CubeIQ Ε.Π.Ε.
Έγγραφο Πολιτικής Ασφαλείας

Έκδοση 2.6.0.GR
Μάιος 2012

Περιεχόμενα

1 Ορισμοί & Συντομογραφίες

Αδυναμία	Σημείο ενός ΠΕΣ, το οποίο μπορεί να επιτρέψει σε μια απειλή να πραγματοποιηθεί και να προκαλέσει ζημιά στο ΠΕΣ. Αναφέρεται και ως ευπάθεια (vulnerability).
Ακεραιότητα	Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.
Ανάδοχος	Φορείς, εταιρείες, οργανισμοί ή φυσικά πρόσωπα με τους οποίους υπήρξαν ή υπάρχουν συμβατικές σχέσεις για την εκτέλεση ενός έργου ή την παροχή υπηρεσιών.
Ανάλυση Επικινδυνότητας	Διαδικασία μέσα από την οποία προσδιορίζονται και αποτιμούνται οι παράγοντες που συνθέτουν την επικινδυνότητα, δηλαδή η αξία των στοιχείων ενός συστήματος, οι απειλές και οι ευπάθειες (αδυναμίες, vulnerabilities).
Αρχεία καταγραφής (audit logs)	Αρχεία ή βάσεις δεδομένων ενός συστήματος, όπου καταγράφονται γεγονότα που συμβαίνουν στο σύστημα (πχ. εκκίνηση συστήματος) και ενέργειες χρηστών.
Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ)	Διοικητική αρχή που έχει ιδρυθεί με σκοπό τη ρύθμιση ζητημάτων που αφορούν την προστασία του απορρήτου των επικοινωνιών κάθε μορφής (ηλεκτρονικές, έγγραφες κλπ.).
Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ)	Ανεξάρτητη διοικητική αρχή που έχει ιδρυθεί με σκοπό την προστασία του ατόμου από την επεξεργασία πληροφοριών προσωπικού χαρακτήρα. Επίσημη ονομασία Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
Ασφάλεια ΠΕΣ	Το οργανωμένο πλαίσιο από έννοιες, αρχές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται, για να προστατευθούν τόσο τα στοιχεία του ΠΕΣ όσο και ολόκληρο το ΠΕΣ από τυχαία ή σκόπιμη απειλή.
Αυθεντικοποίηση	Η εξακρίβωση της γνησιότητας μίας πληροφορίας ή της ταυτότητας ενός χρήστη ή ενός υπολογιστικού συστήματος.

Αυτόκλητα μηνύματα	Μηνύματα ηλεκτρονικού ταχυδρομείου που στέλνονται σε έναν αποδέκτη ενώ αυτός δεν έχει εκφράσει επιθυμία να τα λαμβάνει. Επίσης ανεπιθύμητη αλληλογραφία, (unsolicited mail, spam).
Διαθεσιμότητα	Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας ή των υπολογιστικών πόρων σε νόμιμα εξουσιοδοτημένους χρήστες.
Διαχειριστής	Τεχνικός (μηχανικός) της Εταιρείας που έχει ως αρμοδιότητα την πραγματοποίηση τεχνικών εργασιών στα ΠΕΣ της Εταιρείας. Ο όρος αφορά τόσο όσους διαχειρίζονται ένα σύστημα, όσο και αυτούς που απλά πραγματοποιούν κάποια τεχνική εργασία σε αυτό.
Διοίκηση της Εταιρείας	Τα ανώτερα διοικητικά στελέχη, τα οποία εκφράζουν την Εταιρεία και λαμβάνουν στρατηγικής σημασίας αποφάσεις για αυτήν.
Ελεγκτής ΠΕΣ	Άτομο επιφορτισμένο με την αρμοδιότητα να ασκεί ελέγχους για την ορθή χρήση των ΠΕΣ της Εταιρείας και την τήρηση των προβλεπόμενων πολιτικών και διαδικασιών.
Έλεγχος Πρόσβασης	Διαδικασία με την οποία ελέγχεται εάν ένας χρήστης ή ένα υπολογιστικό σύστημα έχει το δικαίωμα να πραγματοποιήσει μία ενέργεια ή να εισέλθει σε ένα χώρο.
Εμπιστευτικότητα	Αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες.
Επικινδυνότητα	Συνάρτηση της αξίας ενός αγαθού, της έντασης των απειλών, καθώς και της σοβαρότητας των αντίστοιχων αδυναμιών.
Εταιρεία	CubeIQ Ε.Π.Ε.
Ευπάθεια	Σημείο ενός ΠΕΣ, το οποίο μπορεί να επιτρέψει σε μια απειλή να πραγματοποιηθεί και να προκαλέσει ζημιά στο ΠΕΣ. Αναφέρεται και ως αδυναμία (vulnerability).

Πληροφοριακό και Επικοινωνιακό Σύστημα (ΠΕΣ)	Ενα οργανωμένο σύνολο αλληλεπιδρώντων στοιχείων (άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός, διαδικασίες), το οποίο επεξεργάζεται και μεταδίδει πληροφορίες και αποσκοπεί στην εκπλήρωση κάποιου σκοπού.
Πολιτική Ασφάλειας ΠΕΣ	Περιγραφή, σε γενικό-αφαιρετικό επίπεδο, του συνόλου των κανόνων, μέτρων και διαδικασιών που ορίζουν τα φυσικά, διαδικαστικά και οργανωτικά μέτρα ασφάλειας, που λαμβάνονται κατά τη διαχείριση, τη διανομή και την προστασία των στοιχείων ενός ΠΕΣ.
Συνεργάτης (εξωτερικός)	Φορείς, εταιρείες, οργανισμοί ή φυσικά πρόσωπα με τους οποίους υπήρξαν ή υπάρχουν εργασιακές συμβατικές σχέσεις.
Υπεύθυνος Ασφάλειας ΠΕΣ	Ατομο επιφορτισμένο με την ευθύνη για το συντονισμό των ενεργειών που αφορούν την ασφάλεια ενός ΠΕΣ.
Χρήστης	Ατομο που έχει εξουσιοδοτηθεί να χρησιμοποιεί έναν υπολογιστή, μία εφαρμογή ή κάποιο άλλο σύστημα.

2 Πολιτική Ασφάλειας ΠΕΣ της CubeIQ

2.1 Εισαγωγή

Η Πολιτική Ασφάλειας περιγράφει το σύνολο θεμελιωδών αρχών που καθορίζουν τον τρόπο με τον οποίο η CubeIQ προστατεύει την πληροφοριακή υποδομή που υποστηρίζει τις δραστηριότητες της CubeIQ , έτσι ώστε να επιτυγχάνει συγκεκριμένους στόχους ασφάλειας.

Σκοπός της Πολιτικής Ασφάλειας είναι να παράσχει στρατηγική καθοδήγηση στα στελέχη της CubeIQ για την προστασία των ΠΕΣ της. Η Πολιτική Ασφάλειας δεν πρέπει να είναι στατική, αλλά να προσαρμόζεται ακολουθώντας τις αλλαγές της πληροφοριακής υποδομή και του τεχνικοκοινωνικού περιβάλλοντος της Εταιρείας.

Η προτεινόμενη Πολιτική Ασφάλειας βασίστηκε στα αποτελέσματα της ανάλυσης επικινδυνότητας, στις απαιτήσεις της Αρχής Προστασίας Προσωπικών Δεδομένων, στις απαιτήσεις της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, όπως αυτές εκφράζονται από τους σχετικούς κανονισμούς και συστάσεις, στις οδηγίες που περιλαμβάνει το ISO/ IEC 17799, καθώς και στις βασικές διαστάσεις των ορατών στρατηγικών κατευθύνσεων της CubeIQ, σε σχέση με την αξιοποίηση των ΤΠΕ.

2.2 Σκοπός και Χρησιμότητα της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας καθοδηγεί τη λήψη αποφάσεων σε όλες τις βαθμίδες διοίκησης και αποτελεί αποτελεσματικό μέσο για την ασφάλεια των ΠΕΣ της Εταιρείας. Η διασφάλιση της πληροφοριακής υποδομής, ως διαδικασία λήψης αποφάσεων, είναι ουσιαστικά εξαρτημένη από την ύπαρξη σχετικής πολιτικής ασφάλειας. Η CubeIQ καλείται να επιτύχει, με τη βοήθεια της Πολιτικής Ασφάλειας, τους ακόλουθους στόχους:

- Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων και τη διασφάλιση του απορρήτου των επικοινωνιών.

- Διασφάλιση της επιχειρησιακής της ικανότητας, στο βαθμό που εξαρτάται από την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα πληροφοριών και επικοινωνιών.

- Προστασία της επένδυσης που απαιτεί η λειτουργία των ΠΕΣ της CubeIQ.

- Η Πολιτική Ασφάλειας των ΠΕΣ της CubeIQ ανακλά την πρόθεση της Εταιρείας να προστατέψει την πληροφοριακή της υποδομή. Η Πολιτική Ασφάλειας περιγράφει το σύνολο των αρχών και κανόνων που καθορίζουν τον τρόπο με τον οποίο η Εταιρεία πρέπει να διαχειρίζεται και να προστατεύει τους πόρους της, έτσι ώστε να επιτυγχάνει συγκεκριμένους στόχους ασφάλειας. Οι στόχοι αυτοί έχουν καθοριστεί από την ανάλυση επικινδυνότητας και συνοψίζονται στη σύννομη, αδιάλειπτη και αποτελεσματική λειτουργία των ΠΕΣ.Ο χαρακτήρας της Πολιτικής Ασφάλειας δεν αφορά μόνον τεχνικά ή μόνον οργανωτικά θέματα, αλλά αντιμετωπίζει με την ίδια προσοχή και τις δύο αυτές απόψεις διαχείρισης της ασφάλειας των ΠΕΣ.

2.3 Εμβέλεια της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας αφορά στα ΠΕΣ της CubeIQ που υποστηρίζουν δραστηριότητες της CubeIQ. Καλύπτει το σύνολο των πληροφοριών που διακινούνται, τυγχάνουν επεξεργασίας, ή αποθηκεύονται σε ηλεκτρονική μορφή, επεκτείνεται, όμως, και στις περιπτώσεις όπου οι ανωτέρω πληροφορίες μετατρέπονται σε άλλες μορφές (πχ. εκτυπώσεις).

2.4 Περιορισμοί

Η Πολιτική Ασφάλειας ΠΕΣ περιορίζεται στα συστήματα που υποστηρίζουν δραστηριότητες της CubeIQ, καθώς η ανάλυση επικινδυνότητας που πραγματοποιήθηκε αφορούσε αυτά τα συστήματα και οι νομικές και κανονιστικές υποχρεώσεις που αναφέρονται ανωτέρω αφορούν τις τηλεπικοινωνιακές υπηρεσίες που προσφέρει η Εταιρεία. Με βάση, όμως, αυτήν την πολιτική και με μικρές αλλαγές είναι εφικτή η επέκταση της ισχύος της πολιτικής σε όλα τα ΠΕΣ της CubeIQ.

Η διαμόρφωση της παρούσας πολιτικής έχει ως αφετηρία τα προβλεπόμενα στο πρότυπο ISO/IEC 17799 και η εφαρμογή της οδηγεί σε συμμόρφωση με το πρότυπο αυτό. Επίσης, καλύπτει τις σχετικές απαιτήσεις της Αρχής Προστασίας Προσωπικών Δεδομένων και της σχετικής νομοθεσίας.

Το Σχέδιο Κανονισμού για τη "διασφάλιση του απορρήτου κατά την παροχή τηλεπικοινωνιακών υπηρεσιών μέσω Δικτύων Κινητών Επικοινωνιών" της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών έχει ληφθεί υπόψη και έχει καθορίσει σε μεγάλο βαθμό τη δομή της Πολιτικής Ασφάλειας ΠΕΣ. Ομως, η παρούσα πολιτική δεν αναφέρεται στο φυσικό επικοινωνιακό δίκτυο και δεν καλύπτει τις προβλέψεις του Κανονισμού που το αφορούν, καθώς η μελέτη του φυσικού δικτύου δεν εντάσσεται στην οριοθέτηση της παρούσας μελέτης. Επίσης, να σημειωθεί ότι κατά τη διαμόρφωση της παρούσας πολιτικής ο Κανονισμός ήταν ακόμα υπό διαμόρφωση και δεν είχε τεθεί σε ισχύ.

