ΚΑΠΑ ΤΕΛ Α.Ε.
Πηγάσου 2 & Χαλανδρίου - 15125 - Μαρούσι
Τηλ. : 213.01.61800 Fax: 213.01.61770
e-mail: info@kapatel.gr
www.kapatel.gr

Πολιτική Ασφάλειας και Απορρήτου Επικοινωνιών.

Η παρούσα Πολιτική Ασφάλειας για την Διασφάλιση του Απορρήτου των Επικοινωνιών, αφορά τους χρήστες, συνδρομητές, εργαζόμενους και συνεργάτες της Εταιρίας μας.

Η παρούσα Πολιτική Ασφάλειας για την Διασφάλιση του Απορρήτου των Επικοινωνιών δεν συμπεριλαμβάνεται σε ευρύτερη πολιτική ασφάλειας πληροφοριών και επικοινωνιών.

Η Εταιρία υποχρεούται να διατηρεί αρχείων για το σκοπό του ελέγχου της Πολιτικής Διασφάλισης του Απορρήτου των Επικοινωνιών για χρονικό διάστημα δύο (2) ετών, λαμβάνοντας τα κατάλληλα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς τους .

Κάθε αδυναμία συμμόρφωσης με τις απαιτήσεις που ορίζονται στον παρόντα Κανονισμό της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, συμπεριλαμβανομένων των επιμέρους πολιτικών και των διαδικασιών που την υλοποιούν, η οποία, ενδεικτικά, μπορεί να οφείλεται σε μη εφαρμοσιμότητα ή σε τεχνική αδυναμία κάλυψης συγκεκριμένων απαιτήσεων, καταγράφεται και τεκμηριώνεται επαρκώς. Προβλέπεται και εφαρμόζεται εσωτερική διαδικασία καταγραφής και τεκμηρίωσης των αδυναμιών της παρούσας παραγράφου.

Για την υλοποίηση των επιμέρους πολιτικών, ορίζονται, τεκμηριώνονται, εφαρμόζονται και αναθεωρούνται συγκεκριμένες διαδικασίες ασφάλειας και οργανωτικές δομές. Οι διαδικασίες ασφάλειας ορίζουν συγκεκριμένες ενέργειες των εργαζομένων, συνεργατών, χρηστών και συνδρομητών, του υπόχρεου προσώπου, την αλληλουχία των ενεργειών, τους υπεύθυνους για την εκτέλεσή τους και τον τρόπο και τα μέσα τεκμηρίωσής τους.

Η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών με τις επιμέρους πολιτικές που την απαρτίζουν, ορίζει τις διοικητικές οντότητες ή τα φυσικά πρόσωπα με συγκεκριμένες αρμοδιότητες σχετικά με την εφαρμογή της πολιτικής. Τα υπόχρεα πρόσωπα ορίζουν τους αρμόδιους να καθορίζουν και να πραγματοποιούν τις ενέργειες σχεδίασης, ανάπτυξης, προμήθειας, εγκατάστασης, λειτουργίας, διαχείρισης, υποστήριξης, αναβάθμισης, επικαιροποίησης, διαγραφής, απόσυρσης και πρόσβασης σε κάθε ΠΕΣ.

Η Εταιρία οφείλει να ορίσει συγκεκριμένο εργαζόμενο του, ως Υπεύθυνο Διασφάλισης του Απορρήτου των Επικοινωνιών, επιφορτισμένο με την ευθύνη ελέγχου της υλοποίησης των μέτρων και των απαιτήσεων που ορίζονται στην Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών. Η Εταιρία οφείλει να κοινοποιεί στην Α.Δ.Α.Ε. τα στοιχεία επικοινωνίας του εκάστοτε Υπεύθυνου Διασφάλισης του Απορρήτου των Επικοινωνιών

Η Εταιρία υποχρεούται να εξασφαλίζει ότι οι καταγραφές των αρχείων καταγραφής είναι πλήρεις και συνεχείς. Οφείλει, επίσης, να διατηρεί Ειδικό Σχέδιο Αρχείων Καταγραφής, το οποίο, κατ' ελάχιστον, περιλαμβάνει την αρχιτεκτονική και τις επιμέρους μεθόδους δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, πλήρη περιγραφή του περιεχομένου αυτών, καθώς και τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς αυτών .

Η Εταιρία οφείλει να ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας σε περίπτωση διακοπής των καταγραφών και σε περίπτωση περιστατικού παραβίασης της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας αυτών .

Η Εταιρία τηρεί Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου κάθε 2 έτη που σκοπό έχει την αποτίμηση των κινδύνων ή απειλών που σχετίζονται με ενδεχόμενη παραβίαση του απορρήτου των επικοινωνιών. Για τον λόγο αυτό η εταιρία

α. διατηρεί κατάλογο των ΠΕΣ με συνοπτική περιγραφή της λειτουργίας τους

β. Γίνεται αποτίμηση των απειλών που σχετίζονται με ενδεχόμενη παραβίαση του απορρήτου από εξωτερικές απειλές, εργαζόμενους ή συνεργάτες του υπόχρεου προσώπου, αποτίμηση των σχετικών ευπαθειών των ΠΕΣ και αποτίμηση των πιθανών επιπτώσεων των περιστατικών παραβίασης του απορρήτου. Τα αποτελέσματα της αποτίμησης κινδύνου λαμβάνονται υπόψη για τη σύνταξη και την αναθεώρηση της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και την υλοποίηση των κατάλληλων μέτρων για την εφαρμογή της

Τα αποτελέσματα της αποτίμησης κινδύνου λαμβάνονται υπόψη για τη σύνταξη και την αναθεώρηση της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και την υλοποίηση των κατάλληλων μέτρων για την εφαρμογή της. Τα αποτελέσματα της αποτίμησης κινδύνου διατηρούνται από το υπόχρεο πρόσωπο και είναι διαθέσιμα κατά τον τακτικό ή έκτακτο έλεγχο της εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών από την Α.Δ.Α.Ε.

Η Εταιρία ως Υπεύθυνο Διασφάλισης του Απορρήτου ορίζει τον εργαζόμενο της, Αντώνιο Σπύρου ο οποίος είναι επιφορτισμένος με την ευθύνη ελέγχου της υλοποίησης των μέτρων και των απαιτήσεων που ορίζονται στην παρούσα πολιτική.

