VOICELAND

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΗ ΔΙΑΣΦΑΛΙΣΗ ΑΠΟΡΡΗΤΟΥ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

σύμφωνα με τις διατάξεις της Υ.Α. 165/2011 (ΦΕΚ 2715/Β/17.11.2011)

έκδοση: 2η/ **1-2-2023**

έγκριση: **Ι.Μ. Βαμβακάρης**

σκοπός

Σκοπός της Πολιτικής Ασφάλειας για τη Διασφάλιση Απορρήτου Ηλεκτρονικών Επικοινωνιών είναι ο καθορισμός των πολιτικών και των διαδικασιών που εφαρμόζει η εταιρεία στα πλαίσια συμμόρφωσης με τις απαιτήσεις του Κανονισμού της Α.Δ.Α.Ε. και του προτύπου ISO 27011 προκειμένου να προστατεύσει τα δεδομένα επικοινωνίας και τα Πληροφοριακά και Επικοινωνιακά Συστήματα (ΠΕΣ) από πιθανούς κινδύνους με στόχο τη διασφάλιση του απορρήτου των επικοινωνιών και τη διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών που διαχειρίζεται.

περιεχόμενα

0. ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΕΤΑΙΡΙΑΣ

1. Η Voiceland δραστηριοποιείται στο χώρο των τηλεπικοινωνιών. Ιδρύθηκε το 2011 από στελέχη με εμπειρία στον χώρο της πληροφορικής, με έδρα την Αθήνα.
2. Βασικός άξονας δράσης της εταιρείας είναι η παροχή εξειδικευμένων υπηρεσιών τηλεπικοινωνιών που απευθύνονται κυρίως σε επιχειρήσεις και επαγγελματίες. Οι υπηρεσίες αυτές, παρέχονται τόσο ως μελέτη, σχεδιασμό και υλοποίηση ολοκληρωμένων έργων, όσο και υπό τη μορφή υποστήριξης υπαρχουσών εγκαταστάσεων όλων των μεγεθών. Η εταιρεία αναλαμβάνει τη μελέτη και εγκατάσταση δικτυακών και διαδικτυακών τηλεπικοινωνιακών συστημάτων (VoIP) και τηλεφωνικών κέντρων VoIP.
3. Η Voiceland εξειδικεύεται στον χώρο της VoIP τηλεφωνίας καλύπτοντας όλο το φάσμα των υπηρεσιών που προσφέρει αυτή η τεχνολογία και εισάγοντας νέες ιδέες που προσφέρουν στον καταναλωτή καλύτερη και πιο αξιόπιστη επικοινωνία με τον υπόλοιπο κόσμο.
4. Σκοπός μας είναι η συνεχής αξιοποίηση και ενσωμάτωση των VoIP τεχνολογιών για τη βελτίωση της καθημερινότητας των πελατών μας. Στην Voiceland πιστεύουμε και επενδύουμε στις σχέσεις εμπιστοσύνης που αναπτύσσουμε με τους πελάτες μας. Επιδίωξή μας είναι η ανάπτυξη της δραστηριότητας μας, να συνδέεται άρρηκτα με την ανάπτυξη των δραστηριοτήτων των πελατών μας. Η αξιοπιστία, η υποστήριξη και η διασφάλιση των παρεχόμενων υπηρεσιών μας, αποτελεί κύριο γνώμονα της πορείας μας.

0.1. Βασικά στοιχεία

☞ **Έδρα εταιρείας**: Ιφιγενείας 81, Νέα Ιωνία, ΤΚ. 14231

☞ **Χώρος εγκατάστασης τηλεπικοινωνιακού εξοπλισμού**:

- Υπηρεσίες φωνής: Mednautilus(Ελλάδα), Google(Βέλγιο), AWS (Γερμανία)
- Αντίγραφα αρχείων: Google(Βέλγιο), AMAZON AWS (Γερμανία)

☞ **Αριθμός εργαζομένων**: 3

☞ **Στοιχεία επικοινωνίας**:

- Τηλ.: 212-222-8000
- Φαξ: 212-222-8001
- Κιν: 6937-358678
- URL: http:// www.voiceland.gr

0.2. Υπεύθυνος για τη Διασφάλιση του Απορρήτου Επικοινωνιών

5. Υπεύθυνος Ασφαλείας Πληροφοριών και Υπεύθυνος για τη διασφάλιση του απορρήτου των επικοινωνιών και υπεύθυνος για τον έλεγχο υλοποίησης των μέτρων και απαιτήσεων που ορίζονται στην παρούσα Πολιτική Ασφαλείας έχει οριστεί ο κ. Βασίλης Τζανουδάκης , e-mail: vasilios.tzanoudakis@voiceland.gr

0.3. Αδειοδότηση – Παρεχόμενες Υπηρεσίες

6. Η εταιρεία έχει λάβει τις ακόλουθες άδειες από την ΕΕΤΤ:

- A0101 Σταθερό Δημόσιο Τηλεφωνικό Δίκτυο
- B0201-Κ Μετάδοση δεδομένων
- B0201-Σ Μετάδοση δεδομένων
- **B0202-Κ SMS (Short Messaging Service) / MMS (Multimedia Messaging Service)**
- **B0202-Σ SMS (Short Messaging Service) / MMS (Multimedia Messaging Service)**
- B0203-Κ Δεδομένων Προστιθέμενης Αξίας
- B0203-Σ Δεδομένων Προστιθέμενης Αξίας
- B0401-Κ Τηλεηχοπληροφόρηση (Audiotext)
- B0401-Σ Τηλεηχοπληροφόρηση (Audiotext)
- B0403-Κ SMS / MMS Προστιθέμενης Αξίας
- B0403-Σ SMS / MMS Προστιθέμενης Αξίας
- B0701-Κ Παροχή υπηρεσιών πρόσβασης στο διαδίκτυο
- B0701-Σ Παροχή υπηρεσιών πρόσβασης στο διαδίκτυο
- **B0901-Κ Παροχή Τηλεφωνικών Υπηρεσιών**
- **B0901-Σ Παροχή Τηλεφωνικών Υπηρεσιών**
- **B0902-Κ Εικονικός Πάροχος Τηλεφωνικών Υπηρεσιών**
- **B0902-Σ Εικονικός Πάροχος Τηλεφωνικών Υπηρεσιών**
- **B0905-Κ Υπηρεσίες φωνής που παρέχονται μέσω διαδικτύου**
- **B0905-Σ Υπηρεσίες φωνής που παρέχονται μέσω διαδικτύου**
- B0906-Κ Υπηρεσίες Τηλεφωνικών Υπηρεσιών σε σταθερές θέσεις μέσω Προπ/ων Καρτών
- B0906-Σ Υπηρεσίες Τηλεφωνικών Υπηρεσιών σε σταθερές θέσεις μέσω Προπ/ων Καρτών
- B0907-Κ Υπηρεσίες αυτόματης επανάκλησης (Call-back)
- B0907-Σ Υπηρεσίες αυτόματης επανάκλησης (Call-back)
- B0908-Κ Υπηρεσίες Τηλεφωνικού Κέντρου (Call-shop)
- B0908-Σ Υπηρεσίες Τηλεφωνικού Κέντρου (Call-shop)
- B0909-Κ Παροχή κοινόχρηστων τηλεφώνων στο κοινό
- B0909-Σ Παροχή κοινόχρηστων τηλεφώνων στο κοινό

Με έντονη σήμανση παρουσιάζονται οι άδειες/ τομείς δραστηριότητας που χρησιμοποιούνται στην παρούσα φάση από την εταιρεία.

0.4. Προστατευόμενα Δεδομένα Επικοινωνιών

7. Τα δεδομένα επικοινωνίας τα οποία καταγράφονται και ελέγχονται από την εταιρεία είναι τα ακόλουθα:

Α. Υπηρεσίες φωνής

- Καλών αριθμός χρήστη υπηρεσίας
- Καλούμενος αριθμός
- Χρόνος διενέργειας και διάρκεια κλήσης

Β. Υπηρεσίες Fax

- Καλών αριθμός χρήστη υπηρεσίας
- Καλούμενος αριθμός
- Χρόνος διενέργειας και διάρκεια κλήσης

Γ. Υπηρεσίες SMS/ MMS

- Αριθμός αποστολέα χρήστη υπηρεσίας
- Αριθμός παραλήπτη
- Χρόνος διενέργειας

0.5. Σκοπός της Πολιτικής

8. Σκοπός της Πολιτικής Ασφάλειας για τη Διασφάλιση Απορρήτου Ηλεκτρονικών Επικοινωνιών είναι ο καθορισμός των πολιτικών και των διαδικασιών που εφαρμόζει η εταιρεία στα πλαίσια συμμόρφωσης με τις απαιτήσεις του Κανονισμού της Α.Δ.Α.Ε. προκειμένου να προστατεύσει τα δεδομένα επικοινωνίας και τα Πληροφοριακά και Επικοινωνιακά Συστήματα (ΠΕΣ) από πιθανούς κινδύνους με στόχο τη διασφάλιση του απορρήτου των επικοινωνιών και τη διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών που διαχειρίζεται.

9. Η παρούσα πολιτική αφορά τόσο τη Διοίκηση και το προσωπικό της εταιρείας όσο και τους χρήστες, συνδρομητές και συνεργάτες της εταιρείας.

0.6. Συμμόρφωση

10. **Η παρούσα πολιτική ακολουθεί πλήρως τις απαιτήσεις της Υ.Α. 165/2011 (ΦΕΚ 2715/Β/17.11.2011).** σύμφωνα με τον ακόλουθο πίνακα.