2.5 Αξιοποίηση της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας βασίστηκε στις εκτιμήσεις των μελετητών του έργου σχετικά με τις απαιτήσεις ασφάλειας της οργάνωσης, λειτουργίας και τεχνικής υποδομής των ΠΕΣ της CubeIQ. Εντούτοις, η Πολιτική Ασφάλειας είναι άμεσα εξαρτημένη από τη φύση των δραστηριοτήτων της Εταιρείας, τις κατευθύνσεις της Διοίκησης και το περιβάλλον λειτουργίας της Εταιρείας.

Βασικά σημεία για την κατανόηση και αξιοποίηση της Πολιτικής Ασφάλειας αποτελούν οι εξής διαπιστώσεις:

⇒ Η Πολιτική Ασφάλειας αποτελεί βασικό μέσο ανάπτυξης κουλτούρας ασφάλειας στα στελέχη και τους εργαζόμενους της Εταιρείας. Αποτελεί γενικά διαθέσιμο υπηρεσιακό κείμενο και πρέπει να ληφθεί μέριμνα, ώστε όλα τα μέλη του προσωπικού που έχουν ρόλο στη λειτουργία των ΠΕΣ, είτε ως χρήστες, είτε ως διαχειριστές, είτε ως διοικητικά στελέχη, να λάβουν γνώση της.

⇒ Η Πολιτική Ασφάλειας δεν είναι απόλυτη ή στατική. Βασίστηκε στη μελέτη επικινδυνότητας, καθώς και στις βασικές διαστάσεις των στρατηγικών κατευθύνσεων της Εταιρείας που αναγνωρίστηκαν μέσω της μελέτης.

⇒ Το παρόν κείμενο αποτελεί ένα ευέλικτο και αποτελεσματικό πρόπλασμα Πολιτικής Ασφάλειας. Η Εταιρεία μπορεί να ορίσει, με βάση τις εκάστοτε προτεραιότητές της, το ακριβέστερο εύρος, ύφος και περιεχόμενο της Πολιτικής αυτής.

2.6 Βασικά Δομικά Στοιχεία της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας αποτελεί ένα πλαίσιο στο οποίο εντάσσεται ένα σύνολο εξειδικευμένων πολιτικών.

Συγκεκριμένα, η Πολιτική Ασφάλειας περιλαμβάνει τις εξής πολιτικές:

1. Πολιτική Διαχείρισης Ασφάλειας ΠΕΣ

2. Πολιτική Προσωπικού

3. Πολιτική Πρακτικών Θεμιτής Χρήσης

4. Πολιτική Προστασίας Προσωπικών Δεδομένων και Επικοινωνιών

5. Πολιτική Αναδόχων και Συνεργατών

6. Πολιτική Προστασίας ΠΕΣ

Καθεμία από τις Πολιτικές αυτές παρατίθεται αναλυτικά στη συνέχεια. Για κάθε πολιτική παρατίθεται ο σκοπός της, η εμβέλειά της, οι γενικές αρχές της, καθώς και οι οδηγίες και οι συγκεκριμένοι κανόνες ασφαλείας που προβλέπει.

2.7 Πολιτική Διαχείρισης Ασφάλειας ΠΕΣ

2.7.1 Εισαγωγή

Με την πολιτική αυτή η Διοίκηση της CubeIQ εκφράζει τη βούλησή της για τη διασφάλιση των ΠΕΣ που υποστηρίζουν τις δραστηριότητες της CubeIQ και παρέχει τις βασικές κατευθύνσεις για τη διαχείριση της ασφάλειας των ΠΕΣ.

2.7.2 Σκοπός

Σκοπός της Πολιτικής Διαχείρισης Ασφάλειας ΠΕΣ είναι:

- Να εκφράσει ρητά τη βούληση της CubeIQ να διασφαλίσει τη λειτουργία των ΠΕΣ που υποστηρίζουν τις δραστηριότητες της CubeIQ.

- Να δώσει κατευθυντήριες οδηγίες στα στελέχη της Εταιρείας για τον τρόπο με τον οποίο πρέπει να αντιμετωπίζουν τα ζητήματα ασφάλειας ΠΕΣ.

- Να προδιαγράψει ένα Σύστημα Διαχείρισης της Ασφάλειας των ΠΕΣ.

2.7.3 Εμβέλεια

Η Πολιτική καλύπτει όλα τα ΠΕΣ που υποστηρίζουν δραστηριότητες της CubeIQ, είτε έχουν αναπτυχθεί αποκλειστικά για αυτόν το σκοπό, είτε προσφέρουν υπηρεσίες και σε άλλες δραστηριότητες της CubeIQ. Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας ΠΕΣ.

Η Πολιτική απευθύνεται στα στελέχη της CubeIQ που ασκούν διοικητικά καθήκοντα που σχετίζονται με τις δραστηριότητες της CubeIQ ή εποπτεύουν αυτές τις δραστηριότητες ή ασκούν διοίκηση σε τομείς που υποστηρίζουν τη λειτουργία των ΠΕΣ. Απευθύνεται, επίσης, στο σύνολο του προσωπικού που υποστηρίζει τη λειτουργία των ΠΕΣ.

2.7.4 Γενικές Αρχές

Βούληση της διοίκησης

Η CubeIQ αποδίδει υψηλή προτεραιότητα στην ασφάλεια των ΠΕΣ που υποστηρίζουν τις δραστηριότητες της CubeIQ.

Πολιτική ασφάλειας ΠΕΣ

Η CubeIQ θεσπίζει και θέτει σε ισχύ την "Πολιτική Ασφάλειας ΠΕΣ". Η Πολιτική Ασφάλειας ΠΕΣ αποτελείται από την παρούσα Πολιτική Διαχείρισης Ασφάλειας ΠΕΣ, καθώς και από ένα σύνολο θεματικών Πολιτικών Ασφάλειας

Υποστήριξη εφαρμογής της Πολιτικής Ασφάλειας ΠΕΣ

Η Διοίκηση της Εταιρείας υποστηρίζει την εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ εξασφαλίζοντας τους απαραίτητους για αυτό το σκοπό πόρους και μέσα.

Διοικητική και οργανωτική υποστήριξη διαχείρισης της ασφάλειας ΠΕΣ

Με στόχο την αποτελεσματικότερη εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ, αναπτύσσεται η κατάλληλη διοικητική δομή, ορίζονται οι ρόλοι που είναι απαραίτητοι για τη διαχείρισης της ασφάλειας ΠΕΣ, καθορίζονται οι αρμοδιότητες για κάθε ρόλο και ανατίθενται οι ρόλοι στα κατάλληλα άτομα.

Συμμόρφωση με νομικό πλαίσιο

Η Διοίκηση και τα στελέχη της Εταιρείας προβαίνουν σε όλες τις ενέργειες που απαιτούνται για να γίνεται σεβαστή η νομοθεσία που αφορά την προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά η νομοθεσία που αφορά τη χρήση ΠΕΣ.

2.7.5 Οδηγίες και Κανόνες Ασφάλειας

Α . Πολιτική Ασφάλειας ΠΕΣ

Α1. Η Πολιτική Ασφάλειας ΠΕΣ πρέπει να είναι έγγραφη και να έχει επικυρωθεί από τη Διοίκηση της Εταιρείας.

Α2. Η Εταιρεία προβαίνει σε όλες τις απαραίτητες ενέργειες, ώστε να ενημερώσει το προσωπικό για την Πολιτική Ασφάλειας ΠΕΣ και να εξασφαλίσει την άμεση και εύκολη πρόσβαση των υπαλλήλων στο πλήρες κείμενο της πολιτικής.

Α3. Η Πολιτική Ασφάλειας ΠΕΣ αποτελείται από επί μέρους πολιτικές. Σε αυτές περιλαμβάνονται η Πολιτική Διαχείρισης Ασφάλειας ΠΕΣ, η Πολιτική Προσωπικού, η Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΕΣ, η Πολιτική Προστασίας Προσωπικών Δεδομένων και Επικοινωνιών, η Πολιτική Αναδόχων και Συνεργατών και η Πολιτική Προστασίας ΠΕΣ.

Α4. Η Πολιτική Ασφάλειας ΠΕΣ καθορίζεται με βάση την επικινδυνότητα που ενέχεται στη λειτουργία των ΠΕΣ, όπως αυτή αποτιμάται με την εκπόνηση μελέτης ανάλυσης επικινδυνότητας.

Α5. Η Πολιτική Ασφάλειας ΠΕΣ πρέπει να τυγχάνει τακτικής ανασκόπησης και να αναθεωρείται και επικαιροποιείται σε περίπτωση μείζονων αλλαγών στα ΠΕΣ της CubeIQ , καθώς και σε περιπτώσεις σημαντικών μεταβολών του κοινωνικού και τεχνολογικού περιβάλλοντος, από τις οποίες προκύπτουν νέες απειλές, ευπάθειες, ή νέες ευκαιρίες βελτίωσης της ασφάλειας ΠΕΣ. Οι διαδικασίες αναθεώρησης της Πολιτικής περιλαμβάνονται στο Σχέδιο Ασφάλειας ΠΕΣ.

Α6. Τα στελέχη της Εταιρείας πρέπει να συμβουλεύονται την Πολιτική Ασφάλειας ΠΕΣ σε κάθε απόφασή τους, που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα, την ασφάλεια των ΠΕΣ.

Α7. Η εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ είναι υποχρεωτική. Σε περίπτωση παραβίασης της Πολιτικής, η Εταιρεία έχει το δικαίωμα να επιβάλλει κυρώσεις.

Β . Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο

Β1. Η CubeIQ δεσμεύεται για την τήρηση της νομοθεσίας που αφορά την προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά τη νομοθεσία που αφορά τη χρήση ΠΕΣ, καθώς και για την εφαρμογή των σχετικών αποφάσεων της Αρχής Προστασίας Προσωπικών Δεδομένων και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών.

Β2. Η Εταιρεία διαμορφώνει μία Πολιτική Αποδεκτής Χρήσης που απευθύνεται στους πελάτες των υπηρεσιών κινητής τηλεφωνίας και περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες. Η πολιτική αυτή πρέπει να είναι συνοπτική και να δημοσιοποιείται.

Β3. Η Εταιρεία καταρτίζει και εφαρμόζει διαδικασίες που διασφαλίζουν τη διατήρηση των δεδομένων των επικοινωνιών για το χρονικό διάστημα που ορίζει η νομοθεσία.

Β4. Η Εταιρεία προβαίνει σε όλες τις ενέργειες που απαιτούνται, ώστε να παρέχει στις Αρχές διευκολύνσεις και πληροφορίες, όπως προβλέπει η σχετική νομοθεσία. Η Εταιρεία διασφαλίζει ότι οι σχετικές διευκολύνσεις και πληροφορίες παρέχονται μόνο στις περιπτώσεις που προβλέπονται από τη νομοθεσία, ακολουθώντας νόμιμες διαδικασίες.

Β5. Η Διοίκηση της Εταιρείας και ειδικότερα τα στελέχη της Διαχείρισης Ανθρώπινου Δυναμικού μεριμνούν ώστε όλα τα μέλη του προσωπικού να γνωρίζουν τις υποχρεώσεις τους που απορρέουν από τη νομοθεσία σχετικά με την επεξεργασία προσωπικών πληροφοριών και τη διασφάλιση του απορρήτου των επικοινωνιών.

Β6. Η Διοίκηση μεριμνά για την ανάπτυξη οργανωτικών δομών και διαδικασιών με στόχο την προστασία της Εταιρείας από νομικές ενέργειες που στρέφονται εναντίον της.

Β7. Η Εταιρεία μεριμνά για την προστασία του προσωπικού από νομικές συνέπειες που μπορεί να προκύψουν από ενέργειές τους στα πλαίσια της άσκησης των καθηκόντων τους και εφόσον τηρούν πιστά τις πολιτικές και τους κανονισμούς της Εταιρείας.

Γ . Οργανωτική υποδομή

Γ1. Η Εταιρεία αναπτύσσει κατάλληλες οργανωτικές και διοικητικές δομές για την αποτελεσματική διαχείριση της ασφάλειας ΠΕΣ. Η ευθύνη για τη διαχείριση της ασφάλειας ΠΕΣ ανατίθεται σε ανεξάρτητη Διεύθυνση. Ο επικεφαλής της Διεύθυνσης αναλαμβάνει το ρόλο του Υπεύθυνου Ασφάλειας ΠΕΣ.

