσωπικών δεδομένων, να του ζητήσει να το πράξει ή μπορεί να αποφασίσει ότι πληρούται οποιαδήποτε από τις προϋποθέσεις που αναφέρονται στην παράγραφο 3 του άρθρου 34 GDPR.

---

[1] Βλ. Guidelines on personal data breach notification under Regulation 2016/679, Γνωμοδότηση 03/2014 σχετικά με τη γνωστοποίηση παραβίασης προσωπικών δεδομένων και Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the EU, που εκδόθηκαν από την Ομάδα Εργασίας άρθρου 29 για την προστασία προσωπικών δεδομένων.

4.19 Ασφάλεια πληροφοριών κατά τη διαχείριση επιχειρησιακής συνέχειας.

Η EPSILON NET αποδίδει ιδιαίτερη σημασία στη διατήρηση ικανοποιητικού επιπέδου ασφάλειας κατά τη διαχείριση των επιπτώσεων ενός περιστατικού ασφάλειας. Στο πλαίσιο αυτό, έχει μεριμνήσει, ώστε το σχέδιο επιχειρησιακής συνέχειας της εταιρείας να περιλαμβάνει ρόλους, διαδικασίες και μέτρα που διασφαλίζουν το επιθυμητό επίπεδο ασφάλειας των πόρων της εταιρείας.

4.20 Συμμόρφωση.

Η πολιτική, οι διαδικασίες και τα λοιπά μέτρα ασφάλειας της EPSILON NET, λαμβάνουν υπόψη και συμμορφώνονται με τις κανονιστικές ή συμβατικές υποχρεώσεις της εταιρείας. Αντίστοιχα, τα στελέχη που αναλαμβάνουν ρόλους σχετικά με τη διαχείριση της ασφάλειας είναι υπεύθυνα για την εφαρμογή της πολιτικής ασφάλειας στον τομέα ευθύνης τους.

Η Πολιτική Ασφάλειας της εταιρείας λαμβάνει υπόψη τα εξής:

- την ισχύουσα εθνική και ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων,
- τις οδηγίες και αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) όσον αφορά στην προστασία των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας από την εταιρεία,
- το περιβάλλον και τον τρόπο λειτουργίας της εταιρείας και
- το χαρακτήρα και το είδος των υπηρεσιών που παρέχονται από την εταιρεία, τον τρόπο παροχής τους και τους αποδέκτες των υπηρεσιών αυτών.

Το προσωπικό της εταιρείας θα πρέπει να είναι ενήμερο σχετικά με τις απαιτήσεις της νομοθεσίας περί προστασίας προσωπικών δεδομένων. Για τον λόγο αυτό:

- Οι υπάλληλοι της εταιρείας ενημερώνονται τακτικά για την ισχύουσα εθνική και ευρωπαϊκή νομοθεσία και τον τρόπο επεξεργασίας προσωπικών δεδομένων.
- Ο ΥΑΠ/ΠΔ διασφαλίζει ότι κάθε νεοπροσλαμβανόμενος υπάλληλος στην εταιρεία ενημερώνεται σχετικώς. Αντίστοιχη ενημέρωση λαμβάνουν και οι εξωτερικοί συνεργάτες της εταιρείας.
- Σε περίπτωση αλλαγών ή τροποποιήσεων στη νομοθεσία, ο ΥΑΠ/ΠΔ, σε συνεργασία με νομικό σύμβουλο της εταιρείας, προετοιμάζει και αποστέλλει ενημερωτικά σημειώματα στο προσωπικό και τους συνεργάτες της εταιρείας.

4.20.1 Συμμόρφωση με έννομες και συμβατικές υποχρεώσεις.

4.20.1.1 Προστασία προσωπικών δεδομένων.

Η εταιρεία μεριμνά για τη συνεχή συμμόρφωση με τις απαιτήσεις που απορρέουν από την ισχύουσα εθνική και ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων. Βασικά νομοθετήματα που βρίσκουν εφαρμογή στην εταιρεία είναι τα εξής:

- Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
- Ο Ν. 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις».
- Η νομοθεσία περί πνευματικής ιδιοκτησίας (π.χ. Ν. 2121/1993).

Τέλος, η εταιρεία οφείλει να συμμορφώνεται με τις απαιτήσεις εμπιστευτικότητας, εχεμύθειας κλπ. που περιλαμβάνονται σε συμβάσεις που συνάπτει με τρίτα μέρη (προμηθευτές, πελάτες, συνεργάτες κλπ.).