Άρθρο Υ.Α.	§	Άρθρο Υ.Α.	§	Άρθρο Υ.Α.	§
3.1.2	9	**5.2.2**	42	**6.5.3**	60, 61
3.2.1	βλ.Πίν. Περιεχομένων	**5.2.3**	42	**6.5.4**	60
3.2.2	20-21	**5.2.4**	42	**6.5.5**	57
3.2.3	20	**5.2.5**	41, 42, 43	**7.1.2**	62
3.2.4	22	**5.2.6**	41	**7.2.1**	62
3.2.5	22	**6.1.2**	44	**7.2.2**	63
3.2.6	5	**6.2.1**	44	**7.2.3**	63
3.2.7	11-18	**6.2.2**	44	**7.2.4**	62
3.2.8	28	**6.2.3**	45	**7.2.5**	62
3.2.9	29	**6.2.4**	46	**7.2.6**	64, 65
3.3.1	15	**6.2.5**	47	**7.2.7**	66
3.3.1.1	11	**6.2.6**	49	**7.3.1**	68
3.3.1.2	12-16	**6.3.1.1**	50, 51, 52	**7.3.2**	67
3.3.1.3	17	**6.3.1.2**	50	**8.2.1**	69
4.2.1	30	**6.3.1.3**	51	**8.2.2**	69
4.2.2	32	**6.3.1.4**	51	**8.2.3**	73
4.2.3	31	**6.3.2.1**	53	**8.3.1.1**	69
4.2.4	34	**6.4.1**	52, 54, 55, 56	**8.3.1.2**	70
4.3.1	33	**6.4.2.1**	44	**8.3.2.1**	71
4.3.2	31	**6.4.2.2**	54	**8.3.2.2**	71
4.3.3	34	**6.4.2.3**	51	**8.3.2.3**	71
4.4	35	**6.4.2.4**	56	**8.3.3.1**	72
4.5	36-37	**6.5.1**	57	**8.3.3.2**	72, 73
5.2.1	41	**6.5.2**	58, 59	**8.3.4.1**	75

Άρθρο Υ.Α.	§	Άρθρο Υ.Α.	§
8.3.4.2	76	**11.4.2**	98
8.3.4.3	76	**11.5**	100
9.1	77	**11.6.1**	97
9.2.1	77	**12.2.1**	102, 103
9.2.2	78,79, 80	**12.2.2**	104
9.2.3	81, 82	**12.2.3**	105, 106
9.2.4	78	**12.2.4**	107, 108, 109
9.2.5	83	**12.2.5**	109
9.2.6	84	**13.2.1**	110
10.2.1	85	**13.2.2**	111
10.2.2	86	**13.2.3**	112
10.2.3	86	**13.2.4**	112
10.2.4	87	**13.2.5**	113
10.3.1	88	**13.2.6**	113
10.3.2	89	**13.2.7**	112
10.3.3	90	**13.2.8**	114
10.3.4	91, 92, 93	**13.2.9**	113
11.2.1	94, 95		
11.2.2	94, 95		
11.2.3.1	96		
11.2.3.2	96, 97		
11.2.4	97		
11.3	95		
11.4.1	99, 100, 101		

Τα αρχεία που τηρούνται από την εταιρεία στα πλαίσια της παρούσας Πολιτικής παρουσιάζονται με έντονη γραφή (bold) και σημαίνονται με τη χρήση εικονιδίου:

1. Διαδικασία αποτίμησης κινδύνων

11. Ο Υπεύθυνος Ασφάλειας διατηρεί κατάλογο όλων των ΠΕΣ της εταιρείας και τον ενημερώνει ανάλογα με τις μεταβολές των πόρων στο αρχείο **Ε1-1 – Κατάλογος ΠΕΣ**.

12. Ο Υπεύθυνος Ασφάλειας διατηρεί κατάλογο των κινδύνων στο αρχείο **Ε1-2 Κατάλογος Απειλών** που απειλούν τους ανωτέρω πόρους καθώς και των ευπαθειών αυτών στο αρχείο **Ε1-3 Κατάλογος Ευπαθειών**. Ενημερώνει τους καταλόγους όποτε υπάρχει αλλαγή στον εξοπλισμό, τους χώρους ή τις δραστηριότητες της εταιρείας.

13. Οι κίνδυνοι εντάσσονται γενικά στις εξής ομάδες:

- Σκόπιμες κακόβουλες ενέργειες ανθρώπων.
- Φυσικά φαινόμενα.
- Λανθασμένες ενέργειες ανθρώπων – χωρίς δόλο.
- Αστοχία υλικού/λογισμικού/διαδικασιών.

14. Οι ευπάθειες ομαδοποιούνται στις εξής κατηγορίες:

- Περιβάλλον
- Υλικό
- Λογισμικό
- Επικοινωνίες
- Προσωπικό
- Διαδικασίες

15. Η εταιρεία διατηρεί και εφαρμόζει διαδικασία εκτίμησης κινδύνων ασφάλειας πληροφοριών, η οποία εκτελείται κατ' ελάχιστον μία φορά ανά έτος και βασίζεται στην εξής μεθοδολογία: Για κάθε ΠΕΣ εντοπίζονται οι κίνδυνοι που διατρέχει κατά την κανονική ροή της εργασίας και όταν η ροή της εργασίας αποκλίνει από το κανονικό και όταν συμβούν έκτακτα αλλά πιθανά γεγονότα.

16. Η επικινδυνότητα καθορίζεται με βάση τη βαρύτητα των συνεπειών εμφάνισης του κινδύνου στην επιχειρησιακή συνέχεια της εταιρείας και στη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των πληροφοριών, όπως εκφράζεται από την αξία του πόρου, τη στατιστική πιθανότητα εμφάνισης του κινδύνου, το βαθμό ευπάθειας του πόρου απέναντι στον κίνδυνο.

17. Κατά την αξιολόγηση εξετάζεται η χειρότερη περίπτωση που θα μπορούσε να προκύψει λόγω διαρροής, τροποποίησης, καταστροφής ή μη διαθεσιμότητας των ΠΕΣ, τόσο των άυλων, δηλαδή της διακινούμενης πληροφορίας, όσο και των υλικών, δηλαδή του ίδιου του πληροφορικού εξοπλισμού καθώς και του λοιπού τεχνικού εξοπλισμού που στηρίζει τη λειτουργία του ΠΕΣ. Ο Υπεύθυνος Ασφάλειας παρουσιάζει τα αποτέλεσμα της Αποτίμησης Κινδύνων στη διοίκηση της εταιρείας και τα αποτυπώνει στο αρχείο **Ε1-4 – Αποτίμηση Κινδύνων**. Το αρχείο διατηρείται από τον Υπεύθυνο Ασφαλείας προκειμένου να είναι ελέγξιμο, όποτε απαιτηθεί από τους αρμόδιους φορείς. Η αποτίμηση επαναλαμβάνεται ετησίως ή μετά από σημαντικές αλλαγές στα ΠΕΣ της εταιρείας.

18. Με βάση τα αποτελέσματα της Αποτίμησης Κινδύνων, ο Υπεύθυνος Ασφάλειας λαμβάνει σχετικά μέτρα ελέγχου και αντιμετώπισης και ελέγχει την ορθή και αποτελεσματική εφαρμογή τους. Αν απαιτείται προβαίνει στην αναθεώρηση της παρούσας Πολιτικής Ασφαλείας.

2. Γενικές αρχές

19. Η παρούσα Πολιτική Ασφαλείας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών έχει συνταχθεί με βάση τις απαιτήσεις της Απόφασης 165/2011 (ΦΕΚ 2715/Β/17.11.2011) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), λαμβάνοντας υπόψη τις σχετικές απαιτήσεις και πρακτικές του διεθνούς προτύπου ISO 27001:2013 για την εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

20. Η Πολιτική Ασφαλείας της εταιρείας αρθρώνεται σε επιμέρους πολιτικές, που περιέχονται στο παρόν έγγραφο, ακολουθώντας τη δομή των άρθρων της ανωτέρω Απόφασης. Κάθε κεφάλαιο του παρόντος παρουσιάζει τα μέτρα που λαμβάνει η εταιρεία προκειμένου να καλύψει τις απαιτήσεις που τίθενται από την ΑΔΑΕ. Στην περίπτωση απαιτήσεων της ανωτέρω Απόφασης, οι οποίες δεν καλύπτονται από την εταιρεία λόγω μη εφαρμοσιμότητας ή τεχνικής αδυναμίας γίνεται ειδική ανάλυση. Η αντιστοίχιση των απαιτήσεων των άρθρων της Απόφασης με την Πολιτική Ασφάλειας της εταιρείας παρουσιάζεται στην παράγραφο 0.6 του παρόντος.

21. Οι Πολιτικές που περιέχονται στο παρόν έγγραφο υλοποιούνται μέσω τεκμηριωμένων διαδικασιών Ασφαλείας Πληροφοριών, τις οποίες εφαρμόζει η εταιρεία με τη μορφή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Οι Διαδικασίες έχουν ως εξής:
    - ☞ Δ01 Συμβούλιο Ανασκόπησης
    - ☞ Δ02 Ελεγχος εγγραφων και αρχείων
    - ☞ Δ03 Εσωτερικες επιθεωρησεις
    - ☞ Δ04 Διαχείριση αστοχιών & παραπόνων - Διορθωτικες Προληπτικες Ενέργειες
    - ☞ Δ05 Εκπαίδευση προσωπικού
    - ☞ Δ06 Μέτρηση απόδοσης – στοχοθεσία
    - ☞ Δ07 Εκτίμηση κινδύνων
    - ☞ Δ08 Αντιμετώπιση κινδύνων
    - ☞ Δ09 Εγχειρίδιο αντιμετώπισης κινδύνων
    - ☞ Δ10 Διαχείριση περιστατικών ασφαλείας.

22. Οι ανωτέρω διαδικασίες καθορίζουν τις ενέργειες των εργαζομένων, συνεργατών και χρηστών της εταιρείας ως προς τη διαφύλαξη της Ασφάλειας των Πληροφοριών και Επικοινωνιών καθώς και τα τηρούμενα προς τούτο αρχεία. Επιπρόσθετα διαδικασίες ορίζουν τους αρμοδίους για την εκτέλεση των επιμέρους ενεργειών και την εφαρμογή των σχετικών πολιτικών. Για κρίσιμες θέσεις έχουν καταρτιστεί Περιγραφές Θέσεων Εργασίας, οι οποίες περιέχονται στο παράρτημα του παρόντος.