Γ2. Η Εταιρεία μεριμνά για την επαρκή στελέχωση των διευθύνσεων που έχουν ενεργό ρόλο στην ασφάλεια των ΠΕΣ.

Γ3. Στο οργανόγραμμα της Εταιρείας εντάσσονται οι ρόλοι του Υπεύθυνου Ασφάλειας ΠΕΣ, του Υπεύθυνου Πρόσβασης, του Υπεύθυνου Ασφάλειας Συστήματος και του Υπεύθυνου Αντιγράφων Ασφάλειας.

Γ4. Η Εταιρεία μεριμνά ώστε τα άτομα που αναλαμβάνουν ρόλους σχετικούς με την Ασφάλεια ΠΕΣ να έχουν την απαιτούμενη κατάρτιση.

Γ5. Ολες οι διαδικασίες που αφορούν την ασφάλεια ΠΕΣ είναι καταγεγραμμένες. Για κάθε διαδικασία να ορίζεται ένας υπεύθυνος για την καταγραφή, τον έλεγχο της αποτελεσματικότητας, την επικαιροποίηση και τη διάθεσή της στα μέλη του προσωπικού που έχουν ανάγκη γνώσης ("need-to-know").

Δ . Εκπαίδευση και ενημέρωση

Δ1. Η Διοίκηση μεριμνά για την εκπαίδευση και ευαισθητοποίηση σε θέματα ασφάλειας ΠΕΣ των χρηστών και γενικά του προσωπικού της Εταιρείας που σχετίζεται με τη λειτουργία των ΠΕΣ.

Δ2. Η Διοίκηση μεριμνά για την κατάρτιση σε θέματα ασφάλειας ΠΕΣ των διαχειριστών των συστημάτων και ειδικότερα των στελεχών που αναλαμβάνουν ρόλους σχετικούς με την ασφάλεια ΠΕΣ.

Δ3. Η Διοίκηση μεριμνά ώστε υπάρχουν ειδικά προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης του προσωπικού στην ασφάλεια ΠΕΣ.

Δ4. Το πρόγραμμα για την ευαισθητοποίηση των χρηστών σε θέματα ασφάλειας ΠΕΣ ακολουθεί τις αρχές του marketing.

Δ5. Η Διοίκηση μεριμνά ώστε να είναι διαθέσιμες στο προσωπικό πηγές πληροφόρησης για ζητήματα ασφάλειας, καθώς και εκπαιδευτικό υλικό, όπως μαθήματα από απόσταση, εκπαιδευτικά video κλπ.

Δ6. Περίληψη της Πολιτικής Ασφάλειας ΠΕΣ χορηγείται στο προσωπικό της Εταιρείας (μόνιμο ή προσωρινό), καθώς και στους προμηθευτές υπηρεσιών ή στους αναδόχους έργων που μπορεί να επηρεάσουν την ασφάλεια των ΠΕΣ.

Δ7. Ολα τα νέα μέλη του προσωπικού να ακολουθούν ένα βασικό πρόγραμμα εκπαίδευσης, το οποίο περιλαμβάνει και ζητήματα ασφάλειας ΠΕΣ.

Δ8. Τα διοικητικά στελέχη της Εταιρείας αποδεικνύουν την αυξημένη σημασία που έχει η ασφάλεια των ΠΕΣ, εφαρμόζοντας υποδειγματικά την Πολιτική Ασφάλειας ΠΕΣ και τις διαδικασίες ασφάλειας που απορρέουν από αυτήν.

Ε . Ελεγχος Εφαρμογής Πολιτικής Ασφάλειας ΠΕΣ

E1. Ολα τα τμήματα της Εταιρείας που έχουν την ευθύνη της διαχείρισης ΠΕΣ συντάσσουν και υποβάλλουν στον Υπεύθυνο Ασφάλειας ΠΕΣ εξαμηνιαία αναφορά στην οποία αναφέρουν τα μέτρα προστασίας που έχουν λάβει, τις διαδικασίες ασφάλειας που ακολουθούν και τα σχετικά συμβάντα που προέκυψαν σε αυτό το χρονικό διάστημα. Η αναφορά περιλαμβάνει αιτιολόγηση της επιλογής των μέτρων προστασίας και αξιολόγηση της αποτελεσματικότητάς τους.

E2. Τηρούνται αρχεία καταγραφής ενεργειών (audit logs), έτσι ώστε να είναι εφικτός ο έλεγχος της εφαρμογής της πολιτικής ασφάλειας από το προσωπικό.

E3. Υπάρχουν κατάλληλα μέσα για την ανάλυση των αρχείων καταγραφής και την εξαγωγή σχετικών αναφορών.

E4. Τα αρχεία καταγραφής προστατεύονται με τρόπο που διασφαλίζι ότι ούτε οι διαχειριστές των ΠΕΣ έχουν τη δυνατότητα να προβούν σε ενέργειες που δεν καταγράφονται.

E5. Πραγματοποιούνται τακτικοί και έκτακτοι έλεγχοι.

E6. Οι έλεγχοι πραγματοποιούνται τόσο από το αρμόδιο τμήμα της Εταιρείας, όσο και από εξωτερικούς ελεγκτές.

E7. Στόχος των ελέγχων είναι η βελτίωση του επιπέδου ασφάλειας των ΠΕΣ. Οι ελεγκτές λειτουργούν κατά κύριο λόγο συμβουλευτικά και κατά δεύτερο λόγο ελεγκτικά.

2.8 Πολιτική Προσωπικού

2.8.1 Εισαγωγή

Οπως δείχνουν σχετικές μελέτες, ο σημαντικότερος παράγοντας στην ασφάλεια ΠΕΣ είναι η συμπεριφορά και η δράση των ανθρώπων που μετέχουν της λειτουργίας των συστημάτων ως χρήστες ή ως διαχειριστές των συστημάτων ή ασκώντας διοικητικά καθήκοντα.

Η CubeIQ, αναγνωρίζοντας το σημαντικό ρόλο που διαδραματίζουν τα μέλη του προσωπικού στην προσπάθεια διασφάλισης της πληροφοριακής και επικοινωνιακής υποδομής της, ανέπτυξε και θέτει σε εφαρμογή την παρούσα Πολιτική Προσωπικού.

2.8.2 Σκοπός

Σκοπός της Πολιτικής Προσωπικού είναι:

- Η μείωση της επικινδυνότητας που συνδέεται με ανθρώπινα λάθη, με την πιθανή κατάχρηση των συστημάτων, καθώς και με κάθε εκούσια ή ακούσια ενέργεια που μπορεί να θέσει σε κίνδυνο τα ΠΕΣ.

- Η ενίσχυση της ενεργούς συμμετοχής του προσωπικού στη συλλογική προσπάθεια ενδυνάμωσης της ασφάλειας των ΠΕΣ.

2.8.3 Εμβέλεια

Η Πολιτική Προσωπικού απευθύνεται στο σύνολο του προσωπικού της CubeIQ που κατά την άσκηση των καθηκόντων του επηρεάζει τη λειτουργία των ΠΕΣ της CubeIQ , είτε ως χρήστης, είτε ως διαχειριστής, είτε ασκώντας διοικητικά καθήκοντα. Η Πολιτική Προσωπικού αφορά ιδιαίτερα τα στελέχη της CubeIQ που έχουν ως αρμοδιότητα τη διαχείριση του ανθρώπινου δυναμικού.

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας ΠΕΣ.

2.8.4 Γενικές Αρχές

Ρόλος του ανθρώπινου δυναμικού

Η Εταιρεία αποδίδει ιδιαίτερη βαρύτητα στο ρόλο που διαδραματίζει το ανθρώπινο δυναμικό στην προσπάθεια διασφάλισης των ΠΕΣ.

Ενίσχυση του ανθρώπινου δυναμικού

Η Εταιρεία προβαίνει σε όλες τις απαιτούμενες ενέργειες για την ενίσχυση του προσωπικού της με μέσα, κατευθυντήριες οδηγίες, πληροφόρηση και γνώση, ώστε να συμβάλλει με τον πλέον αποτελεσματικό τρόπο στην ασφάλεια ΠΕΣ.

Υποχρέωση ενεργούς συμμετοχής

Όλα τα μέλη του προσωπικού έχουν την υποχρέωση να συμβάλλουν ενεργά στην ασφάλεια της πληροφορικής και επικοινωνιακής υποδομής της Εταιρείας και να απέχουν από κάθε ενέργεια που μπορεί να θέσει σε κίνδυνο την ασφάλεια των ΠΕΣ.

2.8.5 Οδηγίες και Κανόνες Ασφάλειας

Α . Διαχείριση ανθρώπινου δυναμικού

A1. Η Εταιρεία επιλέγει προσωπικό με κατάλληλα τυπικά και ουσιαστικά προσόντα για να στελεχώσει θέσεις που είναι σημαντικές για την ασφαλή λειτουργία των ΠΕΣ.

A2. Η Εταιρεία προβαίνει σε έλεγχο των τυπικών προσόντων και των συστάσεων του προσωπικού το οποίο προσλαμβάνεται για να αναλάβει αρμοδιότητες που είναι σημαντικές για την ασφαλή λειτουργία των ΠΕΣ.

A3. Η σύμβαση εργασίας του νέου προσωπικού περιλαμβάνει όρους που θα προβλέπουν τη συμμόρφωση με την Πολιτική Ασφάλειας ΠΕΣ.

A4. Το νέο προσωπικό υπογράφει δήλωση περί μη αποκάλυψης εταιρικών πληροφοριών, καθώς και πληροφοριών που αφορούν τους συνδρομητές της CubeIQ .

A5. Η Εταιρεία σέβεται το δικαίωμα των υπαλλήλων της να προστατεύουν τα προσωπικά τους δεδομένα και δεν αποκαλύπτει σε άτομα που στερούνται ανάγκης γνώσης (need-to-know), εντός ή εκτός της Εταιρείας, δεδομένα που αναφέρονται σε υπαλλήλους της.

A6. Η Εταιρεία, χωρίς να παραβιάζει τα έννομα δικαιώματα των υπαλλήλων της, διατηρεί το δικαίωμα πρόσβασης στα δεδομένα που δημιουργούνται και αποθηκεύονται στα ΠΕΣ της.

A7. Η Εταιρεία επιβραβεύει τα μέλη του προσωπικού τα οποία, με τις ενέργειές τους, διακρίνονται για την αφοσίωσή τους στον κοινό στόχο της διασφάλισης των ΠΕΣ και των εταιρικών πληροφοριών.

A8. Η Εταιρεία αναλαμβάνει την πρωτοβουλία για τη θέσπιση ενός "κώδικα δεοντολογίας προσωπικού ΤΠΕ". Ο κώδικας πρέπει να απολαμβάνει ευρείας αποδοχής.

Β . Γενικές υποχρεώσεις προσωπικού

B1. Ολα τα μέλη του προσωπικού έχουν την υποχρέωση να συμβάλλουν θετικά στην ασφάλεια των ΠΕΣ της Εταιρείας.

B2. Ολα τα μέλη του προσωπικού οφείλουν να σέβονται την ιδιωτικότητα (privacy) των συναδέλφων τους.

B3. Το προσωπικό έχει την υποχρέωση να αποφεύγει τα δημόσια δυσφημιστικά σχόλια για πελάτες, συνεργάτες ή ανταγωνιστές της Εταιρείας.

B4. Τα μέλη του προσωπικού έχουν την υποχρέωση να αποφεύγουν αρνητικά σχόλια για τους συναδέλφους τους ή για την ίδια την Εταιρεία, παρά μόνο εάν αυτά εντάσσονται στις θεσμοθετημένες διαδικασίες διαλόγου, αξιολόγησης και ελέγχου της Εταιρείας.

B5. Τα μέλη του προσωπικού έχουν την υποχρέωση να αναφέρουν οποιοδήποτε γεγονός ή ενέργεια θεωρούν ότι περιορίζει την ασφάλεια των ΠΕΣ. Η Διοίκηση οφείλει να χρησιμοποιεί αυτές τις πληροφορίες με διακριτικό τρόπο.