1. Πολιτική Αποδεκτής Χρήσης.

1.1. Η Εταιρία υποχρεούται να αναρτεί την Πολιτική Ασφάλειας στην ιστοσελίδα της "www.kapatel.gr" και να ενημερώνει τους εργαζόμενους της, καθώς και να τους εκπαιδεύει στην εφαρμογή αυτής καθώς και σε οποιαδήποτε αναθεώρησή της.

1.2. Οι εργαζόμενοι και συνεργάτες της Εταιρίας οφείλουν να συμμορφώνονται με την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, συμπεριλαμβανομένων των σχετικών διαδικασιών, μέτρων ασφάλειας και οδηγιών. Για το σκοπό αυτό, Η εταιρία ενημερώνει γραπτώς τους εργαζόμενους και συνεργάτες με την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών καθώς τις διαδικασίες, μέτρων ασφαλείας πριν την απόκτηση πρόσβασης στα ΠΕΣ. Οι εργαζόμενοι και συνεργάτες της Εταιρίας υπογράφουν το σχετικό έγγραφο ενημέρωσής τους και κρατείται σε ειδικό κλασέρ, προ της απόκτησης πρόσβασης σε ΠΕΣ και σε δεδομένα επικοινωνίας.

1.3. Η Εταιρία διατηρεί ενημερωμένο αρχείο στο οποίο καταγράφονται οι συνεργάτες του, φυσικά ή νομικά πρόσωπα, οι οποίοι προκειμένου να παράσχουν τις υπηρεσίες τους, αποκτούν ή δύνανται να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών

1.4. Η Εταιρία συνάπτει με τους συνεργάτες της συμβάσεις με τις οποίες οι συνεργάτες αποδέχονται την υποχρέωση τήρησης των μέτρων ασφαλείας για τη διασφάλιση του απορρήτου των επικοινωνιών οι οποίες κατ' ελάχιστο περιλαμβάνει.

- Όρους εμπιστευτικότητας, μη αποκάλυψης και τήρησης του απορρήτου.
- Απαιτήσεις και μέτρα ασφάλειας που λαμβάνονται για τη διασφάλιση του απορρήτου των επικοινωνιών, με τα οποία διασφαλίζεται η εμπιστευτικότητα και ακεραιότητα των δεδομένων επικοινωνίας κατά την επεξεργασία αυτών από τους συνεργάτες του υπόχρεου προσώπου, καθώς και η οριστική διαγραφή και καταστροφή αυτών μετά τη λήξη της συνεργασίας.
- Αποδοχή εκ μέρους των συνεργατών της υποχρέωσης για τήρηση των μέτρων ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών.
- Το υπόχρεο πρόσωπο οφείλει να ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, για κάθε παραβίαση των συμβατικών όρων.

1.5. Οι συνεργάτες της εταιρίας θα ενημερώνονται μέσω της ιστοσελίδα "www.kapatel.gr", με ηλεκτρονικό ταχυδρομείο ή τηλεφωνικά για οποιαδήποτε αναθεώρησή της καθώς και μέσω των μεταξύ τους συμβάσεων.

1.6. Οι εργαζόμενοι και συνεργάτες της Εταιρίας απαγορεύεται να αποκαλύπτουν οποιαδήποτε πληροφορία ή στοιχείο υποπέσει στην αντίληψή τους ή κατοχή τους ως αποτέλεσμα της φύσης της εργασίας τους.

1.7. Οι εργαζόμενοι και συνεργάτες της Εταιρίας υποχρεούνται να ενημερώνουν άμεσα τον αρμόδιο σε περίπτωση που υποπέσει στην αντίληψή τους κάποιο κενό ασφαλείας ή σχετικό περιστατικό το οποίο απειλεί την διασφάλισή του απορρήτου των επικοινωνιών.

1.8. Οι συνεργάτες συμφωνούν με την σύναψη σύμβασης την μη επεξεργασία των δεδομένων επικοινωνίας αλλά και στην περίπτωση που αυτό χρειαστεί, τα στοιχεία θα πρέπει να καταστρέφονται αμέσως μετά την λήξη της εργασίας τους με τα δεδομένα επικοινωνίας.

1.9. Η Εταιρία υποχρεούται να ενεργοποιήσει την Πολιτική Διαχείρισης Περιστατικών Ασφαλείας, για κάθε παράβαση των παραγράφων 1.3, 1.4, 1.5.

1.10. Οι συνδρομητές των παρεχομένων υπηρεσιών θα μπορούν να ενημερώνονται μέσω της ιστοσελίδας της εταιρίας "www.kapatel.gr", για τον τρόπο προστασίας του απόρρητου των επικοινωνιών τους καθώς και για τους κανόνες ορθής χρήσης των παρεχομένων υπηρεσιών.

1.11. Η Εταιρία δεν αποθηκεύει ευαίσθητα δεδομένα σε αποθηκευτικά μέσα (όπως κωδικοί πρόσβασης σε ΠΕΣ ή δεδομένα διάρθρωσης. Εάν αυτό καταστεί αναγκαίο να λάβει χώρα, τότε ο μοναδικός ο οποίος μπορεί να αποθηκεύσει, διακινήσει τα εν λόγο στοιχεία, είναι ο Υπεύθυνος Διασφάλισης του Απορρήτου ο οποίος οφείλει να τα καταστρέψει μετά το πέρας των εργασιών.

2. Πολιτική Φυσικής Ασφάλειας.

2.1. Η φυσική ασφάλεια των συστημάτων και δικτυακών υποδομών της εταιρίας μας, διασφαλίζεται με εξουσιοδοτημένη πρόσβαση στους χώρους όπου αυτά λειτουργούν. Οι αντίστοιχοι αυτοί χώροι προστατεύονται επιπλέον με κωδικούς πρόσβασης.

2.2. Η συγκεκριμένη πολιτική αφορά το προσωπικό του τμήματος τεχνικής υποστήριξης, το προσωπικό του τμήματος Network & Operations, το προσωπικό του τμήματος Development και την διοίκηση της εταιρίας.