2.1. Τήρηση εγγράφων - αρχείων

23. Η παρούσα πολιτική Ασφαλείας υποστηρίζεται από επιμέρους διαδικασίας Ασφαλείας, σύμφωνα με το πρότυπο ISO 27001. Κάθε διαδικασία περιλαμβάνει τις απαιτούμενες ενέργειες, τους υπευθύνους υλοποίησης και τα τηρούμενα αρχεία. Ειδικά ορίζονται οι αρμόδιοι για το σχεδιασμό, ανάπτυξη, προμήθεια, εγκατάσταση, λειτουργία, διαχείριση, υποστήριξη, αναβάθμιση, επικαιροποίηση, διαγραφή και απόσυρση των ΠΕΣ της εταιρείας. Τα έγγραφα του τηρούνται στα πλαίσια της Πολιτικής Ασφάλειας καταγράφονται στο αρχείο **Ε2-1 Έλεγχος Εγγράφων**.
24. Η αναθεώρηση των εγγράφων γίνεται με ευθύνη του Υπεύθυνου Ασφαλείας ύστερα από συνεννόηση με την Διοίκηση της Εταιρείας. Κάθε αναθεώρηση ελέγχεται εάν είναι συμβατή με τις απαιτήσεις της πολιτικής της επιχείρησης, της κείμενης νομοθεσίας και ειδικά της Απόφασης 165/2011.
25. Σε περίπτωση οποιασδήποτε αλλαγής/ αναθεώρησης της παρούσας Πολιτικής, ο Υπεύθυνος Ασφαλείας Πληροφοριών της εταιρείας ενημερώνει σχετικά την ΑΔΑΕ, υποβάλλοντας την τρέχουσα έκδοση.
26. Όλα τα αρχεία που απαιτούνται από τις Πολιτικές και Διαδικασίες Ασφαλείας συμπληρώνονται από τους εκάστοτε υπεύθυνους και περιλαμβάνουν όλες τις πληροφορίες που πρέπει να καταγράφονται σε αυτά. Τα αρχεία οργανώνονται με τρόπο, ώστε να μην καταστρέφονται για το χρονικό διάστημα που πρέπει να τηρούνται, να διαφυλάσσεται η ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητά τους και να ανακτώνται εύκολα και γρήγορα. Τα αρχεία αναγνωρίζονται από τον τίτλο τους ή/ και τον κωδικό τους.
27. Πρόσβαση στα αρχεία έχει μόνο εξουσιοδοτημένο προσωπικό, όπως προκύπτει από τα ελεγχόμενα έγγραφα του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ή έχει λάβει σχετική έγκριση από τον υπεύθυνο τήρησης αυτών. Αρχεία τα οποία περιέχουν προσωπικά δεδομένα πελατών διακινούνται και αποθηκεύονται ασφαλώς και μετά το πέρας του χρόνου τήρησης καταστρέφονται πλήρως (π.χ. με πολλαπλή διαγραφή ή με χρήση καταστροφέα εγγράφων) ώστε να είναι μη αναγνώσιμα από μη εξουσιοδοτημένους τρίτους.
28. **Όλα τα αρχεία τηρούνται κατ' ελάχιστον για δύο (2) έτη από την ημερομηνία παραγωγής τους**, εκτός των εξαιρέσεων που επιβάλλονται από την νομοθεσία (Ν.3471/2006, 3783/2009, 3917/2011). Σε περίπτωση ελέγχου σε εξέλιξη από την ΑΔΑΕ, η εταιρεία διακόπτει κάθε διαδικασία καταστροφής αρχείων (χειροκίνητη ή αυτόματη) μέχρι το πέρας του ελέγχου και την σχετική έγκριση της ΑΔΑΕ.
29. Η εταιρεία διατηρεί ενημερωμένο κατάλογο αρχείων καταγραφής (**Ε2-2 Αρχεία καταγραφής**), ο οποίος περιλαμβάνει την ονομασία και περιγραφή κάθε αρχείου, τη θέση αποθήκευσης αυτού και

τα μέτρα για τη διασφάλιση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας αυτού. Όλες οι καταγραφές είναι πλήρεις και συνεχείς. Σε περίπτωση εντοπισμού οποιασδήποτε διακοπής καταγραφής, η εταιρεία ενεργοποιεί τη διαδικασία χειρισμού περιστατικού ασφαλείας.

3. Πολιτική αποδεκτής χρήσης

30. Οι εργαζόμενοι της εταιρείας κατά την έγκριση της παρούσης και κάθε νέος εργαζόμενος, κατά την έναρξη της εργασίας του λαμβάνει αντίγραφο της παρούσας Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών. Το ίδιο γίνεται και για τους συνεργάτες της εταιρείας, κατά την έναρξη της συνεργασίας. Η αποδοχή και η κατανόηση της Πολιτικής Ασφάλειας δηλώνονται ενυπόγραφα στο αρχείο **Ε3-1 Γνωστοποίηση Πολιτικής Ασφάλειας**.
31. Επιπλέον η κατανόηση, αποδοχή και εφαρμογή της Πολιτικής Ασφαλείας δηλώνεται στις εκάστοτε συμβάσεις έργου ή εργασίας που υπογράφει η εταιρεία με εργαζομένους και συνεργάτες. Μέσω των συμβάσεων συνεργασίας, οι εργαζόμενοι και οι συνεργάτες της εταιρείας δεσμεύονται με σχετικούς όρους εμπιστευτικότητας/ μη αποκάλυψης να μην αποκαλύπτουν οποιαδήποτε πληροφορία ή στοιχείο έλθει στην αντίληψη ή κατοχή τους ως αποτέλεσμα της φύσης της εργασίας τους. Επιπλέον δηλώνουν ότι έχουν λάβει γνώση των απαιτήσεων και μέτρων ασφαλείας, τα οποία λαμβάνει η εταιρεία και ότι αποδέχονται πλήρως και ανεπιφύλακτα την εφαρμογή τους. Τέλος, συμφωνούν στην οριστική διαγραφή και καταστροφή όποιων εταιρικών στοιχείων και δεδομένων ενδέχεται να έχουν περιέλθει στην κατοχή τους μετά τη λήξη της συνεργασίας.
32. Ο Υπεύθυνος Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών αναλαμβάνει να εκπαιδεύσει το προσωπικό της εταιρείας και τους συνεργάτες κατά την έναρξη της συνεργασίας. Επιπλέον διενεργεί περιοδικές εκπαιδεύσεις υπόμνησης της Πολιτικής καθώς και όποτε πραγματοποιούνται αλλαγές στην Πολιτική. Ο Υπεύθυνος Ασφάλειας της εταιρείας διενεργεί αναλυτική εκπαίδευση για τη διαδικασία εντοπισμού και χειρισμού περιστατικών ασφαλείας, ώστε οι εργαζόμενοι και συνεργάτες να είναι σε θέση να τον ενημερώσουν άμεσα αν υποπέσει στην αντίληψή τους κενό ή περιστατικό ασφαλείας που θέτει σε κίνδυνο το απόρρητο των επικοινωνιών.
33. Ο Υπεύθυνος Ασφάλειας τηρεί κατάλογο εργαζομένων και συνεργατών (νομικών και φυσικών προσώπων), οι οποίο έχουν ή ενδέχεται να αποκτήσουν πρόσβαση σε δεδομένων επικοινωνιών:

☞ **Ε3-2: Κατάλογος προσωπικού εταιρείας**

☞ **Ε3-3: Κατάλογος συνεργατών εταιρείας**

34. Σε περίπτωση που εντοπιστεί οποιαδήποτε παραβίαση των ανωτέρω συμβατικών όρων από οποιοδήποτε συνεργάτη ή εργαζόμενο της εταιρείας, ο Υπεύθυνος Ασφαλείας ενεργοποιεί άμεσα τη διαδικασία χειρισμού περιστατικών Ασφαλείας.
35. Η εταιρεία, μέσω της ιστοσελίδας της παρέχει ενημέρωση προς τους χρήστες των υπηρεσιών της σχετικά με τους κανόνες ορθής χρήσης των παρεχόμενων υπηρεσιών και με των διαδικασιών ασφάλειας που οφείλουν να χρησιμοποιούν για τη διασφάλιση του απορρήτου τους.

3.1. Πολιτική Διαχείρισης Αποθηκευτικών Μέσων

36. Τα αποθηκευτικά μέσα που περιέχουν δεδομένα επικοινωνιών ή περιέχουν άλλα δεδομένα που μπορεί να οδηγήσουν σε πρόσβαση σε ΠΕΣ (πχ κωδικούς πρόσβασης) τυγχάνουν ειδικής μεταχείρισης. Συγκεκριμένα κατά την ανακύκλωση / απόρριψη των ιδίων ή των συσκευών που τα περιλαμβάνουν εφαρμόζεται η διαδικασία που αναφέρεται στην πολιτική «Διαχείρισης και Εγκατάστασης ΠΕΣ». Η χρήση τους επιτρέπεται μόνο σε προκαθορισμένους χώρους της εταιρείας. Στις περιπτώσεις έντυπων μέσων αποθήκευσης η φύλαξη τους γίνεται σε ασφαλισμένο χώρο και η καταστροφή τους, όταν δεν χρειάζονται πλέον, είναι ολοσχερής με χρήση καταστροφέα εγγράφων.
37. Οι εξυπηρετητές της εταιρείας βασίζονται σε virtual υποδομές οι οποίες είναι ανεπτυγμένες σε φυσικές υποδομές (φυσικοί Servers και . αποθηκευτικά μέσα) οι οποίες διαθέτουν μηχανισμούς που εξασφαλίζουν υψηλή διαθεσιμότητα.

3.2. Πολιτική Αρχειοθέτησης Δεδομένων

38. Η εταιρεία εφαρμόζει μεθοδολογία λήψης πολλαπλών αντιγράφων ασφαλείας για όλα τα κρίσιμα δεδομένα των συστημάτων της. Οι βασικές αρχές της πολιτικής αρχειοθέτησης είναι οι εξής:

- Καθημερινή λήψη backup όλων των δεδομένων διαμόρφωσης των συστημάτων (συμπεριλαμβανομένων των ρυθμίσεων του firewall), όλων των βάσεων δεδομένων που τηρούν επικοινωνιακά δεδομένα (CDR, logs, κλπ) και όλων των αρχείων ενεργειών (logs)

39. Τα ανωτέρω αρχεία αποθηκεύονται για χρονικό διάστημα που έχει οριστεί ως εξής:

- Ένα (1) έτος για τα δεδομένα επικοινωνιών σύμφωνα με τη νομοθεσία (Ν.3471/2006, 3783/2009, 3917/2011).
- Δύο (2) έτη για τα αρχεία καταγραφών των Πληροφοριακών και Επικοινωνιακών Συστημάτων

Τα αντίγραφα ασφαλείας αποθηκεύονται σε virtual Server ο οποίος είναι εγκατεστημένος στο Datacenter της Google στο Βέλγιο και στην Amazon στη Γερμανία.

4. Πολιτική Φυσικής Ασφάλειας

41. Η εταιρεία λαμβάνει όλα τα δυνατά μέτρα για τη διαφύλαξη της φυσικής ασφάλειας των εγκαταστάσεων του εξοπλισμού της που χρησιμοποιείται για την παροχή υπηρεσιών επικοινωνίας.