2.9 Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΕΣ

2.9.1 Εισαγωγή

Η Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΕΣ ρυθμίζει τα ζητήματα που αφορούν στη χρήση των ΠΕΣ που υποστηρίζουν τις δραστηριότητες της CubeIQ . Με την έκδοση της πολιτικής αυτής δίνεται η δυνατότητα στους χρήστες των ΠΕΣ να γνωρίζουν ποιες ενέργειές τους θεωρούνται επιτρεπτές και ποιες απαγορεύονται.

2.9.2 Σκοπός

Σκοπός της Πολιτικής Θεμιτών Πρακτικών Χρήσης ΠΕΣ είναι:

- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από κακή χρήση των ΠΕΣ της Εταιρείας.

- Η προστασία των χρηστών των ΠΕΣ από τις συνέπειες που μπορεί να υποστούν από την εσφαλμένη χρήση των ΠΕΣ.

- Η διασφάλιση ότι οι χρήστες δεν θα καταχραστούν τις δυνατότητες χρήσης των ΠΕΣ που τους παρέχονται προκειμένου να προβούν σε παράνομες ενέργειες.

2.9.3 Εμβέλεια

Η πολιτική αυτή απευθύνεται στα μέλη του προσωπικού της CubeIQ και στους συνεργάτες της Εταιρείας που χρησιμοποιούν ΠΕΣ που υποστηρίζουν δραστηριότητες της CubeIQ .

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας ΠΕΣ.

2.9.4 Γενικές Αρχές

Αξία των ΠΕΣ

Τα ΠΕΣ συγκαταλέγονται στους πολυτιμότερους πόρους της Εταιρείας και κάθε μέλος του προσωπικού έχει την υποχρέωση να τα χρησιμοποιεί με προσοχή.

ΠΕΣ ως περιουσιακό στοιχείο

Τα ΠΕΣ που προσφέρονται στο προσωπικό της Εταιρείας αποτελούν περιουσιακό της στοιχείο και η χρήση τους πρέπει να γίνεται αποκλειστικά για τους σκοπούς της Εταιρείας.

Υποχρεώσεις συνδεόμενες με τη χρήση των ΠΕΣ

Η χρήση των ΠΕΣ συνεπάγεται την ανάληψη ευθυνών και υποχρεώσεων που περιγράφονται στην Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΕΣ.

2.9.5 Οδηγίες και Κανόνες Ασφάλειας

Α . Δικαιώματα και υποχρεώσεις χρηστών

A1. Το προσωπικό δικαιούται να χρησιμοποιεί τα ΠΕΣ της Εταιρείας σύμφωνα με τα όσα προβλέπονται στην παρούσα Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΕΣ.

A2. Το προσωπικό πρέπει να χρησιμοποιεί σωστά τα ΠΕΣ και να μην αρκείται στην κατά γράμμα εφαρμογή της Πολιτικής Θεμιτών Πρακτικών Χρήσης ΠΕΣ. Σε περίπτωση που κάποιο μέλος του προσωπικού

αμφιβάλλει αν κάποια ενέργειά του είναι συμβατή με την πολιτική, θα πρέπει να απευθύνεται στον Υπεύθυνο Ασφάλειας ΠΕΣ.

Α3. Οι χρήστες έχουν το δικαίωμα να ενημερώνονται σχετικά με τα δεδομένα που συλλέγονται από την Εταιρεία και αφορούν τη χρήση των ΠΕΣ από αυτούς.

Α4. Τα δεδομένα που δημιουργούνται με τη χρήση των ΠΕΣ της Εταιρείας αποτελούν ιδιοκτησία της Εταιρείας.

Α5. Οι χρήστες οφείλουν να σέβονται τους ελέγχους πρόσβασης (access controls), ακόμα και αν αυτοί είναι ανεπαρκείς.

Α6. Οι χρήστες πρέπει να μην παραβιάζουν τους μηχανισμούς ασφάλειας, έστω και αν έχουν στόχο να καταδείξουν τα αδύναμα σημεία τους. Εάν θεωρούν ότι οι μηχανισμοί είναι ανεπαρκείς, οφείλουν να το υποδείξουν στον Υπεύθυνο Ασφάλειας ΠΕΣ. Ο Υπεύθυνος Ασφάλειας ΠΕΣ θα εξετάσει την υπόθεση, χωρίς να απαιτήσει αποδείξεις.

Α7. Οσα μέλη του προσωπικού διαθέτουν φορητό υπολογιστή και τον χρησιμοποιούν για εργασιακούς σκοπούς πρέπει να συμμορφώνονται με τις πολιτικές που ισχύουν για το συμβατικό εξοπλισμό (προσωπικοί υπολογιστές κλπ.).

Α8. Οι χρήστες υποχρεούνται να συμμορφώνονται με την νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας.

Α9. Απαγορεύεται η χρήση λογισμικού που δεν έχει αποκτηθεί με νόμιμο τρόπο.

Α10. Απαγορεύεται η χρήση οποιουδήποτε υλικού ή λογισμικού που δεν είναι σε γνώση της Διεύθυνση Πληροφορικής της Εταιρείας.

Α11. Απαγορεύεται οποιαδήποτε ενέργεια μη εξουσιοδοτημένης χαρτογράφησης του δικτύου της εταιρείας.

Α12. Απαγορεύεται η χρήση μηχανισμού ασφάλειας (πχ. προσωπικά αναχώματα ασφάλειας (firewall), συστήματα προστασίας από ιομορφικό λογισμικό) που δεν έχουν την έγκριση του Υπεύθυνου Ασφάλειας ΠΕΣ.

Α13. Απαγορεύεται η χρήση μη εταιρικών συστημάτων για εταιρικές εργασίες.

Α14. Οι χρήστες οφείλουν να λαμβάνουν όλα τα μέτρα που υποδεικνύουν οι υπεύθυνοι της Εταιρείας για τη διασφάλιση του απορρήτου των επικοινωνιών τους.

Α15. Οι εργαζόμενοι στην Εταιρεία απαγορεύεται να αποκαλύπτουν πληροφορίες που συνδέονται με (α) το περιεχόμενο ή την ουσία των επικοινωνιών των πελατών της CubeIQ , (β) στοιχεία σχετικά με υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο ή (γ) άλλα προσωπικά δεδομένα των χρηστών των τηλεπικοινωνιακών υπηρεσιών, όπως αριθμούς τηλεφώνου ή διευθύνσεις.

Β . Παρακολούθηση και έλεγχος εφαρμογής της πολιτικής

Β1. Τα δεδομένα που δημιουργούνται με τη χρήση των ΠΕΣ της Εταιρείας αποτελούν ιδιοκτησία της Εταιρείας.

Β2. Η χρήση των ΠΕΣ μπορεί να καταγράφεται και να παρακολουθείται από εξουσιοδοτημένα άτομα. Οι χρήστες ενημερώνονται εφάπαξ ότι οι ενέργειές τους καταγράφονται.

Β3. Η Εταιρεία διατηρεί το δικαίωμα να διενεργεί προγραμματισμένους ή έκτακτους ελέγχους για την τήρηση της Πολιτικής Θεμιτών Πρακτικών Χρήσης ΠΕΣ και για την τήρηση των πολιτικών που συμπεριλαμβάνονται στην Πολιτική Ασφάλειας ΠΕΣ. Τους ελέγχους πραγματοποιούν εξουσιοδοτημένα για το σκοπό αυτό άτομα (Ελεγκτές ΠΕΣ) και τα μέλη του προσωπικού οφείλουν να συνεργαστούν με αυτούς. Το προσωπικό έχει δικαίωμα να ενημερωθεί για τα μέσα ελέγχου, τα κριτήρια ελέγχου και τα αποτελέσματα των ελέγχων που το αφορούν.

Γ . Χρήση Ηλεκτρονικού Ταχυδρομείου και Παγκόσμιου Ιστού

Γ1. Απαγορεύεται η χρήση του ηλεκτρονικού ταχυδρομείου για την αποστολή αυτόκλητων μηνυμάτων (unsolicited mail spam).

Γ2. Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου παρέχονται στο προσωπικό της Εταιρείας για να χρησιμοποιούνται αποκλειστικά για τους σκοπούς της Εταιρείας. Η Εταιρεία δεν είναι υποχρεωμένη να προστατεύει τα ηλεκτρονικά μηνύματα ως προσωπικά δεδομένα των υπαλλήλων.

Γ3. Ολα τα ηλεκτρονικά μηνύματα συνοδεύονται από κείμενο που δηλώνει ότι όσα αναφέρονται σε αυτό δεν απηχούν κατανάγκην τις απόψεις της Εταιρείας.

Γ4. Οι χρήστες πρέπει να γνωρίζουν ότι η εμπιστευτικότητα των ηλεκτρονικών μηνυμάτων δεν μπορεί να διασφαλιστεί παρά μόνο εάν εφαρμόζονται ειδικές τεχνικές κρυπτογράφησης.

Γ5. Οι χρήστες πρέπει να γνωρίζουν ότι ο παραλήπτης ενός μηνύματος μπορεί να το διατηρήσει για απροσδιόριστο χρόνο, να το προωθήσει σε τρίτους ή ακόμα να αλλοιώσει το περιεχόμενό του και έπειτα να το προωθήσει σε τρίτους.

Γ6. Οι χρήστες πρέπει να γνωρίζουν ότι η πραγματική ταυτότητα του αποστολέα ενός μηνύματος μπορεί να είναι διαφορετική από την αναγραφόμενη στο μήνυμα.

Γ7. Οι χρήστες δεν πρέπει να χρησιμοποιούν τους λογαριασμούς ηλεκτρονικού ταχυδρομείου συναδέλφων τους. Οποτε απαιτείται περισσότερα του ενός πρόσωπα να χρησιμοποιούν ένα λογαριασμό, τότε δημιουργείται ειδικός λογαριασμός με όνομα που δε συνδέεται με κάποιο πρόσωπο (πχ. info@CubeIQ .gr).

Γ8. Δεν πρέπει να αποστέλλονται εμπιστευτικές πληροφορίες εκτός της Εταιρείας με το ηλεκτρονικό ταχυδρομείο.

Γ9. Η πρόσβαση στο Διαδίκτυο παρέχεται στο προσωπικό της Εταιρείας για να χρησιμοποιηθεί για τους σκοπούς της Εταιρείας και για τη βελτίωση των γνώσεων και δεξιοτήτων του ανθρώπινου δυναμικού της.

Γ10. Η εταιρεία διατηρεί το δικαίωμα να περιορίσει την πρόσβαση σε συγκεκριμένους Ιστοτόπους (Web Sites) του Παγκόσμιου Ιστού (World Wide Web). Οι χρήστες που χρειάζονται πρόσβαση σε Ιστοτόπους που δεν έχουν εγκριθεί από την Εταιρεία έχουν το δικαίωμα να υποβάλλουν σχετικό αίτημα στον Υπεύθυνο Ασφάλειας ΠΕΣ.

Γ11. Οι χρήστες πρέπει να γνωρίζουν ότι οι δυνατότητες των γραμμών που συνδέουν την Εταιρεία με το Διαδίκτυο είναι πεπερασμένες και κατά συνέπεια η κατάχρηση των υπηρεσιών του Διαδικτύου (πχ. η λήψη μεγάλων αρχείων) περιορίζει τη χρήση του Διαδικτύου από τους συναδέλφους τους.

Γ12. Οι χρήστες πρέπει να αποφεύγουν την επίσκεψη σε Ιστοσελίδες (Web Pages) με παράνομο λογισμικό, μη πρέπον υλικό ή άλλο πειρατικό οπτικοακουστικό υλικό. Οι χρήστες πρέπει να γνωρίζουν ότι η επίσκεψη αυτών των Ιστοσελίδων μπορεί να θέσει σε κίνδυνο την ασφάλεια των ΠΕΣ.

Δ . Επιλογή και Διαχείριση Συνθηματικών

Δ1. Οι χρήστες δεν αποκαλύπτουν τα συνθηματικά τους σε τρίτους, έστω και εάν αυτοί είναι στενά συγγενικά πρόσωπα, υπάλληλοι της Εταιρείας, ανώτερα διοικητικά στελέχη ή ακόμα και οι διαχειριστές (μηχανικοί) των ΠΕΣ της Εταιρείας.

Δ2. Απαγορεύεται η αποκάλυψη της μεθόδου με την οποία ο χρήστης έχει επιλέξει το συνθηματικό του.