2.3. Ο χώρος πού εγκαθίστανται τα ΠΕΣ, εντός των εγκαταστάσεων της Εταιρίας, ελέγχεται από ισχυρό μηχανισμό ασφαλείας με την μέθοδο των καρτών ελεγχόμενης εισόδου. Η φυσική πρόσβαση στους χώρους της παρούσας παραγράφου καταγράφεται σε ειδικό αρχείο, σύμφωνα με την παράγραφο 2.8.

2.4. Η φυσική πρόσβαση στους χώρους των *ΠΕΣ* γίνεται με την παρακάτω διαδικασία.
α. Μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν φυσική πρόσβαση στον χώρο των ΠΕΣ.
β. Στην περίπτωση όπου πρέπει να αποκτήσουν πρόσβαση συνεργάτες ή επισκέπτες, τότε θα πρέπει πρώτα να εξουσιοδοτηθούν και αφού εξουσιοδοτηθούν να συνοδεύονται πάντα από έναν εξουσιοδοτημένο εργαζόμενο.
Οι διαδικασία εξουσιοδότησης αναφέρεται στις παραγράφους 2.4 & 2.5 & 2.6

2.5. Για να υπάρχει έλεγχος της εξουσιοδότησης των ατόμων συμπληρώνεται από τον προϊστάμενο του αντίστοιχου τεχνικού τμήματος υπεύθυνου για το άτομο που απαιτείται να χορηγηθεί φυσική πρόσβαση, η αντίστοιχη αίτηση εξουσιοδότησης φυσικής πρόσβασης στα πληροφοριακά συστήματα, και λαμβάνει ενυπόγραφη έγκριση από τον *υπεύθυνο ασφαλείας πληροφοριακών συστημάτων και δικτύων (ΥΑΠΣΔ)* και τον *Διευθυντή πληροφορικής*.

2.6. Η φόρμα αυτή συμπληρώνεται υποχρεωτικά για όλα τα άτομα που πρέπει να αποκτήσουν φυσική πρόσβαση σε κάποιον από τους χώρους πληροφοριακών συστημάτων και δικτύων της εταιρίας από το προσωπικό του τμήματος Network & Operations.

2.7. Αιτήσεις που εγκριθούν πρέπει να κοινοποιηθούν στους εμπλεκόμενους από το προσωπικό του τμήματος Network & Operations καθώς και στους υπεύθυνους φύλαξης και να αρχειοθετηθούν.

2.8. Η πρόσβαση στους χώρους των *ΠΕΣ από εξουσιοδοτημένα άτομα,* καταγράφεται σε ειδικό αρχείο πρόσβασης (ονοματεπώνυμο, ιδιότητα, ώρα εισόδου και εξόδου). Στην περίπτωση πρόσβασης συνεργάτη του υπόχρεου προσώπου ή άλλου επισκέπτη, στο αρχείο της παρούσας παραγράφου καταγράφεται επιπλέον ο λόγος της πρόσβασης, καθώς και τα στοιχεία (ονοματεπώνυμο και ιδιότητα) του εργαζομένου που πρόκειται να συναντήσει.

2.9. Η εταιρεία δεν διαθέτει ΠΕΣ τα οποία είναι υπό την εποπτεία του εκτός των εγκαταστάσεών του.

3. Πολιτική Λογικής Πρόσβασης.

3.1. Η πολιτική αυτή αφορά όλο το προσωπικό της εταιρίας και τους εξωτερικούς

συνεργάτες που για την εργασία τους χειρίζονται κάποιο *ΠΕΣ* της εταιρίας καθώς και τα τμήματα πωλήσεων και marketing.

3.2. Ο έλεγχος πρόσβασης στα *ΠΕΣ* γίνεται με χρήση ενός λογαριασμού πρόσβασης που αποτελείται από ένα ζεύγος ονόματος χρήστη και κωδικό πρόσβασης. Οι μηχανισμοί ελέγχου πρόσβασης και αυθεντικοποίησης του κάθε ΠΕΣ καταγράφονται σε σχετικό αρχείο.

3.3. Κάθε εργαζόμενος και συνεργάτης εκχωρείται με έναν κωδικό πρόσβασης ανά *ΠΕΣ* και η αντιστοίχηση των λογαριασμών πρόσβασης των εργαζομένων και συνεργατών καταγράφεται σε σχετικό αρχείο, έτσι ώστε να διαπιστώνεται με βεβαιότητα ποίος είναι ο κάτοχος κάθε λογαριασμού.

3.4. Ο Κάθε κωδικός πρόσβασης είναι κατηγοριοποιημένος ανάλογα με το είδος της εργασίας που πρόκειται να κάνει και αυτές οι κατηγορίες αναγράφονται σε σχετικό αρχείο.

3.5. Δεν δημιουργούνται κοινοί ή προκαθορισμένοι κωδικοί.

3.6. Διατηρείται αρχείο στο οποίο καταγράφονται οι κατηγορίες των χρηστών και τα δικαιώματα πρόσβασης αυτών για κάθε ΠΕΣ.

3.7. Η Εταιρία καταγράφει σε αρχείο τους τρόπους πρόσβασης των εργαζομένων και συνεργατών του σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών. Κάθε πρόσβαση σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών καταγράφεται και να αιτιολογείται

3.8. Η πρόσβαση στα ΠΕΣ καταγράφεται σε σχετικό αρχείο και περιλαμβάνει το όνομα του χρήστη που απέκτησε την πρόσβαση, την ημερομηνία, ώρα εκκίνησης και ώρα λήξης.

3.9. Η προσθήκη νέων χρηστών ΠΕΣ, η αφαίρεση, η τροποποίηση και μεταβολή δικαιωμάτων ή επιπέδων πρόσβασης αναλύεται στην “Διαδικασία Διαχείρισης Χρηστών ΠΕΣ”.

3.10. Για κάθε μία εκ των ενεργειών που αναφέρονται στην παράγραφο 3.8 του παρόντος προβλέπεται υποχρεωτικά η προηγούμενη έγκριση από αρμόδιο εργαζόμενο της Εταιρίας.

3.11. Στη Διαδικασία Διαχείρισης Χρηστών ΠΕΣ προβλέπεται η υποχρέωση τήρησης αρχείου των αιτήσεων που αφορούν σε κάθε μεταβολή στην κατάσταση πρόσβασης των χρηστών ΠΕΣ. Επίσης προβλέπεται η υποχρέωση τήρησης αρχείου με το ιστορικό

όλων των δικαιωμάτων ή επιπέδων πρόσβασης των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα ΠΕΣ της Εταιρίας, όπως λογαριασμός πρόσβασης, δικαιώματα/επίπεδο πρόσβασης αυτού, χρονικό διάστημα ισχύος.

