ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ **Αρ. Φύλλου 2715**

17 Νοεμβρίου 2011

ΑΠΟΦΑΣΕΙΣ

Αριθμ. αποφ. 165/2011

Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών.

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ
ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)
(Συνεδρίαση της 09.11.2011)

Έχοντας υπόψη:

1. Τις διατάξεις:

α. του άρθρου 1 παρ. 1 και του άρθρου 6 παρ. 1 του Ν. 3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» (ΦΕΚ Α΄ 47/2003),

β. του άρθρου 5 του Ν. 3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (ΦΕΚ Α΄ 136/2008),

γ. της υπ' αριθμ. 629α/2004 απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών» (ΦΕΚ Β΄ 87/2005),

δ. της υπ' αριθμ. 630α/2004 απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών» (ΦΕΚ Β΄ 87/2005),

ε. της υπ' αριθμ. 631α/2004 απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Τηλεπικοινωνιακών Υπηρεσιών μέσω Ασύρματων Δικτύων» (ΦΕΚ Β΄ 87/2005),

στ. της υπ' αριθμ. 632α/2005 απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές» (ΦΕΚ Β΄ 88/2005),

ζ. της υπ' αριθμ. 633α/2005 απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση Απορρήτου Διαδικτυακών Υποδομών» (ΦΕΚ Β΄ 88/2005),

η. της υπ' αριθμ. 634α/2005 απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου» (ΦΕΚ Β΄ 88/2005),

θ. της υπ' αριθμ. 2654/27.11.2008 απόφασης της Α.Δ.Α.Ε. με τίτλο «Σύσταση ομάδας εργασίας για την αναθεώρηση των Κανονισμών της Α.Δ.Α.Ε. για τη διασφάλιση του απορρήτου των επικοινωνιών υπ' αριθμ. 629α, 630α, 631α αποφάσεων» (ΦΕΚ Τεύχος Υπαλλήλων Ειδικών Θέσεων και Οργάνων Διοίκησης Φορέων του Δημοσίου και Ευρύτερου Δημόσιου Τομέα 510/10.12.2008),

ι. της υπ' αριθμ. 2660/27.11.2008 απόφασης της Α.Δ.Α.Ε. με τίτλο «Σύσταση ομάδας εργασίας για την αναθεώρηση των Κανονισμών της Α.Δ.Α.Ε. για τη διασφάλιση του απορρήτου των επικοινωνιών υπ' αριθμ. 632α, 633α, 634α αποφάσεων» (ΦΕΚ Τεύχος Υπαλλήλων Ειδικών Θέσεων και Οργάνων Διοίκησης Φορέων του Δημοσίου και Ευρύτερου Δημόσιου Τομέα 510/10.12.2008).

2. Τη διαπίστωση της ανάγκης αναθεώρησης των ως άνω Αποφάσεων της Α.Δ.Α.Ε. προς την κατεύθυνση της θέσπισης ενιαίου Κανονισμού για τη διασφάλιση του Απορρήτου των επικοινωνιών.

3. Τα πρακτικά των από 14.9.2011, 21.9.2011, 28.9.2011, 26.10.2011 και 09.11.2011 συνεδριάσεων της Ολομέλειας της Α.Δ.Α.Ε.

4. Ότι εκ της παρούσας αποφάσεως δεν προκύπτει δαπάνη για το τρέχον και τα επόμενα οικονομικά έτη εις βάρος του Κρατικού Προϋπολογισμού, αποφασίζει:

Την έκδοση του παρόντος Κανονισμού, οι διατάξεις του οποίου έχουν ως ακολούθως:

ΑΡΘΡΟ 1 - Πεδίο Εφαρμογής

1.1. Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλα τα πρόσωπα που ασχολούνται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών. Τα πρόσωπα αυτά υποχρεούνται να διαθέτουν και να εφαρμόζουν Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, της οποίας το περιεχόμενο είναι σύμφωνο με τις διατάξεις του παρόντος Κανονισμού.