ΚΥΡΙΑΠΕΣ	Τα κύρια ΠΕΣ της εταιρείας φιλοξενούνται σε virtual υποδομές που παρέχουν οι εταιρείες Mednautilus, Amazon, και Google. Οι συγκεκριμένες εταιρείες εφαρμόζουν μέτρα όπως τα ακόλουθα για τη διασφάλιση της Ασφάλειας Πληροφοριών των πληροφοριακών υποδομών μέσω των οποίων παρέχονται οι virtual υποδομές: ▪ Παρακολούθηση και καταγραφή μέσω κλειστού κυκλώματος των εξωτερικών προσβάσεων, των εισόδων, των χώρων και των server rooms ▪ Ελεγχόμενη πρόσβαση στους φυσικούς εξυπηρετητές που φιλοξενούν τις virtual υποδομές ▪ Ελεγχόμενες περιβαλλοντικές συνθήκες ▪ Πολλαπλά συστήματα UPS και H/Z με χρήση πετρελαίου ▪ Συστήματα άμεσης πυρανίχνευσης

ΥΠΟΣΤΗΡΙΚΤΙΚΑΠΕΣ	Η εταιρεία χρησιμοποιεί υποστηρικτικά πληροφοριακά και επικοινωνιακά συστήματα για τη διαχείριση των Κύριων ΠΕΣ. Τα συγκεκριμένα συστήματα είναι εγκατεστημένα στα γραφεία της εταιρείας σε χώρο ελεγχόμενης πρόσβασης.

42. Η πρόσβαση στις ανωτέρω εγκαταστάσεις αυτές είναι αυστηρά ελεγχόμενη σύμφωνα με τις ακόλουθες αρχές και διαδικασίες:

- Απαγορεύεται αυστηρά η μη εξουσιοδοτημένη είσοδος και παραμονή προσωπικού και συνεργατών της εταιρείας.
- Πρόσβαση δίδεται μόνον κατόπιν αίτησης προς τον Υπεύθυνο Ασφάλειας της εταιρείας, για συγκεκριμένη χρονική περίοδο και με πλήρη αιτιολόγηση του σκοπού αυτής.
- Η εταιρεία τηρεί το αρχείο **Ε4-1 – Έλεγχος πρόσβασης**, στο οποίο καταγράφεται:
    - Το ονοματεπώνυμο του προσώπου
    - Η ημερομηνία, η ώρα εισόδου και εξόδου του προσώπου
    - Ο εγκρίνων την πρόσβαση

- Ο σκοπός της πρόσβασης.
- Ο χώρος/ εξοπλισμός στον οποίο επιτρέπεται η πρόσβαση.

- Καθ' όλη την παραμονή του προσώπου, αυτό συνοδεύεται και επιβλέπεται από τον Υπεύθυνο.

43. Οι χώροι εγκατάστασης ΠΕΣ της εταιρείας αναλυτικά και τα σχετικά μέτρα ασφαλείας και ελέγχου πρόσβασης καταγράφονται αναλυτικά στο αρχείο **Ε4-2 Ασφαλείς Περιοχές**.

5. Πολιτική Λογικής Πρόσβασης

44. Η παρούσα πολιτική εφαρμόζεται για όλους του εργαζομένους και συνεργάτες της εταιρείας, οι οποίοι μπορούν να αποκτήσουν πρόσβαση στα ΠΕΣ της εταιρείας. Οι εργαζόμενοι και συνεργάτες της εταιρείας μπορούν να αποκτήσουν πρόσβαση στα ΠΕΣ της εταιρείας μόνο μετά την επιτυχή εισαγωγή προσωπικού κωδικού και συνθηματικού. Ο προσωπικός κωδικός αποδίδεται από την Υπεύθυνο Ασφάλειας και απενεργοποιείται κατά τη λήξη της συνεργασίας. Όλοι οι ενεργοί κωδικοί πρόσβασης το προσφερόμενο επίπεδο πρόσβασης, η Ομάδα Ασφαλείας όπου ανήκουν, η ημερομηνία ενεργοποίησης καθώς και η ημερομηνία απενεργοποίησης τηρούνται από τον Υπεύθυνο Ασφαλείας στο αρχείο **Ε5-1 – Λογαριασμοί πρόσβασης ανά ΠΕΣ**. Οι κωδικοί πρόσβασης είναι προσωπικοί και δεν υποδεικνύουν ρόλο και δικαιώματα πρόσβασης. Αρχικοί κωδικοί και διαχειριστικοί κωδικοί (administrator, root) έχουν απενεργοποιηθεί. Τηρείται πλήρες ιστορικό του ανωτέρω αρχείου με ευθύνη του Υπευθύνου Ασφάλειας, μέσω του οποίου μπορεί να ελεγχθεί η ιστορικότητα δικαιωμάτων και προσβάσεων. Απαγορεύεται αυστηρά η ύπαρξη κωδικών πρόσβασης χωρίς συνθηματικό. Προς τούτο διενεργούνται περιοδικοί έλεγχοι από τον Υπεύθυνο Ασφαλείας.
45. Για τα ΠΕΣ στα οποία δεν είναι εφικτή λόγω τεχνικών χαρακτηριστικών ή επιχειρησιακών αναγκών η δημιουργία προσωπικού κωδικού, ο Υπεύθυνος Ασφαλείας τηρεί το αρχείο **Ε5-2-Κοινόχρηστοι λογαριασμοί πρόσβασης**, όπου καταγράφονται οι εργαζόμενοι που έχουν λάβει γνώση του εν λόγω κωδικού. Οι λόγοι δημιουργίας κοινόχρηστού λογαριασμού είναι οι εξής:
    - Το ΠΕΣ δεν υποστηρίζει την δυνατότητα δημιουργίας προσωπικών κωδικών
    - Αδυναμία τέλεσης εργασιών συντήρησης ή παραμετροποίησης του ΠΕΣ.

    Οι ανωτέρω κοινόχρηστοι κωδικοί αποδίδονται σε πρόσωπα με υψηλό βαθμό πρόσβασης και περιορίζονται σε μια μόνο ομάδα προσώπων.
46. Ο Υπεύθυνος Ασφαλείας τηρεί αρχείο **Ε5-3 Δικαιώματα πρόσβασης**, όπου καταγράφονται όλες οι κατηγορίες των χρηστών και τα δικαιώματα πρόσβασης αυτών για κάθε ΠΕΣ της εταιρείας
47. Τα ΠΕΣ της εταιρείας έχουν παραμετροποιηθεί ώστε να διατηρούν για **τουλάχιστον 2 έτη και αδιάλειπτα αρχεία καταγραφής πρόσβασης (access logs)**, τα οποία αποτυπώνουν το όνομα χρήστη, την ώρα έναρξης και την ώρα λήξης της πρόσβασης στο ΠΕΣ. Επίσης καταγράφουν

αποτυχημένες προσπάθειες εισόδου στο ΠΕΣ. Μετά από 10 αποτυχημένες προσπάθειες (για τα ΠΕΣ όπου αυτό υποστηρίζεται) ο λογαριασμός απενεργοποιείται και μπορεί να ενεργοποιηθεί μόνο από τον Υπεύθυνο Ασφαλείας.

48. Τα ανωτέρω αρχεία έχουν συνεχή και αδιάλειπτη καταγραφή. Σε περίπτωση που κατά τη διάρκεια ελέγχου από τον Υπεύθυνο Ασφάλειας διαπιστωθεί διακοπή στην καταγραφή, ενεργοποιείται η Διαδικασία Χειρισμού Περιστατικών Ασφαλείας.
49. Ειδικά για τα δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των υπηρεσιών της εταιρείας, τηρείται ειδικό αρχείο **E5-4 Πρόσβαση σε δεδομένα επικοινωνιών** με τους χρήστες που είναι εξουσιοδοτημένοι να έχουν πρόσβαση, τον τρόπο πρόσβασης και όλες τις περιπτώσεις στις οποίες αποκτήθηκε πρόσβαση. Το αρχείο περιέχει σχετική αιτιολόγηση για κάθε τέτοια πρόσβαση.

5.1. Διαχείριση λογαριασμών πρόσβασης

50. Η εταιρεία εφαρμόζει σαφή και τεκμηριωμένη διαδικασία διαχείρισης λογαριασμών πρόσβασης, η οποία καλύπτει:
    - Αίτηση, έγκριση από τον Υπεύθυνο Ασφαλείας και δημιουργία λογαριασμού πρόσβασης
    - Αλλαγή δικαιωμάτων πρόσβασης
    - Κατάργηση λογαριασμού πρόσβασης.
51. Όλες οι ανωτέρω ενέργειες ελέγχονται και εγκρίνονται από τον Υπεύθυνο Ασφαλείας της εταιρείας και καταγράφονται στο αρχείο **E5-1 – Λογαριασμοί πρόσβασης ανά ΠΕΣ** (λογαριασμός, δικαιώματα πρόσβασης, χρόνος έναρξης, χρόνος λήξης).
52. Για τη δημιουργία ονομάτων χρήστη, ο Υπεύθυνος Ασφαλείας επιλέγει το αρχικό γράμμα του ονόματος του εργαζομένου, ακολουθούμενο από το πλήρες επώνυμο. Σε περίπτωση που προκύπτει υφιστάμενο όνομα χρήστη, προστίθενται επιπλέον γράμματα του ονόματος του εργαζομένου ή το πατρώνυμο αυτού. Ο κωδικός πρόσβασης παράγεται αυτόματα από σχετική γεννήτρια τυχαίων συνθηματικών, στην οποία έχουν ρυθμιστεί οι προδιαγραφές συνθηματικών που καταγράφονται κατωτέρω. Κατά την ανάθεση του ονόματος χρήστη σε εργαζόμενο ή συνεργάτη, αυτός υπογράφει στο σχετικό αρχείο **E9-10 – Έντυπο έναρξης-λήξης συνεργασίας** και αποδέχεται τους όρους χρήσης του κωδικού πρόσβασης που του έχει δοθεί.
53. Ο Υπεύθυνος Ασφαλείας διενεργεί τριμηνιαίους ελέγχους για:
    - ☞ Την ύπαρξη μόνον εγκεκριμένων λογαριασμών πρόσβασης και την αντιπαραβολή αυτών με το αρχείο E5.1
    - ☞ Για την ακρίβεια και καταλληλότητα των δικαιωμάτων πρόσβασης που έχουν δοθεί

- ☞ Για τις επιτυχημένες και ανεπιτυχείς προσβάσεις που έχουν καταγραφεί στα Access Logs.