3.12. Η εταιρία οφείλει να ακολουθεί την Διαδικασία Ελέγχου Ορθής Εφαρμογής της Πολιτικής Λογικής Πρόσβασης , όπου πραγματοποιούνται περιοδικοί έλεγχοι, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών , στα εξής:

α. Ελέγχονται τα διακαιώματα πρόσβασης των χρηστών ΠΕΣ για να εξακριβωθεί εάν το δικαίωμα πρόσβασης που του δόθηκε είναι το σωστό.

β. Ελέγχονται οι λογαριασμοί πρόσβασης αντιπαραβάλλοντας το αρχείο που περιλαμβάνει τις εγκεκριμένες αιτήσεις (παρ.3.10) με τους λογαριασμούς που προκύπτουν από έκαστο ΠΕΣ.

γ. Ελέγχονται δειγματοληπτικά τα αρχείων καταγραφής πρόσβασης (access logs) για την ανακάλυψη ενδεχομένων μη αιτιολογημένων προσβάσεων.

3.13. Για την δημιουργία και διαχείριση Λογαριασμών Πρόσβασης, η Εταιρία διατηρεί τα ακόλουθα:

α. Αρχείο με περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία ενός ονόματος χρήστη,

β. Αρχείο με περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία ενός κωδικού πρόσβασης,

γ. Διαδικασία σύμφωνα με την οποία αποδίδεται με ασφάλεια σε κάθε εργαζόμενο και συνεργάτη το όνομα χρήστη και ο κωδικός πρόσβασης που τον αφορά,

δ. Διαδικασία σύμφωνα με την οποία επιτυγχάνεται η τακτική αλλαγή των κωδικών πρόσβασης και εν γένει η διαχείρισή τους

ε. Αρχείο με περιγραφή των όρων χρήσης των κωδικών πρόσβασης από τους εργαζόμενους και συνεργάτες του υπόχρεου προσώπου

στ. Διαδικασία σύμφωνα με την οποία διενεργείται έλεγχος για την ορθή εφαρμογή των παραπάνω κανόνων και διαδικασιών, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών .

3.14. Για την υλοποίηση των υποχρεώσεων της παραγράφου 3.12, η Εταιρία λαμβάνει υπόψη τις παρακάτω απαιτήσεις:

α. Τα ονόματα χρήστη δεν πρέπει να υποδηλώνουν τον ρόλο στο ΠΕΣ των εργαζομένων και συνεργατών του υπόχρεου προσώπου (ενδεικτικά, δεν πρέπει να είναι παράγωγα της λέξης admin).

β. Οι χρησιμοποιούμενοι κωδικοί πρόσβασης θα είναι ισχυροί και δημιουργούνται με συνδυασμό δύο (2) τουλάχιστον διαφορετικών ειδών χαρακτήρων (αριθμοί, γράμματα, ειδικοί χαρακτήρες). Οι κωδικοί πρόσβασης θα έχουν ένα επαρκές ελάχιστο μήκος 8

χαρακτήρων, θα απαγορεύεται η χρήση πρόσφατων κωδικών στη διαδικασία αλλαγής τους και δεν θα ακολουθούνται συγκεκριμένα υποδείγματα κατά τη δημιουργία τους.

γ. Οι κωδικοί πρόσβασης θα αλλάζουν περιοδικά, σε συχνότητα που καθορίζεται ρητά ανά ΠΕΣ και αναφέρεται σε αρχείο που διατηρεί η Εταιρία. Η Εταιρία χρησιμοποιεί και καταγράφει στο εν λόγω αρχείο τους τρόπους με τους οποίους επιβάλλει την περιοδική αλλαγή των κωδικών πρόσβασης. Σε χαρακτηριστικές περιπτώσεις όπως είναι, ενδεικτικά, η αφαίρεση χρήστη ΠΕΣ ή η παραβίαση ενός λογαριασμού πρόσβασης, προβλέπεται η άμεση αλλαγή του αντίστοιχου κωδικού πρόσβασης.

δ. Στην περίπτωση επαναλαμβανόμενης εισαγωγής λανθασμένων κωδικών πρόσβασης (μετά από πέντε συνεχόμενες αποτυχημένες απόπειρες εισαγωγής του) ο λογαριασμός πρόσβασης θα μπορεί να χρησιμοποιηθεί μόνο μετά την πάροδο ενός 15 λέπτου.

3.15. Ειδικές Απαιτήσεις σχετικά με τους Συνδρομητές ή Χρήστες των Παρεχομένων Δικτύων ή Υπηρεσιών :

α. Η Εταιρία διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών του στις υπηρεσίες που παρέχει.

β. Η Εταιρία διαμορφώνει και ακολουθεί συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών πρόσβασης των συνδρομητών ή χρηστών στις υπηρεσίες ή/και τα δίκτυα που παρέχει, στην οποία περιγράφεται με σαφήνεια ο τρόπος προσθήκης και κατάργησης λογαριασμών πρόσβασης, καθώς και η απόδοση του ονόματος χρήστη και του κωδικού πρόσβασης στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών της. Κατά τη δημιουργία ή επανέκδοση του κωδικού πρόσβασης, η Εταιρία τον δημιουργεί με τρόπο που να αποτρέπει τον εύκολο προσδιορισμό του. Ενημερώνει με κάθε πρόσφορο μέσο τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών σχετικά με την αναγκαιότητα αλλαγής του κωδικού πρόσβασης, καθώς και σχετικά με ενδεδειγμένους κανόνες δημιουργίας ισχυρών κωδικών πρόσβασης.

γ. Η Εταιρία διαθέτει διαδικασία σύμφωνα με την οποία διενεργείται περιοδικός έλεγχος σχετικά με την αλλαγή του κωδικού πρόσβασης που αυτό αποδίδει στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών και εξασφαλίζει την εκ νέου ενημέρωσή τους σχετικά με την αναγκαιότητα αλλαγής των κωδικών πρόσβασης σε περίπτωση που δεν έχουν προβεί στην σχετική αλλαγή.