4.20.1.2 Δικαιώματα πνευματικής ιδιοκτησίας.

Η εταιρεία λειτουργεί σεβόμενη τα δικαιώματα πνευματικής ιδιοκτησίας που υπάρχουν στους πληροφοριακούς πόρους που διαχειρίζεται. Για τον σκοπό αυτό, η εταιρεία εφαρμόζει τους παρακάτω κανόνες:

- Η εταιρεία προμηθεύεται λογισμικό μόνο από επώνυμες πηγές που διαθέτουν την κατάλληλη άδεια διάθεσης του λογισμικού από τον κατασκευαστή του λογισμικού.
- Το λογισμικό της εταιρείας συνοδεύεται από τις αντίστοιχες άδειες χρήσης του κατασκευαστή / προμηθευτή. Ο αριθμός εγκαταστάσεων του λογισμικού δεν μπορεί να υπερβαίνει σε καμία περίπτωση τον αριθμό των διαθέσιμων αδειών χρήσης.
- Η εγκατάσταση λογισμικού στα συστήματα της εταιρείας που δεν συνοδεύεται από την κατάλληλη άδεια χρήσης ή/και δεν έχει αγοραστεί μέσω της επίσημης διαδικασίας της εταιρείας απαγορεύεται.

- Η αντιγραφή νομίμως αγορασμένου λογισμικού απαγορεύεται. Επιτρέπεται μόνο για τη δημιουργία αντιγράφων ασφαλείας των πρωτότυπων μέσων εγκατάστασης του λογισμικού.
- Οι διαχειριστές των συστημάτων της εταιρείας διεξάγουν ελέγχους σε τακτά χρονικά διαστήματα, προκειμένου να διαπιστώσουν ότι τα συστήματα της εταιρείας είναι εξοπλισμένα αποκλειστικά με νόμιμο λογισμικό που συνοδεύεται από τις κατάλληλες άδειες χρήσης.

4.20.2 Ανασκοπήσεις ασφάλειας πληροφοριών.

Η Διοίκηση της εταιρείας, ο ΥΑΠ/ΠΔ, οι διαχειριστές των συστημάτων και όλα τα στελέχη της εταιρείας μεριμνούν για τη διασφάλιση της συμμόρφωσης με τις πολιτικές και τα πρότυπα ασφάλειας προσωπικών δεδομένων που έχουν εφαρμογή στο πεδίο ευθύνης τους.

Επιπλέον, με ευθύνη του ΥΑΠ/ΠΔ, οι πληροφοριακοί πόροι της εταιρείας ελέγχονται σε τακτά χρονικά διαστήματα, προκειμένου να διαπιστωθεί το επίπεδο συμμόρφωσής τους με τις πολιτικές και τα πρότυπα ασφάλειας της εταιρείας. Σε περίπτωση εντοπισμού σημαντικών μη συμμορφώσεων, ο ΥΑΠ/ΠΔ μεριμνά για το σχεδιασμό και τη λήψη πρόσθετων μέτρων ασφάλειας. Ιδιαίτερα στην περίπτωση εμφάνισης κάποιου πολύ σοβαρού περιστατικού ασφάλειας, ο χρόνος αντίδρασης του συνόλου της οργανωτικής δομής διαχείρισης της ασφάλειας οφείλει να είναι ιδιαίτερα μικρός. Για τον λόγο αυτό, η έγκριση για τη λήψη μέτρων ασφάλειας χαρακτήρα «επείγοντος» δίνεται από τον ΥΑΠ/ΠΔ, ο οποίος στη συνέχεια θα ενημερώσει τη Διοίκηση της εταιρείας μέσω των αναφορών που της υποβάλλει.

Για τον έλεγχο της συμμόρφωσης των συστημάτων της εταιρείας με πολιτικές και πρότυπα ασφάλειας, ο ΥΑΠ/ΠΔ μπορεί να ζητήσει τη βοήθεια ειδικών εμπειρογνωμόνων στον τομέα της ασφάλειας.

4.20.3 Τεχνικές ανασκοπήσεις συμμόρφωσης.