Δ3. Απαγορεύεται οποιοδήποτε σχόλιο για την ανθεκτικότητα του συνθηματικού και οποιοσδήποτε υπαινιγμός για τη σύνθεσή του.

Δ4. Απαγορεύεται στους χρήστες να γνωστοποιούν το συνθηματικό τους σε συναδέλφους τους, όταν πρόκειται να απουσιάσουν (πχ. λόγω αδείας ή ασθενείας). Οι χρήστες πρέπει να συμβουλεύονται τον Υπεύθυνο Ασφάλειας ΠΕΣ για τον τρόπο με τον οποίο μπορεί να επιτευχθεί η συνέχεια των εργασιών που έχουν αναλάβει.

Δ5. Οι χρήστες πρέπει να αλλάζουν το συνθηματικό τους σε κάθε περίπτωση που θεωρούν ότι μπορεί ή έχει ήδη αποκαλυφθεί.

Δ6. Τα συνθηματικά των χρηστών πρέπει να αλλάζουν τουλάχιστον κάθε τρεις μήνες.

Δ7. Τα συνθηματικά δεν πρέπει να καταγράφονται ή να αναφέρονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, επιστολές κλπ.

Δ8. Απαγορεύεται η χρήση λειτουργιών αυτόματης συμπλήρωσης συνθηματικού, όπως η λειτουργία "remember password", καθώς και η αποθήκευση των συνθηματικών σε υπολογιστές ή συσκευές (PDA, κινητά τηλέφωνα κλπ.) χωρίς κρυπτογράφηση.

Δ9. Απαγορεύεται η χρήση συνθηματικών (α) με λιγότερους από οκτώ χαρακτήρες, (β) που περιέχουν μέρος ή ολόκληρο το αναγνωριστικό χρήστη (user name), (δ) που είναι δυνατόν να περιλαμβάνονται σε κάποιο λεξικό, (ε) είναι κοινές λέξεις, όπως ονόματα κλπ., (στ) είναι λέξεις που σχετίζονται με την επωνυμία της Εταιρείας ή των προϊόντων της, (ζ) είναι πληροφορίες που αφορούν το χρήστη, όπως η ημερομηνία γέννησης κλπ., (η) επαναλαμβάνουν τον ίδιο χαρακτήρα πολλές φορές ή έχουν ακολουθίες αριθμών ή γραμμάτων, (θ) οποιαδήποτε από τα ανωτέρω συλλαβισμένο ανάποδα ή με ένα χαρακτήρα εμπρός ή πίσω.

Δ10. Απαγορεύεται η χρήση των ίδιων συνθηματικών για συστήματα της Εταιρείας και για συστήματα ή υπηρεσίες εκτός Εταιρείας (πχ. οικιακοί υπολογιστές).

Δ11. Χρησιμοποιούνται διαφορετικά συνθηματικά για συστήματα με διαφορετικό βαθμό ευαισθησίας.

2.10 Πολιτική Προστασίας Προσωπικών Δεδομένων και Επικοινωνιών

2.10.1 Εισαγωγή

Η CubeIQ έχει την υποχρέωση να προστατεύει τα προσωπικά δεδομένα των πελατών της, καθώς κάθε άλλου προσώπου για το οποίο επεξεργάζεται πληροφορίες, και να διαφυλάσσει το απόρρητο των επικοινωνιών στο βαθμό που αυτό εξαρτάται από τα ΠΕΣ.

Η πολιτική καθορίζει τον τρόπο με τον οποίο η Εταιρεία και το προσωπικό της επιτυγχάνουν την τήρηση αυτών των υποχρεώσεων.

2.10.2 Σκοπός

Σκοπός της Πολιτικής Προστασίας Προσωπικών Δεδομένων και Επικοινωνιών είναι:

- Η συμμόρφωση της Εταιρείας με τις νομικές και κανονιστικές υποχρεώσεις προστασίας προσωπικών δεδομένων και διασφάλισης του απορρήτου των επικοινωνιών.

- Η προστασία της ιδιωτικότητας των πελατών της CubeIQ .

2.10.3 Εμβέλεια

Η πολιτική αφορά τα μέλη του προσωπικού και τους συνεργάτες της Εταιρείας που έχουν ή μπορεί να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα, καθώς και όσους μπορεί να έχουν πρόσβαση ή εμπλέκονται με οποιοδήποτε τρόπο στις επικοινωνίες των πελατών της.

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας ΠΕΣ.

2.10.4 Γενικές Αρχές

Συμμόρφωση με νομικές απαιτήσεις για προστασία προσωπικών δεδομένων

Η Εταιρεία προβαίνει σε όλες τις ενέργειες που απαιτούνται για τη τήρηση των υποχρεώσεών της που απορρέουν από το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων.

Διασφάλιση απορρήτου των επικοινωνιών

Η Εταιρεία προβαίνει σε όλες τις ενέργειες που απαιτούνται για τη τήρηση των υποχρεώσεών της που απορρέουν από το νομοθετικό και κανονιστικό πλαίσιο που αφορά τη διασφάλιση του απορρήτου των επικοινωνιών.

Υποχρέωση νομικής συμμόρφωσης προσωπικού

Ολοι όσοι εργάζονται για την Εταιρεία ή συνεργάζονται με αυτήν έχουν την υποχρέωση να συμβάλλουν στην προστασία των προσωπικών δεδομένων και τη διασφάλιση του απορρήτου των επικοινωνιών.-

2.10.5 Οδηγίες και Κανόνες Ασφάλειας

Α . Προστασία Προσωπικών Δεδομένων

Α1. Η Εταιρεία τηρεί το Ν. 2472/97 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, το Ν. 2774/99 περί προστασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, καθώς το Ν. 2225/94 περί προστασίας της ελευθερίας ανταπόκρισης και επικοινωνίας.

Α2. Η Εταιρεία γνωστοποιεί στην Αρχή Προστασίας Προσωπικών Δεδομένων την τήρηση οποιουδήποτε αρχείου προσωπικών δεδομένων.

Α3. Η Εταιρεία επεξεργάζεται προσωπικά δεδομένα πελατών της μόνο μετά την ενημέρωσή τους και εφόσον έχει τη συγκατάθεση των πελατών της, όπως ο Νόμος ορίζει.

Α4. Η Εταιρεία ενημερώνει τους πελάτες της για την επεξεργασία των προσωπικών τους δεδομένων, όπως ορίζει η σχετική νομοθεσία.

Α5. Η Εταιρεία επεξεργάζεται προσωπικά δεδομένα των υπαλλήλων της μόνο για λόγους που συνδέονται με την άσκηση της εργασίας τους.

Α6. Η Εταιρεία δεν μεταβιβάζει, ούτε αποκαλύπτει στοιχεία των πελατών της σε τρίτους, παρά μόνο κατόπιν δικαστικής ή εισαγγελικής εντολής ή όταν επιβάλλεται από το νόμο. Σε κάθε άλλη περίπτωση απαιτείται η ρητή συγκατάθεση του υποκειμένου.

Α7. Η επεξεργασία δεδομένων που αφορούν πελάτες της CubeIQ γίνεται μόνο για τους σκοπούς που σχετίζονται με την παροχή υπηρεσιών σε αυτούς.

Α8. Η συλλογή προσωπικών δεδομένων περιορίζεται μόνο στα δεδομένα που είναι απαραίτητα για την εκπλήρωση συμβατικών και νομικών υποχρεώσεων της Εταιρείας.

Α9. Η πρόσβαση του προσωπικού της Εταιρείας στα προσωπικά δεδομένα των πελατών της περιορίζεται με βάση την αρχή ανάγκης γνώσης (need-to-know).

Α10. Οι πελάτες της εταιρείας έχουν δικαίωμα πρόσβασης στις πληροφορίες που τους αφορούν. Για την άσκηση του δικαιώματος αυτού η Εταιρεία μπορεί να ζητήσει την καταβολή εύλογου αντίτιμου. Το αντίτιμο καταβάλλεται για να καλύψει έξοδα της Εταιρείας, συνεπώς η Εταιρεία δεν απολαμβάνει κέρδος από αυτό.

Α11. Οι πελάτες έχουν το δικαίωμα να ζητήσουν τη διόρθωση προσωπικών τους στοιχείων που είναι αναληθή ή ανακριβή.

Α12. Η Εταιρεία δεν παρακολουθεί, ούτε καταγράφει το περιεχόμενο των επικοινωνιών των πελατών της.

Α13. Η Εταιρεία λαμβάνει μέτρα για την προστασία του απορρήτου των επικοινωνιών ανάλογα με την επικινδυνότητα, όπως αυτή προκύπτει από σχετική μελέτη.

Α14. Αναφορικά με τη λειτουργία του κινητού τηλεπικοινωνιακού δικτύου, η Εταιρεία λαμβάνει όλα τα απαραίτητα μέτρα για (α) τη διασφάλιση του απορρήτου της ταυτότητας του συνδρομητή, (β) την πιστοποίηση της ταυτότητας του συνδρομητή, έτσι ώστε οι χρεώσεις να γίνονται σωστά, (γ) την προστασία των δεδομένων σηματοδοσίας, ώστε δεδομένα όπως αριθμοί τηλεφώνου να μην μπορούν να υποκλαπούν και (δ) την προστασία του απορρήτου του περιεχομένου της συνομιλίας. Τα μέτρα αυτά εφαρμόζονται στο τμήμα του κινητού τηλεπικοινωνιακού δικτύου που αποτελεί ιδιοκτησία ή βρίσκεται υπό τον έλεγχο της Εταιρείας.

Β . Πολιτική Άρσης του Απορρήτου των Επικοινωνιών

Β1. Η Εταιρεία δεν μπορεί να άρει το απόρρητο των επικοινωνιών στην περίπτωση που ένας από τους συμμετέχοντες στη συνδιάλεξη το ζητήσει.

Β2. Η Εταιρεία αίρει το απόρρητο των επικοινωνιών μόνο κατόπιν δικαστικής ή εισαγγελικής εντολής και σύμφωνα με τα όσα ορίζει ο Ν. 2225/94 και ο Ν. 2774/99.

Β3. Η Εταιρεία συντάσσει ειδικό σχέδιο που περιγράφει με σαφήνεια και σύμφωνα με τα προβλεπόμενα από το νόμο, το μηχανισμό, τη διαδικασία και τους υπεύθυνους εφαρμογής της άρσης του απορρήτου. Το σχέδιο προβλέπει και μέτρα για την αντιμετώπιση τυχόν προβλημάτων εμφανισθούν κατά τη φάση της άρσης και της αποκατάστασης της προστασίας του απορρήτου μετά την ολοκλήρωση της διαδικασίας άρσης του.

2.11 Πολιτική Αναδόχων και Συνεργατών

2.11.1 Εισαγωγή

Οι δραστηριότητες των συνεργατών της CubeIQ, είτε πρόκειται για φυσικά πρόσωπα είτε για εταιρείες που αναλαμβάνουν διάφορες εργασίες, όπως εργασίες ανάπτυξης και συντήρησης συστημάτων, εκτυπωτικές εργασίες κλπ., καθώς και των προμηθευτών υπηρεσιών, όπως οι τηλεπικοινωνιακές υπηρεσίες, μπορεί να θέσουν σε κίνδυνο την εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ της Εταιρείας.

Η Εταιρεία διατηρεί την ευθύνη απέναντι στο Νόμο για την παραβίαση του απορρήτου των επικοινωνιών ή την κατάχρηση των προσωπικών δεδομένων των πελατών όταν αυτή προέλθει από συνεργάτες της Εταιρείας ή από αναδόχους εργασιών. Για αυτούς τους λόγους πρέπει να διασφαλίζεται ότι αυτοί οι ανάδοχοι και οι συνεργάτες συμμορφώνονται και εφαρμόζουν τα όσα ορίζει η Πολιτική Ασφάλειας ΠΕΣ.

2.11.2 Σκοπός

Σκοπός της Πολιτικής Αναδόχων και Συνεργατών είναι:

- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από τις δραστηριότητες των αναδόχων εργασιών και των συνεργατών της Εταιρείας.

- Να διασφαλιστεί ότι προστατεύονται τα προσωπικά δεδομένα και το απόρρητο των επικοινωνιών των πελατών της CubeIQ .