δ. Η Εταιρία δεν προσφέρει τη δυνατότητα στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας τους (όπως εξερχόμενες κλήσεις, ηλεκτρονικό ταχυδρομείο) μέσω συγκεκριμένης ιστοθέσης

ε. Η Εταιρία ενημερώνει τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών, τουλάχιστον κατά την σύναψη της μεταξύ τους σύμβασης, με έντυπη ή ηλεκτρονική ενημέρωση, αλλά και σε εύκολα προσβάσιμο σημείο του ιστοτόπου του, σχετικά με τους κανόνες ενδεδειγμένης χρήσης για την προστασία των κωδικών πρόσβασης που κατέχουν.

4. Πολιτική Απομακρυσμένης Λογικής Πρόσβασης.

4.1. Η Πολιτική αφορά τους εργαζόμενους και συνεργάτες της Εταιρίας οι οποίοι, στο πλαίσιο της εργασίας τους, αποκτούν απομακρυσμένη πρόσβαση στα *ΠΕΣ*.

4.2. Απομακρυσμένη πρόσβαση στα *ΠΕΣ* αποκτούν μόνο άτομα εξουσιοδοτημένα και μόνον εφόσον κριθεί αναγκαίο για τις επιχειρησιακές ανάγκες της εταιρίας. Η Εταιρία διατηρεί αρχείο με τις αιτήσεις για απομακρυσμένη πρόσβαση στο οποίο αναγράφεται ο λόγος της πρόσβασης, το *ΠΕΣ* που θα αποκτηθεί η πρόσβαση καθώς και το χρονικό διάστημα που απαιτείται.

4.3. Η Εταιρία εξασφαλίζει ότι κάθε σύνδεση εργαζομένων και συνεργατών του στα ΠΕΣ αυτού επιτρέπεται μόνο εφόσον η σύνδεση αυτή δεν παραβιάζει κάποιον από τους κανόνες ασφάλειας του δικτύου του

4.4. Η απομακρυσμένη πρόσβαση του εξουσιοδοτημένου ατόμου πραγματοποιείται με χρήση μηχανισμών ασφαλούς αυθεντικοποίησης (Cisco VPN) και η πρόσβαση αυτή επιτρέπεται μόνο για συγκεκριμένο χρονικό διάστημα, μετά το πέρας αυτού, οι κωδικοί πρόσβασης απενεργοποιούνται.

4.5. Η Εταιρία επιτρέπει την απομακρυσμένη πρόσβαση των συνεργατών της στα συστήματά της μόνο κατόπιν έγκρισης των σχετικών αιτημάτων, στα οποία αναγράφεται ο λόγος της πρόσβασης, το σύστημα στο οποίο θα πραγματοποιηθεί η πρόσβαση καθώς και το χρονικό διάστημα που απαιτείται. Η Εταιρία για τον λόγο αυτό τηρεί αρχείο με όλες τις πληροφορίες της παρούσας παραγράφου.

4.6. Τα εξουσιοδοτημένα άτομα με δυνατότητα απομακρυσμένης πρόσβασης καταγράφονται σε αρχείο (ονοματεπώνυμο και ιδιότητα), καθώς και τα δικαιώματα πρόσβασης που τους αντιστοιχούν για κάθε *ΠΕΣ.*

4.7. Η εταιρία ακολουθεί την “Διαδικασία Διαχείρισης Απομακρυσμένης Πρόσβασης” για την διαχείριση των λογαριασμών απομακρυσμένης πρόσβασης των εργαζομένων και συνεργατών του.

4.8. Η εταιρία διενεργεί ελέγχους κατ' ελάχιστον κάθε τρεις μήνες (3) για

4.8.1 Αντιστοίχηση των λογαριασμών απομακρυσμένης πρόσβασης σύμφωνα με το αρχείο της παραγράφου 4.4.

4.8.2 Τις μεταβολές ή απενεργοποιήσεις των κωδικών σύμφωνα με το αρχείο

της παραγράφου 4.3.

5. Πολιτική Διαχειρησης και Εγκατάστασης ΠΕΣ.

5.1. Η εταιρία κατά την διαχείριση και εγκατάσταση ΠΕΣ λαμβάνει όλα τα απαραίτητα μέτρα για την ελαχιστοποίηση του κινδύνου διαρροής πληροφοριών που σχετίζονται με το απόρρητο των επικοινωνιών.

5.2. Οι αλλαγές (εισαγωγή/μεταβολή/διαγραφή) στο λογισμικό/υλικό των ΠΕΣ που σχετίζονται με τη διασφάλιση του απορρήτου των επικοινωνιών θα πραγματοποιούνται χωρίς υπαίτια καθυστέρηση.

5.3. Για οποιαδήποτε αλλαγή υλικού ή λογισμικού η εταιρία διατηρεί αρχείο στο οποίο καταγράφεται η ημερομηνία, ο τρόπος, η αιτιολόγηση και ο εργαζόμενος ή συνεργάτης πού πραγματοποίησε την αλλαγή. Το αρχείο ενημερώνεται και διατηρείται από συγκεκριμένο εργαζόμενο της Εταιρίας.

5.4. Για την Προμήθειας−Ανάπτυξης Υλικού και Λογισμικού των ΠΕΣ ακολουθείται διαδικασία στην οποία η Εταιρία πραγματοποιεί αποτίμηση κινδύνου για τον εντοπισμό των πιθανών απειλών, αδυναμιών και κινδύνων αναφορικά με το απόρρητο των επικοινωνιών του υπό προμήθεια/ανάπτυξη ΠΕΣ .

5.5. Στο πλαίσιο της Διαδικασίας Προμήθειας−Ανάπτυξης υλικού και λογισμικού των ΠΕΣ, συντάσσεται κατάλογος απαιτήσεων που αφορούν ρυθμίσεις ή χαρακτηριστικά του υπό προμήθεια/ανάπτυξη ΠΕΣ, σχετικά με τη διασφάλιση του απορρήτου των επικοινωνιών. Στις απαιτήσεις διασφάλισης του απορρήτου περιλαμβάνονται επίσης και οι ελάχιστες απαιτήσεις που αφορούν στα χαρακτηριστικά διαμόρφωσης και διαχείρισης του υπό προμήθεια/ανάπτυξη ΠΕΣ και οι απαιτήσεις διαμόρφωσης της καταγραφής της πρόσβασης και των ενεργειών, ώστε να συμμορφώνεται με τις προδιαγραφές ασφάλειας που καθορίζονται από τα αποτελέσματα της αποτίμησης κινδύνου και από τις βέλτιστες πρακτικές ασφάλειας. Τα αρχεία της παρούσας παραγράφου εγκρίνονται από το αρμόδιο προσωπικό του υπόχρεου προσώπου και φυλάσσονται.