54. Τα συνθηματικά που επιβάλλονται από τα ΠΕΣ για τους διαχειριστές και το προσωπικό της εταιρείας αποτελούνται από τουλάχιστον 8 χαρακτήρες (μικρά- κεφαλαία), αριθμούς και σύμβολα, απαιτείται από το ΠΕΣ η αλλαγή τους κάθε 90 ημέρες και δεν μπορεί να είναι τα ίδια με τα 5 προηγούμενα συνθηματικά.
55. Κατά τη δημιουργία του συνθηματικού τα ΠΕΣ ρυθμίζονται ώστε να ζητούν υποχρεωτική αλλαγή συνθηματικού από το χρήστη. Εναλλακτικά ο χρήστης επιλέγει νέο συνθηματικό επί τόπου.
56. Μετά από 10 αποτυχημένες προσπάθειες (για τα ΠΕΣ όπου αυτό υποστηρίζεται) ο λογαριασμός απενεργοποιείται και μπορεί να ενεργοποιηθεί μόνο από τον Υπεύθυνο Ασφαλείας.

5.2. Έλεγχος πρόσβασης χρηστών/ συνδρομητών

57. Οι χρήστες των υπηρεσιών που προσφέρονται από την εταιρεία έχουν πρόσβαση σε αυτές μέσω προσωπικού ονόματος και κωδικού χρήστη που τους αποδίδεται κατά την εγγραφή τους και την υπογραφή σχετικής σύμβασης. Δεν επιτρέπεται καμία πρόσβαση στις υπηρεσίες επικοινωνίας καθώς σε εφαρμογές διαχείρισης αυτών (π.χ. αρχείο κλήσεων, τιμολογήσεις) χωρίς την εισαγωγή σχετικού κωδικού πρόσβασης. Μέσω της σύμβασης, η εταιρεία ενημερώνει τους χρήστες ότι οι κωδικοί είναι αυστηρά προσωπικοί και δεν επιτρέπεται η αποκάλυψή τους σε τρίτους. Επιπλέον τους ενημερώνει για τους ισχύοντες κανόνες ενδεδειγμένης χρήσης.
58. Για την ενεργοποίηση πρόσβασης στις υπηρεσίες της, ο Υπεύθυνος Ασφάλειας ζητά και τηρεί αρχείο αντιγράφου της Ταυτότητας ή του Διαβατηρίου του πελάτη καθώς αντίγραφο λογαριασμού Τηλεφωνίας ή ΔΕΚΟ, μέσω των οποίων αποδεικνύεται η ταυτότητα του, η νόμιμη διεύθυνση και η ιδιοκτησία συγκεκριμένων αριθμών τηλεφώνου. Αν πρόκειται για Εταιρεία τότε ζητείται και το καταστατικό ή το ΦΕΚ. Τα ανωτέρω αρχεία τηρούνται κρυπτογραφημένα στον εξυπηρετητή της εταιρείας.
59. Η διαχείριση των ανωτέρω λογαριασμών γίνεται μέσα από ειδική εφαρμογή διαχείρισης, η οποία παράγει το όνομα και το συνθηματικό του χρήστη σύμφωνα με κανόνες που έχουν αναφερθεί ανωτέρω.
60. Μέσω εφαρμογής διαχείρισης των υπηρεσιών που προσφέρεται στο χρήστη, δίνεται η δυνατότητα αλλαγής και επαναφοράς του συνθηματικού του. Η εφαρμογή επιβάλλει την επιλογή ισχυρού κωδικού πρόσβασης στο χρήστη. Επιπλέον, οι χρήστες θα ενημερώνονται κάθε 3 μήνες να αλλάζουν τα passwords για λόγους ασφαλείας. Η πρόσβαση στην εφαρμογή διαχείρισης προστατεύεται με κρυπτογράφηση SSL (σελίδα HTTPS).

61. Μετά τη λήξη της παροχής υπηρεσιών σε χρήστη/ συνδρομητή ο λογαριασμός του απενεργοποιείται κεντρικά – χωρίς να διαγράφεται, οπότε διακόπτεται κάθε δυνατότητα πρόσβασης και χρήσης των υπηρεσιών και συστημάτων. Όλα τα αρχεία καταγραφής που τον αφορούν δε διαγράφονται αλλά διατηρούνται για το προβλεπόμενο χρονικό διάστημα.

6. Πολιτική Απομακρυσμένης Λογικής Πρόσβασης

62. Η παρούσα πολιτική εφαρμόζεται για όλους του εργαζομένους και συνεργάτες της εταιρείας, οι οποίοι μπορούν να αποκτήσουν απομακρυσμένη πρόσβαση στα ΠΕΣ της εταιρείας. Άδεια απομακρυσμένης λογικής πρόσβασης δίδεται σε εργαζομένους και συνεργάτες της εταιρίας για την τέλεση τεχνικών εργασιών σε ΠΕΣ ή άντληση πληροφοριών όταν συντρέχει λόγος και μόνον εφόσον δεν παραβιάζονται οι κανόνες και πολιτικές ασφάλειας των δικτύων. Η απομακρυσμένη πρόσβαση υλοποιείται μόνο μέσω ασφαλών μηχανισμών (VPN, SSH) με χρήση θυρών διαφορετικών από τις συνήθεις και προσωπικούς κωδικούς πρόσβασης.
63. Ο Υπεύθυνος Ασφαλείας τηρεί το αρχείο **Ε6-1 – Απομακρυσμένη πρόσβαση**, στο οποίο αποτυπώνει ανά ΠΕΣ τους εργαζομένους ή συνεργάτες για τους οποίους έχει εγκριθεί η πρόσβαση, ο μηχανισμός ασφαλείας (VPN, SSH), το επίπεδο της πρόσβασης και η διάρκεια της (κατ' αίτηση ή μόνιμη), η ημερομηνία έναρξης και λήξης της έγκρισης.
64. Η δυνατότητα απομακρυσμένης πρόσβασης, ειδικά στην περίπτωση συνεργατών, δεν έχει μόνιμο χαρακτήρα. Για αυτό το λόγο οι λογαριασμοί που χρησιμοποιούνται για απομακρυσμένη πρόσβαση είναι απενεργοποιημένοι και ενεργοποιούνται μόνο όταν συντρέχει λόγος απομακρυσμένης πρόσβασης και με το πέρας απενεργοποιούνται.
65. Τα ΠΕΣ της εταιρείας έχουν παραμετροποιηθεί ώστε να διατηρούν για τ**ουλάχιστον 2 έτη και αδιάλειπτα αρχεία καταγραφής απομακρυσμένης πρόσβασης (access logs)**, τα οποία αποτυπώνουν το όνομα χρήστη, την ώρα έναρξης και την ώρα λήξης της απομακρυσμένης πρόσβασης στο ΠΕΣ. Επίσης καταγράφουν αποτυχημένες προσπάθειες εισόδου στο ΠΕΣ.
66. Η άδεια προς τους συνεργάτες για απομακρυσμένη πρόσβαση εγκρίνεται όταν ο Υπεύθυνος Ασφαλείας κρίνει ότι συντρέχει λόγος και αφού προαποφασιστεί για ποια ΠΕΣ πρόκειται και για ποια χρονική περίοδο. Οι κινήσεις/ εργασίες που πραγματοποιεί ο συνεργάτης σε ΠΕΣ κατά την διάρκεια της απομακρυσμένης πρόσβασης παρακολουθούνται κατά το μέγιστο εφικτό βαθμό από τον Υπεύθυνο Ασφαλείας της εταιρίας. Η δημιουργία και ενεργοποίηση σχετικών κωδικών από τον Υπεύθυνο Ασφαλείας, ο λόγος πρόσβασης στο ΠΕΣ και το χρονικό διάστημα που αυτή ήταν εφικτή καταγράφεται στο αρχείο **Ε6-2 – Ιστορικό απομακρυσμένης πρόσβασης**.
67. Ο Υπεύθυνος Ασφάλειας κάθε 2 μήνες ελέγχει ότι υπάρχουν λογαριασμοί απομακρυσμένης λογικής πρόσβασης μόνο για τους εργαζόμενους και συνεργάτες που αναφέρονται στο ανωτέρω αρχείο, και ότι είναι απενεργοποιημένοι ως προεπιλογή.
68. Η δημιουργία, διαχείριση, ενεργοποίηση και απενεργοποίηση των λογαριασμών απομακρυσμένης πρόσβασης εφαρμόζεται από τον Υπεύθυνο Ασφαλείας της εταιρείας σύμφωνα με τα ανωτέρω.

7. Πολιτική Διαχείρισης και Εγκατάστασης ΠΕΣ

69. Η εταιρεία διατηρεί και εφαρμόζει τεκμηριωμένες διαδικασίες για την προμήθεια/ ανάπτυξη υλικού και λογισμικού, την εγκατάσταση και λειτουργία αυτού και τη συντήρηση/ υποστήριξη/ λειτουργία αυτού καθώς και την απόσυρσή του. Πριν την έναρξη διαδικασιών προμήθειας ΠΕΣ, γίνεται αποτίμηση κινδύνων σχετικά με το απόρρητο των επικοινωνιών που θα μπορούσε να επηρεάσει το υπό προμήθεια/ εγκατάσταση ΠΕΣ. Κάθε αλλαγή στα ΠΕΣ που σχετίζεται με τη διασφάλιση του απορρήτου θα πραγματοποιείται άμεσα μετά την αναγνώριση της ανάγκης της και χωρίς καθυστέρηση. Οι βασικές αρχές που διέπουν τις ανωτέρω διαδικασίες με στόχο την ελαχιστοποίηση του κινδύνου διαρροής πληροφοριών που σχετίζονται με το απόρρητο των επικοινωνιών των συνδρομητών ή χρηστών των υπηρεσιών είναι οι εξής:

70. **Α. Προμήθεια**: Στην περίπτωση προμήθειας ολοκληρωμένου ΠΕΣ (αυτόνομη συσκευή που περιλαμβάνει ειδικό υλικό τηλεπικοινωνιών και ειδικό λογισμικό τηλεπικοινωνιών) από συγκεκριμένο κατασκευαστή, καταρτίζεται λίστα απαιτήσεων από το τεχνικό τμήμα που θα πρέπει να πληροί το υποψήφιο ΠΕΣ ώστε να διασφαλίζει την ομαλή λειτουργία του, το απόρρητο των επικοινωνιών και ο κατασκευαστής υποχρεούται σε συμμόρφωση. Σε περίπτωση προμήθειας ΠΕΣ, που αποτελείται από μεμονωμένα υλικά και λογισμικό που οι κατασκευαστές τα προορίζουν για γενική χρήση δεν απαιτείται η σύνταξη προδιαγραφών προς τον κατασκευαστή. Σε κάθε περίπτωση συντάσσονται προδιαγραφές ασφαλείας του προς προμήθεια υλικού σε σχέση με τη διασφάλιση του απορρήτου των επικοινωνιών και εγκρίνονται από τον Υπεύθυνο Ασφαλείας.