2.11.3 Εμβέλεια

Η πολιτική αφορά τους συνεργάτες της CubeIQ, είτε πρόκειται για φυσικά, είτε για νομικά πρόσωπα που έχουν ή μπορεί να έχουν πρόσβαση στα ΠΕΣ ή στις πληροφορίες που συλλέγει και επεξεργάζεται η CubeIQ. Επίσης, αφορά αναδόχους εργασιών και προμηθευτές υπηρεσιών που έχουν ή μπορει να έχουν πρόσβαση στα ΠΕΣ ή στις πληροφορίες που συλλέγει και επεξεργάζεται η CubeIQ.

Η εφαρμογή της πολιτικής είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της σύμβασης συνεργασίας.

2.11.4 Γενικές Αρχές

Υποχρεώσεις αναδόχων και συνεργατών

Οι συνεργάτες της εταιρείας και οι ανάδοχοι εργασιών έχουν τις ίδιες υποχρεώσεις αναφορικά με την ασφάλεια ΠΕΣ που έχει και το προσωπικό της Εταιρείας.

Διασφάλιση απορρήτου των επικοινωνιών

Η Εταιρεία προβαίνει σε όλες τις ενέργειες που διασφαλίζουν ότι οι δραστηριότητες των αναδόχων και των συνεργατών δεν θέτουν σε κίνδυνο τα δικαιώματα των πελατών της αναφορικά με την προστασία των προσωπικών τους δεδομένων και τη διασφάλιση του απορρήτου των επικοινωνιών.

Προστασία ΠΕΣ από ενέργειες αναδόχων και συνεργατών

Η Εταιρεία αναγνωρίζει τους κινδύνους που προέρχονται από τις δραστηριότητες των συνεργατών της και των αναδόχων εργασιών και λαμβάνει όλα τα μέτρα ώστε να τους περιορίσει.

2.11.5 Οδηγίες και Κανόνες Ασφάλειας

Α . Υποχρεώσεις Αναδόχων και Συνεργατών

Α1. Οι ανάδοχοι εργασιών και οι συνεργάτες της Εταιρείας οφείλουν να γνωρίζουν και να εφαρμόζουν την Πολιτική Ασφάλειας ΠΕΣ της Εταιρείας. Για το προσωπικό των αναδόχων που εκτελούν εργασίες στις εγκαταστάσεις ή/και στα ΠΕΣ της Εταιρείας ισχύουν οι ίδιοι κανόνες με το προσωπικό της Εταιρείας.

Α2. Οι ανάδοχοι εργασιών και οι συνεργάτες της Εταιρείας οφείλουν να αναφέρουν κάθε περιστατικό που μπορεί να θέσει σε κίνδυνο τα ΠΕΣ της Εταιρείας.

Α3. Οι ανάδοχοι εργασιών και οι συνεργάτες της Εταιρείας οφείλουν να διατηρούν την εμπιστευτικότητα των δεδομένων στα οποία αποκτούν πρόσβαση.

Α4. Οι ανάδοχοι εργασιών και οι συνεργάτες της Εταιρείας απαγορεύεται να αποκαλύπτουν πληροφορίες ή άλλα στοιχεία που συνδέονται με (α) το περιεχόμενο ή την ουσία των επικοινωνιών των πελατών της, (β) στοιχεία σχετικά με υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο ή (γ) άλλα προσωπικά δεδομένα χρηστών των τηλεπικοινωνιακών υπηρεσιών, όπως αριθμούς τηλεφώνου ή διευθύνσεις.

Β . Προκηρύξεις Διαγωνισμών και Συμβάσεις

Β1. Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των ΠΕΣ της Εταιρείας περιλαμβάνουν όρους που εξασφαλίζουν συμβατικά και τεχνικά την τήρηση της Πολιτικής Ασφάλειας ΠΕΣ της Εταιρείας.

Β2. Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των ΠΕΣ της Εταιρείας περιλαμβάνουν ρήτρες σε περίπτωση μη συμμόρφωσης με την Πολιτική Ασφάλειας ΠΕΣ της Εταιρείας.

Β3. Για την πρόσβαση σε προσωπικά δεδομένα πελατών ή σε δεδομένα που αφορούν τις επικοινωνίες των πελατών της CubeIQ απαιτείται η λήψη άδειας από τον Υπεύθυνο Ασφάλειας ΠΕΣ.

Β4. Ο Υπεύθυνος Ασφάλειας ΠΕΣ οφείλει να ελέγχει και να γνωμοδοτεί για την επάρκεια των όρων της σύμβασης σε σχέση με την ασφάλεια ΠΕΣ, όπως επίσης και για τη δυνατότητα του αναδόχου ή συνεργάτη να ανταποκριθεί στις απαιτήσεις ασφάλειας που θέτει η Εταιρεία.

Β5. Οι όροι που αφορούν την τήρηση της Πολιτικής Ασφάλειας ΠΕΣ περιλαμβάνονται και στις προκηρύξεις των έργων.

Β6. Τα άτομα που πραγματοποιούν εργασίες στα ΠΕΣ της Εταιρείας καταγράφονται και η ταυτότητά τους ελέγχεται.

Β7. Εξωτερικά συνεργεία συντήρησης, επισκευών και καθαρισμού συνοδεύονται διαρκώς από άτομα της Εταιρείας όταν βρίσκονται σε ευαίσθητους χώρους.

2.12 Πολιτική Προστασίας ΠΕΣ

2.12.1 Εισαγωγή

Η Πολιτική Προστασίας ΠΕΣ προδιαγράφει τα μέσα και τις διαδικασίες με τα οποία διασφαλίζονται τα ΠΕΣ της Εταιρείας. Η Πολιτική αναφέρεται κυρίως στα τεχνικά μέσα και στις διαδικασίες που εφαρμόζουν οι διαχειριστές-μηχανικοί της Εταιρείας.

Με την πολιτική αυτή διασφαλίζεται ότι υφίσταται και λειτουργεί ένα επαρκές σύστημα ασφάλειας, ικανό να επιτύχει τους σχετικούς με την ασφάλεια στόχους, όπως αυτοί περιγράφονται στην Πολιτική Ασφάλειας ΠΕΣ.

2.12.2 Σκοπός

Σκοπός της Πολιτικής Προστασίας ΠΕΣ είναι:

- Να προδιαγράψει τα απαιτούμενα μέσα και τις κατάλληλες διαδικασίες για την προστασία των ΠΕΣ από εκούσιες ή ακούσιες απειλές.

- Να διασφαλίσει ότι τα τεχνικά μέτρα προστασίας επαρκούν για την εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ.

- Να διασφαλίσει ότι η Εταιρεία έχει τα τεχνικά μέσα που απαιτούνται για να ανταποκριθεί στις νομικές, κανονιστικές και συμβατικές υποχρεώσεις της.

2.12.3 Εμβέλεια

Η Πολιτική Προστασίας ΠΕΣ αφορά το σύνολο των συστημάτων που υποστηρίζουν τις δραστηριότητες της CubeIQ ή που μπορεί να επηρεάσουν τις δραστηριότητές της.

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας ΠΕΣ.

2.12.4 Γενικές Αρχές

Τεχνική επάρκεια μέσων προστασίας

Η Εταιρεία εγκαθιστά ένα σύνολο μέσων προστασίας και εφαρμόζει διαδικασίες ικανές να διασφαλίσουν, από τεχνική άποψη, την εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ.

Προσανατολισμός μέσων προστασίας

Τα μέσα προστασίας έχουν ως στόχο την προστασία των ΠΕΣ τόσο από εξωτερικές όσο και από εσωτερικές απειλές.

Εύρος απειλών

Τα μέσα προστασίας αποσκοπούν στην προστασία των ΠΕΣ τόσο από κακόβουλες όσο και από ακούσιες ενέργειες, όπως επίσης και από απειλές που προέρχονται από τεχνικούς και περιβαλλοντικούς παράγοντες.

2.12.5 Οδηγίες και Κανόνες Ασφάλειας

Α . Ανάπτυξη ή προμήθεια συστημάτω ν και εγκατάστασή τους

A1. Ολες οι προμήθειες συστημάτων βασίζονται σε προδιαγραφές, οι οποίες λαμβάνουν υπόψη και τα ζητήματα ασφάλειας.

A2. Στις περιπτώσεις που οι προμήθειες συστημάτων γίνονται με διαγωνισμό, τότε οι προδιαγραφές ασφάλειας αναφέρονται στο κείμενο της διακήρυξης.

A3. Οι προδιαγραφές ασφάλειας ελέγχονται από τον Υπεύθυνο Ασφάλειας ΠΕΣ, καθώς και από τη διεύθυνση που θα αναλάβει τη διαχείριση των συστημάτων έπειτα από την εγκατάστασή τους.

A4. Ολα τα συστήματα ελέγχονται και τίθενται σε δοκιμαστική λειτουργία πριν τεθούν σε παραγωγική λειτουργία.

A5. Ολα τα συστήματα, ανεξαρτήτως μεγέθους και πολυπλοκότητας, που αναπτύσσονται από στελέχη της Εταιρείας ενσωματώνουν επαρκείς μηχανισμούς ασφάλειας. Ιδιαίτερη προσοχή αποδίδεται στην αυθεντικοποίηση (authentication) και τον έλεγχο πρόσβασης των χρηστών.

Β . Έλεγχος πρόσβασης

B1. Η απονομή δικαιωμάτων πρόσβασης στα ΠΕΣ της εταιρείας ακολουθεί την αρχή ανάγκης γνώσης (need-to-know).

B2. Τα δικαιώματα πρόσβασης που παρέχονται σε κάθε πρόσωπο ή διεργασία λογισμικού (software process) καταγράφονται και τηρείται σχετικός κατάλογος.

B3. Η πρόσβαση στα ΠΕΣ ελέγχεται από κατάλληλους μηχανισμούς ελέγχου πρόσβασης.

Β4. Η Εταιρεία τηρεί σαφείς διαδικασίες για τη προσθήκη νέων χρηστών, τις μεταβολές στα επίπεδα πρόσβασης των χρηστών, την πρόσβαση σε κρυπτογραφικούς μηχανισμούς, κλειδιά κλπ.

Β5. Η Εταιρεία προδιαγράφει τους μηχανισμούς ταυτοποίησης και ελέγχου πρόσβασης που εφαρμόζει.

Β6. Οι μηχανισμοί ελέγχου πρόσβασης καλύπτουν τα δεδομένα σε όλες τις μορφές τους, συμπεριλαμβανομένων των μαγνητικών ή οπτικών μέσων μεταφοράς, τα εφεδρικά αντίγραφα δεδομένων (back up), τα δεδομένα που μεταβιβάζονται μέσω δικτύων ή τηλεπικοινωνιακών γραμμών, δεδομένα σε έντυπη μορφή κλπ.

Β7. Οι μηχανισμοί ελέγχου πρόσβασης διασφαλίζουν ότι υπάρχει δυνατότητα ταυτοποίησης του ατόμου που πραγματοποίησε μία ενέργεια. Η αρχή αυτή ισχύει τόσο για τους χρήστες, όσο και για τους διαχειριστές (μηχανικούς, τεχνικούς κλπ.).

Β8. Οι διαχειριστές των συστημάτων δεν έχουν τη δυνατότητα να παρακάμψουν τους μηχανισμούς ελέγχου πρόσβασης χωρίς εξουσιοδότηση και με την προϋπόθεση ότι η ενέργειά τους αυτή καταγράφεται και ελέγχεται.

Β9. Οι χρήστες λαμβάνουν οδηγίες για την επιλογή και διαχείριση των συνθηματικών τους.

Β10. Η αυστηρότητα των μηχανισμών ελέγχου πρόσβασης είναι αντίστοιχη της διαβάθμισης των δεδομένων.

Γ . Αντιμετώπιση Περιστατικών και Διασφάλιση Συνέχειας Λειτουργίας

Γ1. Ολα τα ύποπτα περιστατικά αναφέρονται στον Υπεύθυνο Ασφάλειας ΠΕΣ. Για αυτόν το σκοπό αναπτύσσονται διαδικασίες που διευκολύνουν την αναφορά τους.

Γ2. Το προσωπικό ενθαρρύνεται να αναφέρει ύποπτα περιστατικά, έστω και εάν υπάρχουν περιορισμένες πιθανότητες να αφορούν πραγματική απειλή για τα ΠΕΣ της Εταιρείας.