5.6. Η Εταιρία ακολουθεί Διαδικασία Δοκιμών, Αποδοχής και Ελέγχου Ορθής Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ στην οποία πραγματοποιούνται δοκιμές της υλοποίησης ή διαμόρφωσης των απαιτήσεων που έχουν καθοριστεί κατά το στάδιο της περιγραφής απαιτήσεων Διασφάλισης του Απορρήτου των Επικοινωνιών και ελέγχεται η συμμόρφωση με αυτές τις απαιτήσεις. Τα αποτελέσματα των δοκιμών καταγράφονται και τηρούνται σε σχετικό αρχείο.
Με την επιτυχή ολοκλήρωση της δοκιμαστικής λειτουργίας, συντάσσεται και υπογράφεται από τα εμπλεκόμενα μέρη έκθεση αποδοχής του ΠΕΣ, η οποία τηρείται από το υπόχρεο πρόσωπο σε σχετικό αρχείο.
Κατά το αρχικό στάδιο της λειτουργίας πραγματοποιείται παρακολούθηση της ορθής λειτουργίας του ΠΕΣ, ώστε να εντοπιστούν έγκαιρα τυχόν σφάλματα ή κενά ασφάλειας. Τα αποτελέσματα των ελέγχων καταγράφονται και τηρούνται σε σχετικό αρχείο

5.7. Η Εταιρία για την Προμήθεια-Ανάπτυξη υλικού-λογισμικού, Εγκατάσταση-Λειτουργία υλικού-λογισμικού, Συντήρηση-Υποστήριξη-Λειτουργία υλικού-λογισμικού και Διαγραφή-Απόσυρση Υλικού και Λογισμικού ΠΕΣ, ακολουθεί τις ανάλογες διαδικασίες.

5.8. Η Εταιρία ακολουθεί Διαδικασία Ελέγχου Συντήρησης−Υποστήριξης− Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ , όπου περιλαμβάνεται η παρακολούθηση της ορθής λειτουργίας των ΠΕΣ, μέσω του ελέγχου των συμβάντων και των συναγερμών κάθε συστήματος, ώστε να εντοπίζονται αμελλητί τυχόν σφάλματα ή κενά ασφάλειας. Η Εταιρία καταγράφει και να διατηρεί σε αρχείο τις ενέργειες στο λειτουργικό σύστημα και στις εφαρμογές των ΠΕΣ, καθώς και τα συμβάντα συστήματος των ΠΕΣ.

5.9. Η Εταιρία ακολουθεί Διαδικασία Διαγραφής−Απόσυρσης Υλικού και Λογισμικού των ΠΕΣ όπου η Εταιρία εξασφαλίζει πώς όταν διαγράφεται και αποσύρεται υλικό ή λογισμικό των ΠΕΣ, η πληροφορία που έχει εγγραφεί στον εξοπλισμό των ΠΕΣ (π.χ. σε μνήμες ROM, σκληρούς δίσκους, μαγνητικές ταινίες κλπ.) διαγράφεται οριστικά και δεν μπορεί να χρησιμοποιηθεί από τρίτους. Η Εταιρία διατηρεί αρχείοκαταγραφής στο οποίο καταγράφονται τα ΠΕΣ, τα οποία αποσύρονται. Η Εταιρία διατηρεί, επίσης αρχείο καταγραφής των ενεργειών διαγραφής των δεδομένων του ΠΕΣ, στο καταγράφεται το όνομα χρήστη του εργαζομένου ή του συνεργάτη που διενεργεί τη διαγραφή

6. Πολιτική Διαχείρισης Περιστατικών Ασφαλείας.

6.1. Η Εταιρία ενεργοποιεί την διαδικασία διαχείρισης Περιστατικών ασφαλείας αμελλητί σε κάθε περίπτωση περιστατικού ασφαλείας.

6.2. Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας καταγράφονται τα παρακάτω στοιχεία που αφορούν το περιστατικό ασφαλείας, καθώς επίσης κρατείται αρχείο με όλες τις εγγραφές που σχετίζονται με τα περιστατικά ασφάλειας, από τα οποία θα τεκμηριώνεται και η εκτέλεση των αντίστοιχων προβλεπόμενων ενεργειών.
α. Ημερομηνία, ώρα εκδήλωσης και περιγραφή του περιστατικού,
β. Ημερομηνία και ώρα που έγινε αντιληπτό το περιστατικό ,
γ. Σημείο στο οποίο εκδηλώθηκε το περιστατικό (σύστημα, υπηρεσία, εφαρμογή, πρωτόκολλα, τύπος δεδομένων),
δ. Εκτιμούμενη αιτία εκδήλωσης του περιστατικού,
ε. Συνέπειες του περιστατικού (πλήθος χρηστών που επηρεάστηκαν, τύπος και όγκος των δεδομένων που επηρεάστηκαν),
στ. Συλλεχθέντα στοιχεία από το υπόχρεο πρόσωπο για τη διερεύνηση του περιστατικού (αρχεία καταγραφής, στοιχεία παραβίασης, κ.α.),
ζ. Ενημέρωση για την ενδεχόμενη εμφάνιση του περιστατικού περισσότερες φορές,
η. Χρόνος επίλυσης του προβλήματος,
θ. Διορθωτικά μέτρα και σχετικό χρονοδιάγραμμα,
ι. Ενημέρωση θιγόμενων συνδρομητών ή άλλων ατόμων που επηρεάστηκαν από το περιστατικό και γνωστοποίηση στις αρμόδιες αρχές σύμφωνα με την κείμενη νομοθεσία,
ια. Ενδεχόμενες συστάσεις σε θιγόμενους συνδρομητές ή άλλα άτομα που επηρεάστηκαν από το περιστατικό, με σκοπό τον μετριασμό των αρνητικών επιπτώσεων του