71. **Β. Δοκιμή – Αποδοχή**: Στην περίπτωση εγκατάστασης κάθε νέου ΠΕΣ υλοποιείται δοκιμαστική φάση λειτουργίας, πριν δοθεί για παραγωγική χρήση. Τα αποτελέσματα των δοκιμών βάσει των απαιτήσεων καθώς και η αξιολόγηση τους από τον Υπεύθυνο Ασφαλείας καταγράφονται σε σχετικό αίτημα στο σύστημα ticketing του Συστήματος. Πιο συγκεκριμένα καταγράφονται οι ακόλουθες πληροφορίες:

- ☞ Η ταυτότητα του ΠΕΣ το οποίο θα τεθεί σε δοκιμαστική λειτουργία
- ☞ Οι έλεγχοι που θα πραγματοποιηθούν
- ☞ Τα αποτελέσματα των ελέγχων

Κατά το αρχικό στάδιο λειτουργίας γίνεται στενή παρακολούθηση για τον έγκαιρο εντοπισμό πιθανών σφαλμάτων, είτε πρόκειται για σφάλματα που εμποδίζουν την ομαλή παροχή υπηρεσιών ή σφάλματα σχετικά με την ασφάλεια. Πιθανά ευρήματα καταγράφονται στο

ανωτέρω αρχείο. Στο τέλος της διαδικασίας, ο Υπεύθυνος Ασφαλείας συντάσσει το **Ε7-2 Έκθεση Αποδοχής ΠΕΣ**.

72. **Γ. Λειτουργία - Συντήρηση**: Όλα τα ΠΕΣ παρακολουθούνται κατά την διάρκεια λειτουργίας τους και ελέγχονται οι καταγραφές των συμβάντων ώστε αν προκύψει ζήτημα ασφάλειας ή σφάλματος να γίνει άμεσα αντιληπτό και να ενημερωθεί ο Υπεύθυνος Ασφαλείας, ώστε να ενεργοποιήσει τη διαδικασία Διαχείρισης Περιστατικών Ασφαλείας. Στο λειτουργικό σύστημα των ΠΕΣ της εταιρείας είναι ενεργοποιημένη η δυνατότητα καταγραφής συμβάντων που παρέχει ο κατασκευαστής του λειτουργικού, τουλάχιστο στα κυρίως τμήματα (συστήματος, εφαρμογής) (event logs). **Οι εγγραφές διατηρούνται για διάστημα τουλάχιστο 2 ετών**.
73. Για κάθε αλλαγή σε λειτουργικό ΠΕΣ (τόσο στο hardware όσο και στο software – λειτουργικό σύστημα και εφαρμογές) η εταιρεία εφαρμόζει διαδικασία διαχείρισης αλλαγών (Change Management). Τα αιτήματα αλλαγών υποβάλλονται στον Υπεύθυνο Ασφαλείας μέσω αιτήματος στο σύστημα ticketing, στο οποίο καταγράφονται:
    - ☞ Το ΠΕΣ που επηρεάζεται
    - ☞ Το είδος της αλλαγής και οι πιθανές επιπτώσεις ως προς τη Ασφάλεια
    - ☞ Ενέργειες υλοποίησης της αλλαγής
    - ☞ Σχέδιο ανάκαμψης σε περίπτωση αποτυχίας της αλλαγής
    - ☞ Η ημερομηνία και ο υπεύθυνος υλοποίησης της αλλαγής.
    - ☞ Ο έλεγχος καλής λειτουργίας μετά την αλλαγή.
74. Ο Υπεύθυνος Ασφαλείας τα αξιολογεί και εφόσον τα εγκρίνει, προχωρά η υλοποίηση. Αλλαγές σε λογισμικό ή υλικό των ΠΕΣ που σχετίζονται άμεσα με την ασφάλεια δεδομένων επικοινωνιών πραγματοποιούνται χωρίς καθυστερήσεις.

75. **Δ. Απόσυρση**: Όταν ο κύκλος ζωής ενός ΠΕΣ έχει τελειώσει και δεν υπάρχει περίπτωση να ξαναχρησιμοποιηθεί στο μέλλον, αποσύρεται και διαγράφεται από τα πάγια της εταιρίας προκειμένου να απορριφθεί σε κατάλληλο χώρο. Κατά την διαδικασία απόσυρσης, δεδομένα ή λογισμικό επικοινωνιών που είναι αποθηκευμένα σε μαγνητικά μέσα, οπτικά μέσα, ή μέσα με ηλεκτρονικά κυκλώματα (αναφέρονται ενδεικτικά: σκληροί δίσκοι, CD-ROM, Solid State Disks) καταστρέφονται ώστε να μην είναι δυνατή η ανάγνωση τους με θραύση ή διάτρηση. Πριν την εξαγωγή ΠΕΣ από τις εγκαταστάσεις της εταιρίας προς απόσυρση, τα αποθηκευτικά μέσα που αναφέρονται ανωτέρω, καταστρέφονται οριστικά (με μηχανικά ή άλλα μέσα) παρουσία του Υπευθύνου Ασφαλείας.

76. Ο Υπεύθυνος Ασφαλείας τηρεί το αρχείο **Ε7-4 – Κατάλογος αποσυρθέντων ΠΕΣ**, όπου καταγράφονται η ημερομηνία απόσυρσης, ο τρόπος καταστροφής και ο τρόπος διάθεσης, καθώς και στοιχεία για τη διαγραφή των δεδομένων του ΠΕΣ και του εργαζομένου που την υλοποίησε.

8. Πολιτική Διαχείρισης Περιστατικών Ασφαλείας

77. Η εταιρεία εφαρμόζει ανελλιπώς και χωρίς εξαιρέσεις διαδικασία Διαχείρισης Περιστατικών Ασφαλείας. Προκειμένου να καταγράφεται συστηματικά κάθε περιστατικό ή παρ' ολίγον περιστατικό ασφάλειας πληροφοριών, να διερευνώνται τα αίτιά του, να γίνεται αποτελεσματική αντιμετώπισή του και έγκαιρη ενημέρωση της ΑΔΑΕ και άλλων αρμόδιων αρχών.
78. Όποτε υποπέσει στην αντίληψη εργαζομένου ή συνεργάτη της εταιρείας οποιαδήποτε συμπεριφορά, καταγραφή ή ενέργεια, η οποία δεν εντάσσεται στην συνήθη λειτουργία των συστημάτων ή δεν αντιστοιχεί στα εγκεκριμένα αρχεία ρυθμίσεων ενημερώνεται τηλεφωνικά και με e-mail ο Υπεύθυνος Ασφαλείας της εταιρείας για το χειρισμό του περιστατικού. Στην κατηγορία αυτή εντάσσεται κρίσιμα σφάλματα που καταγράφονται στα συστήματα και λογισμικά των ΠΕΣ της εταιρείας.
79. Ο Υπεύθυνος Ασφάλειας καταγραφεί στο αρχείο **Ε8-1 – Καταγραφή Περιστατικού Ασφαλείας** τα ακόλουθα στοιχεία:
    - ☞ Ημερομηνία και ώρα που εκδηλώθηκε το περιστατικό και περιγραφή αυτού
    - ☞ Ημερομηνία και ώρα που έγινε αντιληπτό το περιστατικό,
    - ☞ το σύστημα ή τα συστήματα που εκδηλώθηκε,
    - ☞ εκτιμούμενη αιτία,
    - ☞ συνέπειες που έχει επιφέρει το περιστατικό (πχ πόσοι χρήστες ή πόσα δεδομένα επηρεάστηκαν),
    - ☞ ποια στοιχεία έχουν συλλεχτεί για την διερεύνηση (πχ αρχεία καταγραφής),
    - ☞ αν είναι επαναλαμβανόμενο ή όχι
    - ☞ χρόνος επίλυσης,
    - ☞ ποια διορθωτικά μέτρα θα εφαρμοστούν και πότε,
    - ☞ ενημέρωση αρμοδίων αρχών
    - ☞ ενημέρωση θιγομένων συνδρομητών και συστάσεις προς αυτούς για πιθανό μετριασμό του αρνητικού αντίκτυπου.
80. Κάθε αναφορά συμβάντος είναι χρονολογημένη και καταγράφει ακριβώς τι συνέβη, ποιος το διαπίστωσε και αν υπήρχαν άλλοι μάρτυρες. Επίσης βεβαιώνεται η κανονική κατάσταση λειτουργίας προ του συμβάντος, στο βαθμό που αυτό είναι δυνατό.
81. Ο Υπεύθυνος Ασφάλειας προβαίνει άμεσα στη ενημέρωση της Α.Δ.Α.Ε. με την υποβολή του εγγράφου **Ε8-2 Έκθεση άμεσης αναφοράς περιστατικού ασφαλείας**. Το έγγραφο περιέχει όσα από τα ανωτέρω στοιχεία είναι διαθέσιμα κατά την στιγμή της υποβολής.

82. Μετά την ολοκλήρωση της αντιμετώπισης του περιστατικού υποβάλλεται το αρχείο **Ε8-3 Έκθεση τελικής αναφοράς περιστατικού ασφαλείας**, εμπλουτισμένη με όσα επιπλέον στοιχεία έχουν προκύψει.
83. Σε περίπτωση που οποιοσδήποτε χρήστης των υπηρεσιών της εταιρείας διαπιστώσει συμβάν το οποίο θίγει το απόρρητο των επικοινωνιών του, έχει τη δυνατότητα να επικοινωνήσει άμεσα με το τηλεφωνικό κέντρο της εταιρείας, το οποίο θα τον δρομολογήσει απευθείας στον Υπεύθυνο Ασφαλείας καθώς και να στείλει σχετικό ηλεκτρονικό μήνυμα προς την εταιρεία.
84. Τουλάχιστον μια φορά ετησίως ο Υπεύθυνος Ασφάλειας προγραμματίζει δοκιμαστική/ πλασματική αναφορά περιστατικού ασφαλείας, προκειμένου να διαπιστωθεί η ετοιμότητα της εταιρείας στη διερεύνηση και καταγραφή αυτής.