Γ3. Ολα τα ύποπτα περιστατικά διερευνώνται.

Γ4. Σε περιπτώσεις όπου υπάρχουν ποινικά αδικήματα τα στοιχεία διαβιβάζονται στις εισαγγελικές αρχές.

Γ5. Η γνώση που προκύπτει από τη διερεύνηση των ύποπτων περιστατικών αξιοποιείται για τη βελτίωση της ασφάλειας των ΠΕΣ.

Γ6. Η διαδικασίες συλλογής στοιχείων είναι διαφανείς και δεν αφήνουν περιθώρια αμφισβήτησης των στοιχείων.

Γ7. Η διερεύνηση των περιστατικών ακολουθεί το τεκμήριο αθωότητας.

Γ8. Αναπτύσσεται και εφαρμόζεται σχέδιο συνέχειας λειτουργίας (business continuity plan).

Γ9. Το σχέδιο συνέχειας λειτουργίας βασίζεται στις απαιτήσεις διαθεσιμότητας των ΠΕΣ και ακεραιότητας των πληροφοριών.

Γ10. Το σχέδιο συνέχειας λειτουργίας λαμβάνει υπόψη την πιθανότητα καταστροφικών γεγονότων που μπορεί να θέσουν εκτός λειτουργίας ολόκληρες εγκαταστάσεις (πχ. σεισμός, πυρκαγιά, τρομοκρατική επίθεση κλπ.).

Δ . Χρήση κρυπτογραφικών μεθόδων

Δ1 Χρησιμοποιούνται κρυπτογραφικές μέθοδοι που ακολουθούν διεθνή πρότυπα.

Δ2 Δεν χρησιμοποιούνται κρυπτογραφικές μέθοδοι που δεν έχουν τεθεί σε δημόσιο έλεγχο.

Δ3. Επιλέγονται κρυπτογραφικές μέθοδοι ανάλογα με την εφαρμογή για την οποία χρησιμοποιούνται.

Δ4. Η χρήση κρυπτογραφικών μεθόδων γίνεται σύμφωνα με το νομοθετικό και κανονιστικό πλαίσιο που ισχύει στη χώρα.

Δ5. Το μήκος του κλειδιού έχει επαρκές μέγεθος και έχει εγκριθεί από τον Υπεύθυνο Ασφάλειας ΠΕΣ.

Δ6. Η διαχείριση των κλειδιών εξασφαλίζει αφενός ότι δεν παραβιάζεται η πολιτική ελέγχου πρόσβασης και αφετέρου ότι δεν υφίσταται κίνδυνος απώλειας των δεδομένων λόγω απώλειας των κλειδιών.

Ε . Ασφάλεια εγκαταστάσεω ν

Ε1. Οι εγκαταστάσεις που επιλέγονται για να στεγάσουν κρίσιμες λειτουργίες των ΠΕΣ παρέχουν επαρκή προστασία από κλοπή, τρομοκρατική ενέργεια, βανδαλισμούς, φωτιά, πλημμύρα, σεισμό, ή άλλες φυσικές καταστροφές και κινδύνους.

Ε2. Οι εγκαταστάσεις είναι κατάλληλες ώστε να διασφαλίσουν την απρόσκοπτη λειτουργία του εξοπλισμού.

Ε3. Χρησιμοποιούνται σύγχρονες τεχνολογίες ελέγχου πρόσβασης (πχ. proximity cards), προκειμένου να διασφαλίζεται ο επαρκής έλεγχος σε συνδυασμό με την ευκολία πρόσβασης και διακίνησης των εξουσιοδοτημένων προσώπων.

ΣΤ . Προστασία συστημάτων

ΣΤ1. Ο σχεδιασμός προστασίας του λογισμικού προστατεύει το λογισμικό εφαρμογών, το λογισμικό συστήματος και τα εργαλεία ανάπτυξης.

ΣΤ2. Τα δίκτυα διαχωρίζονται ανάλογα με τη διαβάθμιση των δεδομένων που διακινούνται σε αυτά.

ΣΤ3. Τα δίκτυα προστατεύονται τόσο από εσωτερικές, όσο και από εξωτερικές απειλές.

ΣΤ4. Η προστασία των δικτύων περιλαμβάνει και την προστασία του δικτυακού εξοπλισμού.

ΣΤ5. Εγκαθίστανται αποτελεσματικοί μηχανισμοί για την προστασία των ΠΕΣ της Εταιρείας από ιομορφικό λογισμικό.

ΣΤ6. Η χρήση του ηλεκτρονικού ταχυδρομείου και του Διαδικτύου ελέγχεται, ώστε να μην εκτίθενται σε κινδύνους τα ΠΕΣ της Εταιρείας.

ΣΤ7. Η ανεπιθύμητη ηλεκτρονική αλληλογραφία (spam) περιορίζεται.

ΣΤ8. Ο βασικός εξοπλισμός ΤΠΕ προστατεύεται, τόσο φυσικά, όσο και λογικά.

2.13 Σύνοψη Πολιτικής Ασφάλειας ΠΕΣ

Η Πολιτική Ασφάλειας ΠΕΣ αποτελεί ένα εκτενές κείμενο, το οποίο, αν και είναι γραμμένο σε απλή και απαλλαγμένη από τεχνικούς όρους γλώσσα, δύσκολα θα εντυπωθεί τη μνή-
μη όσων επιχειρήσουν να το μελετήσουν.

Επιπλέον, πρέπει να ληφθεί υπόψη το γεγονός ότι οι επιμέρους πολιτικές που απαρτίζουν την Πολιτική Ασφάλειας ΠΕΣ απευθύνονται σε διαφορετικούς αποδέκτες εντός και εκτός της Εταιρείας. Για παράδειγμα, η Πολιτική Θεμιτών Πρακτικών Χρήσης ΠΕΣ απευθύνεται στους απλούς χρήστες των συστημάτων, η Πολιτική Διαχείρισης Ασφάλειας ΠΕΣ στα διοικητικά στελέχη της Εταιρείας και η Πολιτική Αναδόχων και Συνεργατών απευθύνεται σε άτομα εκτός της Εταιρείας.

Κατά συνέπεια θα ήταν χρήσιμο να συνταχθούν περιλήψεις των πολιτικών για κάθε κατηγορία αποδεκτών. Οι περιλήψεις θα έχουν τα βασικά σημεία και θα διανέμονται με πρόσφορο τρόπο.

Στις παραγράφους που ακολουθούν προτείνονται τέσσερις περιλήψεις, οι οποίες απευθύνονται στους χρήστες των συστημάτων, στα διοικητικά στελέχη, στους διαχειριστές (μηχανικούς) των συστημάτων και στους εξωτερικούς συνεργάτες, αναδόχους εργασιών και προμηθευτές υπηρεσιών.

2.13.1 Σύνοψη Πολιτικής Ασφάλειας ΠΕΣ για τους Χρήστες των Συστημάτων

Τι πρέπει να προσέχετε:

Η ασφάλεια των Πληροφοριακών και Επικοινωνιακών Συστημάτων (ΠΕΣ) της Εταιρείας αποτελεί ζήτημα μεγάλης σπουδαιότητας. Είναι υποχρέωση όλων των εργαζομένων να συμβάλλουν ενεργά στην προσπάθεια αυτή. Ιδιαίτερη προσοχή οφείλεται στα παρακάτω:

- Η εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ είναι υποχρεωτική. Ολα τα μέλη του προσωπικού έχουν την υποχρέωση να μελετήσουν τα κείμενα όπου περιγράφεται.

- Η Εταιρεία θα πραγματοποιεί ελέγχους τήρησης της Πολιτικής Ασφάλειας ΠΕΣ και διατηρεί το δικαίωμα να επιβάλλει κυρώσεις σε περιπτώσεις παραβίασης.

- Η χρήση των ΠΕΣ μπορεί να εποπτεύεται από ειδικά εξουσιοδοτημένα για αυτόν το σκοπό άτομα.

- Η Εταιρεία διατηρεί το δικαίωμα πρόσβασης σε όλα τα δεδομένα που δημιουργούνται και αποθηκεύονται στα ΠΕΣ της.

- Η Εταιρεία διατηρεί το δικαίωμα να περιορίσει την πρόσβαση σε συγκεκριμένους Ιστοτόπους (Web Sites) του Παγκόσμιου Ιστού (World Wide Web). Οι χρήστες που χρειάζονται πρόσβαση σε Ιστοτόπους που δεν έχουν εγκριθεί από την Εταιρεία πρέπει να υποβάλλουν σχετικό αίτημα στον Υπεύθυνο Ασφάλειας ΠΕΣ.

- Οι χρήστες πρέπει να γνωρίζουν ότι η εμπιστευτικότητα των μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails) και των πληροφοριών που διακινούνται μέσω του Διαδικτύου δεν διασφαλίζεται επαρκώς.

Δεν επιτρέπεται να:

- Χρησιμοποιείτε τα συστήματα της Εταιρείας για παράνομες δραστηριότητες.

- Χρησιμοποιείτε συσκευές ή λογισμικό που δεν έχει εγκριθεί από τη Διεύθυνση Πληροφορικής.

- Χρησιμοποιείτε μη εταιρικά συστήματα για εταιρικές εργασίες.

- Χρησιμοποιείτε συστήματα της Εταιρείας για μη εταιρικές εργασίες.

- Αποκαλύπτετε οποιαδήποτε δεδομένα αφορούν την Εταιρεία ή πελάτες της σε τρίτους.

- Χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο για την αποστολή εμπιστευτικών εταιρικών πληροφοριών σε παραλήπτες εκτός της Εταιρείας.

- Να επισκέπτεστε Ιστότοπους (Web Sites) με παράνομο λογισμικό, μη πρέπον υλικό ή άλλο πειρατικό οπτικοακουστικό υλικό.

- Αποκαλύπτετε τα συνθηματικά σας (passwords) σε τρίτους, έστω και εάν αυτοί είναι συγγενικά πρόσωπα, υπάλληλοι της Εταιρείας, ανώτερα διοικητικά στελέχη ή ακόμα και διαχειριστές (μηχανικοί) των συστημάτων της Εταιρείας.

- Γνωστοποιείτε το συνθηματικό σας σε συναδέλφους όταν πρόκειται να απουσιάσετε (πχ. λόγω αδείας ή ασθενείας).

- Καταγράφετε τα συνθηματικά σας σε οποιοδήποτε μέσο (χαρτί, ηλεκτρονικό ταχυδρομείο, κινητό τηλέφωνο, PDA, υπολογιστή, λειτουργίες τύπου "remember Password" κλπ.).

- Απαγορεύεται η χρήση συνθηματικών:
  - με λιγότερους από 8 χαρακτήρες,
  - που περιέχουν μέρος ή ολόκληρο το αναγνωριστικό χρήστη (user name),

- που είναι δυνατόν να περιλαμβάνονται σε κάποιο λεξικό,
- είναι κοινές λέξεις, όπως ονόματα κλπ.,
- είναι λέξεις που σχετίζονται με την επωνυμία της Εταιρείας ή των προϊόντων της,
- είναι πληροφορίες που αφορούν το χρήστη, όπως η ημερομηνία γέννησης του κλπ.,
- επαναλαμβάνουν τον ίδιο χαρακτήρα πολλές φορές ή έχουν ακολουθίες αριθμών ή γραμμάτων,
- οποιαδήποτε από τα ανωτέρω συλλαβισμένο ανάποδα ή με ένα χαρακτήρα εμπρός ή πίσω.

- Απαγορεύεται η χρήση των ίδιων συνθηματικών για συστήματα της Εταιρείας και για συστήματα ή υπηρεσίες εκτός Εταιρείας (πχ. οικιακοί υπολογιστές).

Πρέπει να:

- Αναφέρετε στον Υπεύθυνο Ασφάλειας ΠΕΣ οποιαδήποτε θεωρείτε ότι περιορίζει την ασφάλεια των ΠΕΣ.

- Συμβουλεύεστε τον Υπεύθυνο Ασφάλειας ΠΕΣ για κάθε απορία που έχετε σε σχέση με την ασφάλεια των ΠΕΣ, την εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ και τους τρόπους που μπορείτε να συμβάλλετε στη βελτίωση της ασφάλειας των ΠΕΣ.