6.3. Σε περίπτωση περιστατικού ασφαλείας Η εταιρία υποχρεούται να ενημερώνει αμελλητί τη Α.Δ.Α.Ε υποβάλλοντας άμεση αναφορά περιστατικού το οποίο θα καταγράφει τα στοιχεία που ορίζονται στην Διαδικασία Διαχείρισης Περιστατικών Ασφαλείας, σύμφωνα με τα δεδομένα που είναι διαθέσιμα την δεδομένη στιγμή και μετά την ολοκλήρωση της διερεύνησης του περιστατικού, θα υποβάλει στην Α.Δ.Α.Ε την Τελική έκθεση Αναφοράς Περιστατικού Ασφαλείας στην οποία θα καταγράφονται με λεπτομέρεια όλες οι πληροφορίες που ορίζονται στην Διαδικασία Διαχείρισης Περιστατικών Ασφαλείας καθώς και όποια πρόσθετη πληροφορία έχει στην κατοχή της η Εταιρία.

6.4. Η Εταιρία παρέχει στους συνδρομητές των υπηρεσιών της, την δυνατότητα να καταγγέλλουν την ενδεχόμενη παραβίαση του απορρήτου των επικοινωνιών τους μέσω e-mail και μέσω τηλεφώνου.

6.5. Η Εταιρία ελέγχει σε τακτά χρονικά διαστήματα την ετοιμότητα ενεργοποίησης της Διαδικασίας Διαχείρισης Περιστατικών Ασφαλείας.

6.6. Αρμόδια στελέχη τα οποία θα ενημερώνονται άμεσα για κάθε περιστατικό ασφαλείας είναι τα εξής:

α. Λαζάρου Ιωάννης
β. Αντώνιος Σπύρου

7. Πολιτική Ασφάλειας Δικτύου

7.1. Η Εταιρία καταγράφει σε αρχείο τα συστήματα και μηχανισμούς που χρησιμοποιεί σε υλικό και λογισμικό για τους σκοπούς της πολιτικής Ασφάλειας Δικτύου. Η λειτουργία των μηχανισμών είναι συνεχής, με την εξαίρεση των περιπτώσεων προγραμματισμένης συντήρησης ή αναβάθμισης .

7.2. Η Εγκατάσταση, η επικαιροποίηση και η διαχείριση τών μηχανισμών και συστημάτων είναι σύμφωνη με την τις αρχές της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ.

7.3. Σε περίπτωσή που ένας μηχανισμός ή σύστημα εντοπίσει κάποιο μή σύνηθες συμβάν, ενεργοποιείται ειδοποίηση (alert) και αναλόγως της σοβαρότητας του, ενεργοποιείται ή όχι η Πολιτική Διαχείρισης Περιστατικών Ασφαλείας.

7.4. Η Εταιρία διατηρεί σχηματικό διάγραμμα δικτύου, το οποίο περιέχει την αρχιτεκτονική του δικτύου, την κατάτμηση αυτών, τα συστήματα καθώς και η ζώνη ασφαλείας που έχουν τοποθετηθεί καθώς διατηρεί και τις προηγούμενες εκδόσεις του εν λόγω αρχείου .

7.5. Τα συστήματα τα οποία περιέχουν τις βάσεις δεδομένων καθώς και το λογισμικό το οποίο τις χρησιμοποιεί, έχουν τοποθετηθεί σε εσωτερικές έμπιστες ζώνες.

7.6. Τα συστήματα τα οποία παρέχουν στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών , τοποθετούνται σε εσωτερικές έμπιστες ζώνες.

7.7. Τα συστήματα τα οποία δεν είναι τοποθετημένα σε εσωτερικά έμπιστα δίκτυα ή σε

αποστρατικοποιημένη ζώνη χρησιμοποιούν κατάλληλους μηχανισμούς ασφαλείας και η εταιρία διατηρεί αρχείο με πλήρη ανάλυση των μέτρων προστασίας και ασφαλείας που έχουν υλοποιηθεί.

8. Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφαλείας για την Διασφάλιση του Απορρήτου των Επικοινωνιών.

8.1. Η Εταιρία πραγματοποιεί έλεγχο εφαρμογής της Πολιτικής Ασφάλειας για την Διασφάλιση του Απορρήτου των Επικοινωνιών κάθε 2 χρόνια και καλύπτει όλο το εύρος εφαρμογής της Πολιτικής.

8.2. Ο έλεγχος περιλαμβάνει τη χρήση και την εξέταση των αρχείων καταγραφής κάθε ΠΕΣ και γίνεται μόνο από τους ειδικά εξουσιοδοτημένους εργαζόμενους της Εταιρίας, οι αρμοδιότητες τους περιγράφονται αναλυτικά σε ειδικό αρχείο και δεν ανήκουν στο τμήμα των ελεγχομένων συστημάτων ή στην ανάπτυξη κώδικα, εγκατάσταση ή λειτουργία του υπό έλεγχο συστήματος.

8.3. Στην περίπτωση διεξαγωγής ελέγχου εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών από εξωτερικό φορέα, λαμβάνεται μέριμνα αναφορικά με ζητήματα τήρησης της εμπιστευτικότητας και μη διαρροής πληροφοριών και δεδομένων, μέσω σχετικής σύμβασης. Καθ' όλη τη διάρκεια διεξαγωγής του ελέγχου από τον εξωτερικό φορέα, παρίσταται ειδικά εξουσιοδοτημένος προς τούτο εργαζόμενος της Εταιρίας.

8.4. Για την προετοιμασία ελέγχου καταγράφονται σε σχετικό αρχείο τα παρακάτω:
α. Καθορισμός του συστήματος και των διαδικασιών/μηχανισμών διασφάλισης του απορρήτου που θα ελεγχθούν και των ελέγχων για την εύρεση τεχνικών ευπαθειών .
β. Το χρονοδιάγραμμα διεξαγωγής του ελέγχου
γ. Τη συλλογή των απαιτούμενων πληροφοριών και δεδομένων και
δ. Τον ορισμό των προσώπων που απαρτίζουν την Ομάδα Ελέγχου.