9. Πολιτική Ασφάλειας Δικτύου

85. Το δίκτυο της εταιρίας προστατεύεται τόσο με λογικά μέσα ελέγχου (δημιουργία ζωνών, ιδεατών δικτύων ή/ και λιστών ελέγχου πρόσβασης) όσο και με την υποστήριξη εξειδικευμένου λογισμικού (endpoint protection). Η λίστα με τους παραπάνω μηχανισμούς και τις συσκευές που συμμετέχουν στην προστασία του δικτύου, καθώς και περιγραφή τους, αποτυπώνονται στο αρχείο **E9-1 Υποδομή ασφάλειας δικτύου**.
86. Η εγκατάσταση τέτοιων συσκευών θα πρέπει να είναι σύμφωνη με το άρθρο 7 της παρούσης πολιτικής ασφαλείας. Η λειτουργία τους είναι συνεχής εκτός από τις περιόδους προγραμματισμένης συντήρησης ή σημαντικής αναβάθμισης.
87. Σε περίπτωση που συσκευή ή λογισμικό ή μηχανισμός εντοπίσει κάποιο σοβαρά ασυνήθιστο γεγονός ενεργοποιεί προειδοποιητικό συναγερμό/ ενημέρωση προς τον Υπεύθυνο Ασφαλείας για περαιτέρω διερεύνηση. Αν απαιτηθεί, ο Υπεύθυνος Ασφαλείας εκκινεί τη διαδικασία Διαχείρισης περιστατικών ασφαλείας.
88. Το Τεχνικό Τμήμα διατηρεί στο αρχείο **E9-2 – Αρχιτεκτονική δικτύου** το λογικό διάγραμμα που περιγράφει την αρχιτεκτονική του δικτύου, το λογικό διαχωρισμό σε ιδεατά ή μη υποδίκτυα, την θέση των διακομιστών, και των λοιπών στοιχείων (δρομολογητές, firewalls, κλπ.) του δικτύου. Τα ανωτέρω ενημερώνονται ώστε να αντικατοπτρίζουν κάθε αλλαγή στη δομή του δικτύου, και τηρείται ιστορικό εκδόσεων.
89. Σε περίπτωση των υπηρεσιών που προσφέρονται στο γενικό κοινό και όχι μόνο σε εργαζόμενους και συνεργάτες (π.χ. ιστοσελίδα εταιρείας) ή χρήστες των υπηρεσιών της εταιρείας, οι διακομιστές που εξυπηρετούν τις εν λόγω υπηρεσίες διαθέτουν αυτόνομο σύστημα Firewall (IPTables) καθώς και λειτουργικότητα Intrusion Detection/ Prevention με χρήση του Fail2Ban, το οποίο διακόπτει την πρόσβαση σε διευθύνσεις IP, οι οποίες παρουσιάζουν ύποπτη συμπεριφορά (π.χ. πολλαπλές αποτυχίες ταυτοποίησης, αποστολή κακόβουλων εντολών) κατά την επικοινωνία τους με τα ΠΕΣ της εταιρείας.
90. Τα ΠΕΣ που χρησιμοποιούνται για την τέλεση των κυρίων δραστηριοτήτων ηλεκτρονικών επικοινωνιών ή αποθήκευση δεδομένων από ηλεκτρονικές επικοινωνίες έχουν εγκατασταθεί σε δική τους ζώνη, με αυστηρούς κανόνες ελέγχου πρόσβασης. Τα ΠΕΣ που χρησιμοποιούνται από το προσωπικό της εταιρείας μόνον, για την εκτέλεση επιχειρησιακών ή διαχειριστικών διαδικασιών έχουν εγκατασταθεί σε εσωτερική, έμπιστη ζώνη.
91. Για τα ΠΕΣ που δεν ανήκουν ή δεν τοποθετούνται σε (εσωτερική, έμπιστη) ζώνη και διαθέτουν πάνω από ένα πρωτόκολλο/ μέθοδο για την πρόσβαση σε αυτά επιλέγεται και ενεργοποιείται η

πιο ασφαλής μέθοδος. Η εταιρεία διατηρεί κατάλογο ανά ΠΕΣ με τα εφαρμοζόμενα μέτρα ελέγχου και προστασίας, στο αρχείο **Ε9-3 – Μέτρα ασφαλείας ανά ΠΕΣ**.

92. Όλα τα συνδεδεμένα στο δίκτυο της εταιρείας μηχανήματα διαθέτουν μοναδικό αναγνωριστικό όνομα. Στα ΠΕΣ έχουν ενεργοποιηθεί οι ελάχιστες απαραίτητες δικτυακές θύρες και έχουν απενεργοποιηθεί όλες οι διαγνωστικές και ρυθμιστικές θύρες, όταν δεν απαιτείται παραμετροποίηση του εξοπλισμού
93. Η εταιρεία διατηρεί και καταγράφει σε αρχεία (logs) όλες τις συνδέσεις των χρηστών. Τα αρχεία καταγραφής υφίστανται περιοδικό έλεγχο από τον Υπεύθυνο Ασφάλειας. Όλα τα συστήματα της εταιρείας συγχρονίζουν την ώρα του συστήματος από εξωτερική αξιόπιστη πηγή (NTP Server).

10. Πολιτική Ελέγχου της Εφαρμογής της Πολιτικής Ασφαλείας

94. Η εταιρεία διενεργεί σε ετήσια βάση επιθεώρηση ελέγχου της Πολιτικής Ασφαλείας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών σε όλο το εύρων των ΠΕΣ και των διαδικασιών της. Στην επιθεώρηση:

- ελέγχονται τα τηρούμενα αρχεία και τα μέσα διαχείρισης και αποθήκευσης πληροφοριών και δεδομένων (φάκελοι, software, hardware, κλπ)
- μέσω συνεντεύξεων με το προσωπικό και τους συνεργάτες αξιολογείται η κατανόηση των διαδικασιών και πολιτικών
- επιθεωρούνται οι ρυθμίσεις και τα αρχεία καταγραφής των ΠΕΣ και αντιπαραβάλλονται με τις αντίστοιχες εγγραφών των τηρούμενων αρχείων
- καταγράφονται τα ευρήματα σε σχετικό αρχείο και προβαίνει σε αξιολόγησή τους,
- ενεργοποιείται η διαδικασία Διαχείρισης Περιστατικών Ασφαλείας, όπου απαιτείται.

95. Για κάθε έλεγχο συντάσσεται σχετικό αρχείο **Ε10-1 Προγραμματισμός επιθεωρήσεων**, όπου πριν τη διεξαγωγή του ελέγχου, καταγράφονται:

- το πρόσωπο που θα διεξάγει τον έλεγχο,
- το χρονοδιάγραμμα διεξαγωγής του ελέγχου,
- τι θα ελεγχθεί σχετικά με τη διασφάλιση του απορρήτου και την ανεύρεση τεχνικών δυσλειτουργιών (ΠΕΣ, διαδικασίες, μέτρα ελέγχου,
- ποια δεδομένα/ αρχεία θα συλλεχθούν.

96. Ο έλεγχος πραγματοποιείται από:

- εργαζόμενο της εταιρίας με τις κατάλληλες τεχνικές γνώσεις και αρμοδιότητες, εξαιρουμένων του Υπευθύνου Ασφαλείας, με την προϋπόθεση ότι δεν ανήκει στο Τμήμα της εταιρείας που ελέγχεται και δεν έχει συμμετάσχει στην ανάπτυξη εφαρμογών ή συστημάτων εντός του αντικειμένου ελέγχου.
- κατάλληλο εξωτερικό φορέα, υπό την προϋπόθεση να αναφέρεται στη σύμβαση όρος ως προς την διαφύλαξη του απορρήτου των επικοινωνιών και παρίσταται εξουσιοδοτημένος εκπρόσωπος της εταιρίας καθ' όλη την διάρκεια του ελέγχου.

97. Οι αρμοδιότητες του ελεγκτή, καθώς και η διαδικασία και μεθοδολογία ελέγχου παρουσιάζονται αναλυτικά στη διαδικασία Δ03 - Εσωτερικές επιθεωρήσεις. Η διαδικασία καθορίζει τα στάδια προετοιμασίας, διεξαγωγής, αποτελεσμάτων και διορθωτικών ενεργειών, σύμφωνα με την παρούσα, καθώς και τα σχετικά αρχεία.

98. Για την υλοποίηση του ελέγχου η απόδοση δικαιωμάτων πρόσβασης σε μέλος της ομάδας ελέγχου, είτε πρόκειται περί λογικής πρόσβασης σε συστήματα ή λογισμικά είτε πρόκειται περί φυσικής πρόσβασης, ενεργοποιείται για περιορισμένο χρονικό διάστημα, και αφού ληφθούν

υπόψη οι πολιτικές ασφαλείας της εταιρείας. Οι προσβάσεις απενεργοποιούνται μετά το πέρας του ελέγχου με ευθύνη του Υπευθύνου Ασφαλείας.

99. Τα αποτελέσματα του ελέγχου αποτυπώνονται στο αρχείο **Ε10-2 Αναφορά επιθεώρησης**, η οποία διατηρείται από τον Υπεύθυνο Ασφάλειας ακόμα και στην περίπτωση που δεν υπάρχουν ευρήματα από τον έλεγχο.

100. Για κάθε εύρημα του ελέγχου ο Υπεύθυνος Ασφαλείας καταγράφει:

- την απαιτούμενη διόρθωση,
- τη διορθωτική ενέργεια προκειμένου να αντιμετωπιστεί η πρωταρχική αιτία,
- τον υπεύθυνο υλοποίησης και
- την προθεσμία ολοκλήρωσης

101. Ο Υπεύθυνος Ασφαλείας:

- ελέγχει την αποτελεσματικότητα των απαιτούμενων διορθωτικών ενεργειών, όταν αυτές υλοποιηθούν.
- ενημερώνει άμεσα τη Διοίκηση της εταιρείας συντάσσοντας σχετική αναφορά, στην οποία περιλαμβάνονται:
  - ☞ τα αποτελέσματα της επιθεώρησης
  - ☞ ο βαθμός υλοποίησης των διορθωτικών και προληπτικών ενεργειών
  - ☞ η γενικότερη εικόνα του επιπέδου εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

11. Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού

102. Η εταιρεία εφαρμόζει κάθε τεχνικά εφικτό μέτρο για την αποφυγή εγκατάστασης και λειτουργίας κακόβουλου λογισμικού. Συγκεκριμένα:

- ☞ Όλοι οι υπολογιστές της εταιρείας είναι εφοδιασμένοι με λειτουργικά συστήματα Windows και Linux, τα οποία είναι ενημερωμένα με τις τρέχουσες ενημερώσεις ασφαλείας.
- ☞ Στους προσωπικούς υπολογιστές έχει ενεργοποιηθεί το Firewall του λειτουργικού συστήματος.
- ☞ Οι χρήστες δεν επιτρέπεται να εγκαθιστούν λογισμικό στους υπολογιστές τους.
- ☞ Το Τεχνικό Τμήμα παρακολουθεί ότι τα antivirus πραγματοποιούν καθημερινά updates, είναι σε λειτουργία και δεν έχουν ανιχνεύσει κακόβουλο λογισμικό.
- ☞ Το Τεχνικό Τμήμα παρακολουθεί για κενά ασφαλείας και προβαίνει σε περιοδικές και έκτακτες ενημερώσεις ασφαλείας όλων των συστημάτων.