Η εταιρεία δύναται να κάνει χρήση τεχνικών μέσων για τη διαπίστωση της συμμόρφωσης με την εγκεκριμένη πολιτική ασφάλειας. Η χρήση τεχνικών μέσων, όπως εργαλείων ανάλυσης ευπαθειών ασφάλειας (vulnerability scanners) και δοκιμών διείσδυσης (penetration testing) και γενικά εργαλείων που αποσκοπούν στον εντοπισμό κενών ασφάλειας στις υποδομές της εταιρείας, επιτρέπεται μόνο στους διαχειριστές της εταιρείας και στον ΥΑΠ/ΠΔ και μόνο για σκοπούς που εξυπηρετούν τη λειτουργία της εταιρείας και την ασφάλεια των πληροφοριών της, σύμφωνα με την πολιτική της εταιρείας για τη χρήση προγραμμάτων utility programs.

Η εταιρεία προβαίνει στην εκτέλεση ελέγχων ασφάλειας με τεχνικά μέσα τουλάχιστον μία φορά ανά έτος, ακολουθώντας σχετικό πλάνο. Μετά την εκτέλεση των ελέγχων ασφάλειας, καταγράφονται τα αντίστοιχα αποτελέσματα. Η εταιρεία δύναται να χρησιμοποιήσει υπηρεσίες τρίτων για την εκτέλεση τεχνικών ελέγχων, εφόσον αυτό κριθεί σκόπιμο.

5. Παράρτημα - Πολιτική ασφάλειας της EPSILON NET.

Η Διοίκηση της εταιρείας EPSILON NET Α.Ε. δεσμεύεται να διαχειρίζεται τα θέματα Διαχείρισης Ασφάλειας Πληροφοριών με την ίδια υπευθυνότητα και σημασία με την οποία αντιμετωπίζει το σύνολο των λειτουργιών των εταιρειών της. Πιστεύουμε ότι, με τον τρόπο αυτό μεγιστοποιείται η ωφέλεια από τη λειτουργία των εταιρειών για τους πελάτες και τους εργαζομένους μας.

Συγκεκριμένα, δεσμευόμαστε να υποστηρίξουμε την εφαρμογή μεθόδων Διαχείρισης Ασφάλειας Πληροφοριών, ώστε να εξασφαλίζεται η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα των πληροφοριών που διαχειριζόμαστε.

Σκοπεύουμε να πραγματοποιήσουμε τη δέσμευσή μας ακολουθώντας τις αρχές της πρόληψης και προστασίας σύμφωνα με τις νομοθετικές διατάξεις αλλά και με τις απαιτήσεις που προκύπτουν από το ευρύτερο πλαίσιο που έχει αναπτύξει ο Όμιλος Epsilon Net για τη διαχείριση κινδύνων στρατηγικής σημασίας, καθώς και μέσω της δημοσιοποίησης των ενεργειών μας και της συνεχούς βελτίωσης της επίδοσής μας στους τομείς της Ασφάλειας Πληροφοριών.

Η συνεχής αυτή προσπάθεια πραγματοποιείται με την παρακολούθηση και εφαρμογή των σύγχρονων τεχνολογιών και διεθνών πρακτικών, με τον καθορισμό στόχων και κριτηρίων βάσει των οποίων διενεργείται συνεχής αξιολόγηση του επιπέδου επικινδυνότητας, με την υλοποίηση προγραμμάτων αντιμετώπισης και με την ενημέρωση, εκπαίδευση και συμμετοχή των εργαζομένων στη διαχείριση της ασφάλειας πληροφοριών.

Η διαρκής αναζήτηση μεθόδων βελτίωσης των εφαρμοζόμενων μεθόδων διαχείρισης της ασφάλειας πληροφοριών, θα βοηθήσει την Εταιρεία να προστατεύει συνεχώς όλο και πιο αποτελεσματικά τις πληροφορίες που διαχειρίζεται. Για την εξέλιξη των ενεργειών μας αυτών, θα ενημερώνουμε τους πελάτες, τους εργαζόμενους και τους μετόχους.

Η Διοίκηση της Εταιρείας δίνει την πλήρη υποστήριξή της στο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO 27001:2023 και σε συνεννόηση με το προσωπικό δεσμεύεται να καθορίζει αντικειμενικούς σκοπούς και στόχους τους οποίους και θα ανασκοπεί σε τακτά χρονικά διαστήματα ώστε να βρίσκεται πάντα εντός των προδιαγραφών που έχει θέσει.

Η Διοίκηση