8.5. Οι αρμοδιότητες των εργαζομένων της Εταιρίας, οι οποίοι διενεργούν τους ελέγχους, καθορίζονται και περιγράφονται αναλυτικά σε σχετικό αρχείο.

8.6. Τα ευρήματα κατά την διεξαγωγή του ελέγχου καθώς και όποιες προτεινόμενες βελτιώσεις ή τροποποιήσεις καταγράφονται σε ειδικό αρχείο το οποίο διατηρεί η εταιρία ακόμη και αν δεν υπάρχουν ευρήματα κατά τον έλεγχο.

8.7. Η απόδοση σε ένα ή περισσότερα μέλη της Ομάδας Ελέγχου δικαιωμάτων πρόσβασης σε εργαλεία λογισμικού, συστήματα ή χώρους των εγκαταστάσεων, επιτρέπεται μόνο για το χρονικό διάστημα του αντίστοιχου ελέγχου.

8.8. Σε περίπτωση που προκύψουν ευρήματα κατά τον έλεγχο, η Εταιρία οφείλει να ορίσει τίς απαιτούμενες ενέργειες, όπως η αναθεώρηση διαδικασιών κλπ, το απαιτούμενο χρονοδιάγραμμα, τα εξουσιοδοτημένα άτομα. Αναλόγως με την κρισιμότητα των ευρημάτων η Εταιρία μπορεί να ενεργοποιήσει ή όχι η Πολιτική Διαχείρισης Περιστατικών Ασφαλείας.

8.9. Η Εταιρία διαθέτει και εφαρμόζει διαδικασία στην οποία αποτυπώνονται τα στάδια προετοιμασίας, διεξαγωγής, αποτελεσμάτων και διορθωτικών ενεργειών ελέγχου, σύμφωνα με τα αναφερόμενα στο παρόν άρθρο, και να διατηρεί, για όλους τους διεξαχθέντες ελέγχους, τα αντίστοιχα αρχεία.

9. Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού.

9.1. Η Εταιρία λαμβάνει όλα τα πιθανά μέτρα για την προστασία των ΠΕΣ από κακόβουλο λογισμικό χρησιμοποιώντας προγράμματα Anti-Virus και ενημερώνοντας τους εργαζόμενους της για τους τρόπους προστασίας και αντιμετώπισης των συστημάτων τους από κακόβουλο λογισμικό.

9.2. Σε περίπτωση ανίχνευσης κακόβουλου λογισμικού, η Εταιρία προβαίνει σε άμεση αξιολόγηση του περιστατικού και αναλόγως της κρισιμότητας του, ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφαλείας.

9.3. Η Εταιρεία προβαίνει σε ελέγχους στα ΠΕΣ κατά διαστήματα έτσι ώστε να διαπιστώσει ή μη, την ύπαρξη άλλου λογισμικού, μη εξουσιοδοτημένο.

9.4. Η Εταιρία διατηρεί αρχείο στο οποίο καταγράφονται οι λεπτομέρειες εφαρμογής των παραπάνω.

10. Πολιτική Χρήσης Κρυπτογραφίας.

10.1. Η Εταιρία για την πρόσβαση στα ΠΕΣ χρησιμοποιεί SSH (Secure Shell), και μόνο από την έμπιστη εσωτερική ζώνη δικτύου.

10.2. Όπου οι χρήστες των υπηρεσιών χρειάζεται να τοποθετήσουν κωδικούς πρόσβασης,

προστατεύονται με την χρήση SSL (Secure Socket Layers), τα οποία μπορεί να προέρχονται είτε από κάποιον πιστοποιημένο πάροχο ή από την ίδια την Εταιρία.

10.3. Η Εταιρία για την δημιουργία και διαχείριση των παραγομένων από την ίδια κλειδιών κρυπτογράφησης, τηρεί τις ανάλογες διαδικασίες.

10.4. Η κρυπτογράφηση εφαρμόζεται στα ΠΕΣ με βάση τα αποτελέσματα που προκύπτουν από την αποτίμηση κινδύνου σύμφωνα με την Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου .

10.5. Όπου χρησιμοποιούνται αλγόριθμοι και συστήματα κρυπτογράφησης, συμπεριλαμβανομένων και των αλγορίθμων ψηφιακής υπογραφής, λαμβάνονται υπόψη τα διεθνώς ευρέως αποδεκτά πρότυπα.

10.6. Το μήκος κλειδιού που χρησιμοποιείται λαμβάνει υπόψη τα διεθνώς και ευρέως αποδεκτά πρότυπα, ανάλογα με τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης και με τα αποτελέσματα της αποτίμησης κινδύνου, σύμφωνα με την Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου .

10.7. Η Εταιρία αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση στα κλειδιά τα οποία χρησιμοποιούνται για κρυπτογράφηση, αυθεντικοποίηση ή ψηφιακή υπογραφή.

10.8. Όπου χρησιμοποιούνται ασύμμετροι κρυπτογραφικοί αλγόριθμοι (α) για λογική πρόσβαση σε ΠΕΣ, (β) για κρυπτογράφηση ή (γ) για ψηφιακή υπογραφή, κάθε ζεύγος ιδιωτικού/δημόσιου κλειδιού αντιστοιχεί σε έναν μοναδικό χρήστη και το αντίστοιχο ιδιωτικό κλειδί είναι γνωστό μόνο στον συγκεκριμένο χρήστη, στον οποίο αντιστοιχεί.

10.9. Σε περίπτωση που Η Εταιρία χρησιμοποιήσει ψηφιακά πιστοποιητικά δημόσιων κλειδιών, τα οποία παράγονται από παρόχους υπηρεσιών πιστοποίησης, εξασφαλίζει ότι ο πάροχος υπηρεσιών πιστοποίησης συμμορφώνεται με την κείμενη νομοθεσία.

10.10. Σε περίπτωση που η Εταιρία παράξει και διαχειριστεί κλειδιά κρυπτογράφησης τα οποία χρησιμοποιούνται σε ΠΕΣ, καταρτίζει και τηρεί κατάλληλες διαδικασίες για τη δημιουργία, πιστοποίηση, διανομή και ανάκληση των κρυπτογραφικών κλειδιών.

10.11. Η Εταιρία διατηρεί αρχείο στο οποίο καταγράφονται οι λεπτομέρειες εφαρμογής των παραπάνω