103. Όπου δεν είναι τεχνική εφικτή η εγκατάσταση antivirus, πραγματοποιείται απομακρυσμένη σάρωση από το Τεχνικό Τμήμα.

104. Όλοι οι εργαζόμενοι ενημερώνονται περιοδικά από τον Υπεύθυνο Ασφαλείας για τους τρόπους αποφυγής ιών και κακόβουλων λογισμικών, ειδικά σε σχέση με downloads από το Internet και άνοιγμα επισυναπτόμενων στα e-mails τους.

105. Σε όλα τα ΠΕΣ που διαχειρίζονται δεδομένα επικοινωνιών δικαίωμα εγκατάστασης εφαρμογών έχει μόνον το Τεχνικό Τμήμα της εταιρείας. Χρησιμοποιούνται πάντοτε τα αυθεντικά CD εγκατάστασης των κατασκευαστών του λειτουργικού συστήματος και των εφαρμογών.

106. Ο Υπεύθυνος Ασφαλείας χρησιμοποιεί περιοδικά εξειδικευμένα λογισμικά (π.χ. Nessus) για τον εντοπισμό ευπαθειών και αδυναμιών ασφαλείας.

107. Σε περίπτωση ανίχνευσης κακόβουλου λογισμικού ενημερώνεται άμεσα ο Υπεύθυνος Ασφαλείας για τον περιορισμό και την απομόνωση της προσβολής. Το ΠΕΣ αποκόπτεται άμεσα από το υπόλοιπο δίκτυο και εκκινείται η διαδικασία Διαχείρισης Περιστατικών Ασφαλείας για τη διερεύνηση της προσβολής, των αιτίων της, των συνεπειών και του ενδεδειγμένου τρόπου αντιμετώπισης αυτής.

108. Εφόσον η προσβολή έχει σοβαρό χαρακτήρα, αν ανιχνευτεί μη εξουσιοδοτημένη από τον προμηθευτή ή την εταιρεία λογισμικό και σε κάθε περίπτωση, κατά την οποία υπάρχει υποψία διαρροής δεδομένων επικοινωνιών ενημερώνεται σχετικά η Α.Δ.Α.Ε.

109. Η διαδικασία αντιμετώπισης κακόβουλου λογισμικού αναλύεται στο έγγραφο Δ10 Διαχείριση Περιστατικών Ασφαλείας. Τα μέτρα και τα αποτελέσματα ελέγχου για κακόβουλο λογισμικό καταγράφονται από τον Υπεύθυνο Ασφαλείας στο αρχείο **Ε11-1 Έλεγχος κακόβουλου λογισμικού.**

12. Πολιτική Χρήσης Κρυπτογραφίας

110. Η εταιρεία εφαρμόζει συστήματα κρυπτογράφησης προκειμένου να διασφαλίσει το απόρρητο των προσωπικών δεδομένων και των δεδομένων επικοινωνίας των χρηστών των υπηρεσιών της, τόσο κατά την αποθήκευσή όσο και κατά τη μεταφορά τους.

111. Με στόχο τη βέλτιστη στόχευση των εργαλείων και μεθόδων κρυπτογράφησης, η χρήση αυτών γίνεται σύμφωνα με τα αποτελέσματα της εκτίμησης κινδύνου Ασφάλειας Πληροφοριών, για τα συστήματα (ΠΕΣ) και δεδομένα τα οποία διατρέχουν υψηλό κίνδυνο διαρροής ή αλλοίωσης δεδομένων.

112. Η εταιρεία χρησιμοποιεί κρυπτογράφηση με χρήση υποδομών PKI, βασισμένες σε πιστοποιητικά SSL της εταιρείας Comodo για την πρόσβαση στις διαδικτυακές (Web) εφαρμογές της. Τα συνθηματικά των πιστοποιητικών τηρούνται από τον Υπεύθυνο Ασφαλείας της εταιρείας. Το μήκος του κλειδιού είναι 256bit, σύμφωνα με τις διεθνώς αποδεκτές πρακτικές δημόσια κρυπτογραφίας. Η εταιρεία Comodo είναι διεθνώς αναγνωρισμένη και αποδεδειγμένα αξιόπιστη, καθώς χρησιμοποιείται από οργανισμούς σε παγκόσμιο επίπεδο.

113. Τα ιδιωτικά κλειδιά των ανωτέρω πιστοποιητικών φυλάσσονται ασφαλώς σε θέση εκτός των δημοσίων εξυπηρετητών, σε ΠΕΣ εντός του ασφαλούς δικτύου, για την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Όλα τα ιδιωτικά κλειδιά ανήκουν στον Υπεύθυνο Ασφάλειας, ο οποίος μεριμνά για την ορθή χρήση των δημόσιων και ιδιωτικών κλειδιών. Τα σχετικά πιστοποιητικά τηρούνται στο αρχείο **Ε12-1 Πιστοποιητικά/ κρυπτογραφία**.

114. Η εταιρεία παράγει κλειδιά κρυπτογράφησης τα οποία χρησιμοποιούνται για τη δημιουργία ασφαλών καναλιών σύνδεσης με τα ΠΕΣ τα οποία διαχερίζεται. Ακολουθούνται οι ακόλουθες ενέργειες για την ασφαλή διαχείριση των κλειδιών κρυπτογράφησης:

- Σε περίπτωση διανομής κρυπτογραφικών κλειδιών μέσω USB, διαγράφονται από το φορητό μέσο αποθήκευσης αμέσως μετά την εγκατάστασή τους.
- Τα αρχεία των κρυπτογραφικών κλειδιών κρυπτογραφούνται όταν διακινούνται μέσω email
- Σε περίπτωση αποχώρησης υπαλλήλων, αναιρούνται άμεσα τα κρυπτογραφικά κλειδιά που τους έχουν παραδοθεί κατά το διάστημα εργασίας τους

- Όταν υπάρχει ανάγκη τήρησης αντιγράφων αρχείων κρυπτογραφικών κλειδιών, αυτά τηρούνται αποθηκευμένα σε κρυπτογραφημένη μορφή και σε χώρο προσβάσιμο μόνο από εξουσιοδοτημένο προσωπικό.
- Περιπτώσεις απώλειας ή διαρροής κρυπτογραφικών κλειδιών αναφέρονται άμεσα στον Υπεύθυνο Ασφάλειας Πληροφοριών.

115. Η εταιρεία τηρεί μόνο τα δεδομένα για τη φύλαξη των οποίων έχει συναινέσει ο ιδιοκτήτης τους/ χρήστης, με βάση τους όρους τους οποίους έχει αποδεχτεί κατά την αίτηση παροχής υπηρεσίας ή τα οποία απαιτούνται για την παροχή της υπηρεσίας, σε συμφωνία με την ισχύουσα εθνική και κοινοτική νομοθεσία. Ο χρόνος τήρησης των δεδομένων είναι ο ελάχιστος αναγκαίος, όπως προσδιορίζεται από τις συμβατικές υποχρεώσεις της εταιρείας ή την ισχύουσα νομοθεσία καθώς και τις απαιτήσεις ελέγχου της Α.Δ.Α.Ε.

13. Περιγραφή Θέσης Εργασίας Υπευθύνου Ασφάλειας Πληροφοριών

116. Ο Υπεύθυνος Ασφάλειας Πληροφοριών και Υπεύθυνος Διασφάλισης του Απορρήτου των Επικοινωνιών αναπτύσσει μεθόδους, εκπονεί διαδικασίες και εφαρμόζει συστήματα προκειμένου να διασφαλίζεται ότι :

- ☞ το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών της Εταιρίας καθιερώνεται, εφαρμόζεται και διατηρείται σύμφωνα με το πρότυπο ISO 27001:2013 και την Πολιτική Ασφαλείας για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών.
- ☞ ενημερώνεται έγκαιρα και τεκμηριωμένα η Διοίκηση της Εταιρίας για την επίδοση του συστήματος αυτού και των αναγκών της βελτίωσής του και
- ☞ διατηρείται το προσωπικό και τα στελέχη της Εταιρίας σε συνεχώς αυξανόμενη ετοιμότητα για την κατανόηση των απαιτήσεων και προσδοκιών των Ενδιαφερόμενων Μερών.

117. Έχει την ευθύνη για:

- ☞ τη διαχείριση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με τις καθιερωμένες Διαδικασίες, Οδηγίες και Πολιτικές Ασφάλειας
- ☞ την αναφορά στη Διοίκηση της εταιρείας για θέματα και συμβάντα Ασφάλειας.
- ☞ τη διερεύνηση και την αντιμετώπιση Περιστατικών Ασφάλειας Πληροφορικών και την ενημέρωση της Διοίκησης της εταιρείας
- ☞ την παρακολούθηση της Νομοθεσίας που σχετίζεται με την Ασφάλεια των Πληροφοριών και την ενσωμάτωση των απαιτήσεων στο Σύστημα Ασφάλειας Πληροφοριών
- ☞ την ενημέρωση του προσωπικού της Εταιρίας σε θέματα ασφάλειας πληροφοριών καθώς και ασφαλούς διαχείρισης των πληροφοριών.
- ☞ την παρακολούθηση του επιπέδου ασφάλειας πληροφοριών της Εταιρίας, τον έλεγχο υλοποίησης των μέτρων Ασφαλείας και την λήψη των αναγκαίων διορθωτικών ή προληπτικών μέτρων.
- ☞ την παρακολούθηση των τεχνολογικών εξελίξεων και των νέων τάσεων σε θέματα ασφάλειας ώστε να ενσωματώνει τις νέες πρακτικές στο Σύστημα Ασφάλειας Πληροφοριών.
- ☞ την τήρηση των αρχών Ασφάλειας Πληροφοριών τόσο κατά την εσωτερική ανάπτυξη εφαρμογών, όσο και κατά την προμήθειά τους από τρίτους
- ☞ την τήρηση των αρχείων που αφορούν στην πολιτική ασφάλειας και στην καταγραφή σχετικών συμβάντων
- ☞ τον έλεγχο, την μέτρηση και την ανάλυση της επίδοσης της Εταιρίας στον τομέα της Ασφάλειας Πληροφοριών.

Ι.Μ. Βαμβακάρης