- Σέβεστε τους μηχανισμούς ελέγχου πρόσβασης (access control), ακόμα και αν αυτοί είναι ανεπαρκείς.

- Αλλάζετε το συνθηματικό σας σε κάθε περίπτωση που θεωρείτε ότι μπορεί να έχει αποκαλυφθεί.

- Επιλέγετε συνθηματικά που σας είναι εύκολο να θυμόσαστε, αλλά δύσκολο για οποιονδήποτε άλλον να μαντέψει. Αν χρειάζεστε βοήθεια συμβουλευτείτε τον Υπεύθυνο Ασφάλειας ΠΕΣ.

2.13.2 Σύνοψη Πολιτικής Ασφάλειας ΠΕΣ για Διοικητικά Στελέχη

Τι πρέπει να προσέχετε:

Η CubeIQ αποδίδει υψηλή προτεραιότητα στην ασφάλεια των Πληροφοριακών και Επικοινωνιακών Συστημάτων (ΠΕΣ) που υποστηρίζουν τις δραστηριότητες της CubeIQ . Είναι υποχρέωση όλων των διοικητικών στελεχών να υποστηρίζουν ενεργά την προσπάθεια διασφάλισης των συστημάτων αυτών. Ιδιαίτερη προσοχή οφείλεται στα παρακάτω:

- Ολες οι δραστηριότητες που αφορούν την ασφάλεια ΠΕΣ βασίζονται σε ρητές πολιτικές και διαδικασίες.

- Η Εταιρεία δεσμεύεται για την τήρηση της νομοθεσίας που αφορά την προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά τη νομοθεσία που αφορά τη χρήση ΠΕΣ.

- Η Διοίκηση της Εταιρείας μεριμνά ώστε όλα τα μέλη του προσωπικού να γνωρίζουν τις υποχρεώσεις τους που απορρέουν από τη Πολιτική Ασφάλειας ΠΕΣ.

- Η Εταιρεία είναι υπεύθυνη απέναντι στο νόμο για την τήρηση των νομικών και κανονιστικών προβλέψεων που αφορούν την προστασία προσωπικών δεδομένων και τη διασφάλιση του απόρρητου των επικοινωνιών, έστω και εάν η παραβίαση προέλθει από εξωτερικούς συνεργάτες ή αναδόχους εργασιών.

Δεν επιτρέπεται να:

- Μεταβιβάζετε στοιχεία των πελατών της Εταιρείας σε τρίτους, παρά μόνο κατόπιν δικαστικής ή εισαγγελικής εντολής ή όταν επιβάλλεται από το νόμο.

- Παρακάμπτετε την Πολιτική Ασφάλειας ΠΕΣ, να εξουσιοδοτείτε ενέργειες που παραβιάζουν την Πολιτική ή να δείχνετε ανοχή σε τέτοιες ενέργειες.

Πρέπει να:

- Αποδεικνύετε τη σημασία που έχει η ασφάλεια των ΠΕΣ, εφαρμόζοντας υποδειγματικά την Πολιτική Ασφάλειας ΠΕΣ και τις διαδικασίες ασφάλειας που απορρέουν από αυτήν.

- Συμβουλεύεστε την Πολιτική Ασφάλειας ΠΕΣ σε κάθε απόφασή σας που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα, την ασφάλεια των ΠΕΣ.

- Παρέχετε τα απαραίτητα μέσα για την αποτελεσματική εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ.

- Παρέχετε πρόσβαση στο προσωπικό σε πηγές πληροφόρησης για ζητήματα ασφάλειας, καθώς και σε σχετικό εκπαιδευτικό υλικό, όπως μαθήματα εξ' αποστάσεως, εκπαιδευτικά video κλπ.

- Μεριμνάτε για την εκπαίδευση και ευαισθητοποίηση σε θέματα ασφάλειας ΠΕΣ του προσωπικού της Εταιρείας που σχετίζεται με τη λειτουργία των ΠΕΣ.

- Επιλέγετε προσωπικό με κατάλληλα τυπικά και ουσιαστικά προσόντα για την πλήρωση θέσεων που είναι σημαντικές για την ασφαλή λειτουργία των ΠΕΣ.

- Συνεργάζεστε με τον Υπεύθυνο Ασφάλειας ΠΕΣ και τους Ελεγκτές ΠΕΣ για ζητήματα που αφορούν την Ασφάλεια ΠΕΣ.

- Ενημερώνεστε για το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων και τη διασφάλιση του απόρρητου των επικοινωνιών.

2.13.3 Σύνοψη Πολιτικής Ασφάλειας ΠΕΣ για τους Διαχειριστές

Τι πρέπει να προσέχετε

Η CubeIQ αποδίδει υψηλή προτεραιότητα στην ασφάλεια των Πληροφοριακών και Επικοινωνιακών Συστημάτων (ΠΕΣ) που υποστηρίζουν τις δραστηριότητες της CubeIQ . Είναι υποχρέωση όλων των στελεχών που υποστηρίζουν τεχνικά τα συστήματα αυτά να καταβάλλουν κάθε προσπάθεια για την προστασία τους. Ιδιαίτερη προσοχή οφείλεται στα παρακάτω:

- Η εφαρμογή της Πολιτικής Ασφάλειας ΠΕΣ είναι υποχρεωτική για όλα τα μέλη του προσωπικού της Εταιρείας, χωρίς εξαιρέσεις.

- Η ασφάλεια των ΠΕΣ της Εταιρείας στηρίζεται τόσο στην πιστή τήρηση των πολιτικών και των διαδικασιών, όσο και στη συνεχή προσοχή και μέριμνα, καθώς και στην κριτική ικανότητα των ανθρώπων που διαχειρίζονται τα ΠΕΣ.

- Η Εταιρεία δεσμεύεται για την τήρηση της νομοθεσίας που αφορά την προστασία των προσωπικών δεδομένων και του απορρήτου των επικοινωνιών. Η συμβολή των διαχειριστών των συστημάτων στην προσπάθεια ανταπόκρισης της Εταιρείας στις υποχρεώσεις της είναι απαραίτητη.
-

Δεν επιτρέπεται να:

- Επιχειρείτε να παραβιάσετε τους μηχανισμούς ασφάλειας για να δείξετε τα αδύναμα σημεία τους. Εάν θεωρείτε ότι οι μηχανισμοί αυτοί είναι ανεπαρκείς οφείλετε να το υποδείξετε στον Υπεύθυνο Ασφάλειας ΠΕΣ. Ο Υπεύθυνος Ασφάλειας ΠΕΣ θα εξετάσει την υπόθεση, χωρίς να απαιτήσει αποδείξεις και θα εξουσιοδοτήσει τα κατάλληλα πρόσωπα για τον έλεγχό των μηχανισμών.

- Παραβιάζετε τη νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας, όπως και να προβαίνετε σε οποιαδήποτε παράνομη ενέργεια χρησιμοποιώντας εξοπλισμό της Εταιρείας. Σε αντίθετη περίπτωση η Εταιρεία επιφυλάσσεται να επιβάλλει και διοικητικές κυρώσεις, πέρα από τις όποιες ποινικές συνέπειες.

- Αποκαλύπτεται σε τρίτους οποιεσδήποτε πληροφορίες αφορούν τους πελάτες της Εταιρείας.

- Κάνετε χρήση κοινών λογαριασμών και συνθηματικών.

- Παραβιάζετε ή παρακάμπτετε τους μηχανισμούς ελέγχου πρόσβασης με τρόπο που να καθιστά αδύνατη την ταυτοποίηση των ατόμων που εκτέλεσαν την κάθε ενέργεια.

Πρέπει να:

- Συμβουλεύεστε την Πολιτική Ασφάλειας ΠΕΣ σε κάθε απόφασή σας που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα, την ασφάλεια των ΠΕΣ.
- Αναφέρετε κάθε ύποπτο περιστατικό στον Υπεύθυνο Ασφάλειας ΠΕΣ.

- Σέβεστε τα δικαιώματα των συναδέλφων σας και να μην παρακολουθείτε ή επεμβαίνετε στις δραστηριότητές τους εάν δεν έχετε σχετική εξουσιοδότηση και μόνο εάν είναι απαραίτητο για την εργασία που έχετε αναλάβει.

- Συνεργάζεστε με τους Ελεγκτές ΠΕΣ της Εταιρείας παρέχοντάς τους τις πληροφορίες που χρειάζονται και όποιες άλλες διευκολύνσεις τους είναι απαραίτητες.

- Ακολουθείτε αυστηρές πρακτικές για την ορθή επιλογή και διαχείριση των συνθηματικών που χρησιμοποιείτε.

- Τηρείτε την αρχή ανάγκης γνώσης (need-to-know) για την πρόσβασή σας σε συστήματα και δεδομένα.

- Εποπτεύετε τους αναδόχους έργων, εξωτερικούς συνεργάτες και παρόχους υπηρεσιών που μπορεί να επηρεάσουν τη λειτουργία των ΠΕΣ της Εταιρείας.

- Συμβάλλετε στη βελτίωση των διαδικασιών ασφάλειας υποβάλλοντας προτάσεις βελτίωσης και να μεριμνάτε για τη διάδοση της γνώσης που αποκτούν κατά την άσκηση των καθηκόντων τους.

- Θέτετε σε δοκιμαστική λειτουργία και να ελέγχετε κάθε νέο σύστημα πριν τεθεί σε παραγωγική λειτουργία, καθώς και κάθε παλαιό σύστημα στο οποίο γίνονται σημαντικές αλλαγές.

- Μεριμνάτε ώστε οι εφαρμογές που αναπτύσσουν, ανεξάρτητα του μεγέθους τους, να ενσωματώνουν επαρκείς και αποτελεσματικούς μηχανισμούς ασφάλειας.

2.13.4 Σύνοψη Πολιτικής Ασφάλειας ΠΕΣ για Εξωτερικούς Συνεργάτες

Οι εξωτερικοί συνεργάτες, οι ανάδοχοι έργων της CubeIQ, καθώς και όσοι παρέχουν υπηρεσίες στην Εταιρεία οφείλουν να σέβονται την Πολιτική Ασφάλειας ΠΕΣ της Εταιρείας και να επιδεικνύουν ιδιαίτερη ευαισθησία στα ζητήματα ασφάλειας και προστασίας προσωπικών δεδομένων. Ιδιαίτερη προσοχή οφείλεται στα παρακάτω:

- Οφείλετε να λαμβάνετε γνώση και να εφαρμόζετε την Πολιτική Ασφάλειας ΠΕΣ της CubeIQ για την εκτέλεση οποιασδήποτε εργασίας αφορά τα ΠΕΣ της Εταιρείας.

- Οφείλετε να αναφέρετε κάθε γεγονός που μπορεί να θέσει σε κίνδυνο τα ΠΕΣ της Εταιρείας και κάθε αδυναμία των συστημάτων η οποία υπέπεσε στην αντίληψή σας.

- Οφείλετε να τηρείτε αυστηρά την εμπιστευτικότητα των δεδομένων στα οποία αποκτάτε πρόσβαση.

- Απαγορεύεται να αποκαλύπτετε σε οποιοδήποτε άτομο (συνεργάτη, συνάδελφο ή τρίτο πρόσωπο) πληροφορίες ή οποιαδήποτε στοιχεία που συνδέονται με (α) το περιεχόμενο ή την ουσία των επικοινωνιών των πελατών της CubeIQ , (β) στοιχεία σχετικά με υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο ή (γ) άλλα προσωπικά δεδομένα των χρηστών των τηλεπικοινωνιακών υπηρεσιών, όπως αριθμούς τηλεφώνου ή διευθύνσεις.

- Τα άτομα που πραγματοποιούν εργασίες στα ΠΕΣ της Εταιρείας πρέπει να δηλώνονται ώστε να διευκολύνεται η καταγραφή τους και ο έλεγχος της ταυτότητάς τους.

- Ολα τα άτομα που αναλαμβάνουν εργασίες που έχουν άμεση ή έμμεση σχέση με τα ΠΕΣ της CubeIQ πρέπει να υπογράφουν δήλωση περί τήρησης εμπιστευτικότητας.

- Τα άτομα που εργάζονται στους χώρους της CubeIQ δεν πρέπει να εκτελούν εργασίες ή να επισκέπτονται ευαίσθητους χώρους, χωρίς την επίβλεψη στελεχών της CubeIQ.

****** EOF ******