1.2. Τα πρόσωπα που παρέχουν δίκτυα ή/και υπηρεσίες ηλεκτρονικών επικοινωνιών υπό καθεστώς Γενικής Άδειας, όπως αυτό καθορίζεται από την εκάστοτε ισχύουσα νομοθεσία, υποχρεούνται να υποβάλλουν στην Α.Δ.Α.Ε. προς έγκριση την προβλεπόμενη στην προηγούμενη παράγραφο Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, καθώς και κάθε αναθεώρηση αυτής, όποτε αυτή λάβει χώρα. Εξαιρούνται της υποχρέωσης υποβολής προς έγκριση στην Α.Δ.Α.Ε. της εφαρμοζόμενης Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών τα πρόσωπα που παρέχουν τις ακόλουθες κατηγορίες δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, όπως προβλέπονται στον Κανονισμό Γενικών Αδειών της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων, όπως ισχύει:

α) Α0102: Σταθερά δίκτυα τηλεμετρίας, τηλεματικής, ραδιοεντοπισμού

β) Α0108: Δίκτυο μετάδοσης σημάτων επίγειας ψηφιακής ευρυεκπομπής, με χρήση συχνοτήτων για την εκπομπή ραδιοτηλεοπτικού σήματος

γ) A0109: Δίκτυο μετάδοσης σημάτων επίγειας αναλογικής ευρυεκπομπής, με χρήση συχνοτήτων για την εκπομπή ραδιοτηλεοπτικού σήματος

δ) A0204: Ειδικό ραδιοδίκτυο (εξαιρουμένων επιβατηγών αυτοκινήτων δημόσιας χρήσης με μετρητή (ταξί))

ε) A0205: Ειδικό ραδιοδίκτυο για επιβατηγά αυτοκίνητα δημόσιας χρήσης με μετρητή (ταξί)

στ) A0206: Κινητά δίκτυα τηλεμετρίας, τηλεματικής, ραδιοεντοπισμού

ζ) A0402: Δίκτυο μεταφερόμενων επίγειων δορυφορικών σταθμών (SNG)

η) A0403: Δίκτυο μεταφερόμενων επίγειων σταθμών (ENG)

θ) B0204: Παροχή υπηρεσιών τηλεματικής, τηλεμετρίας, ραδιοεντοπισμού.

ι) B0205: Υπηρεσία εντοπισμού κινδυνεύοντος πλοίου

ια) B0301: Μονοκατευθυντική μετάδοση ειδήσεων (ήχος, σχέδιο και/η κείμενο)

ιβ) B08: Τεχνική παροχή ευρυεκπομπής (broadcasting) (B0801 έως και B0805).

ΑΡΘΡΟ 2 - Ορισμοί

Για τους σκοπούς του παρόντος Κανονισμού νοούνται ως:

«Δεδομένα Επικοινωνίας»: το περιεχόμενο και τα συναφή δεδομένα κίνησης και θέσης για κάθε επικοινωνία.

«Περιστατικό Ασφάλειας»: κάθε συμβάν που δύναται να σχετίζεται με τη διασφάλιση του απορρήτου των επικοινωνιών ή κάθε ιδιαίτερος κίνδυνος παραβίασης του απορρήτου των επικοινωνιών, καθώς και κάθε περίπτωση μη εφαρμογής ή ιδιαίτερου κινδύνου μη εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

«Πληροφοριακά και Επικοινωνιακά Συστήματα (ΠΕΣ)»: συστήματα ή τερματικά του υπόχρεου προσώπου με τα οποία πραγματοποιούνται εργασίες σε δεδομένα επικοινωνίας, όπως η συλλογή, η καταχώρηση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή δεδομένων επικοινωνίας. Αναφέρονται κατ' ελάχιστον τα μέσα μετάδοσης και διασύνδεσης, οι μεταγωγείς, οι δρομολογητές, τα συστήματα διαχείρισης και εποπτείας αυτών, οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου, τα αναχώματα ασφάλειας, τα συστήματα ανίχνευσης/αποτροπής εισβολών, τα συστήματα ανίχνευσης κακόβουλου λογισμικού, τα συστήματα καταγραφής, τα συστήματα χρέωσης συνδρομητών, τα συστήματα πωλήσεων και εξυπηρέτησης πελατών, τα συστήματα πρόληψης τηλεπικοινωνιακής απάτης, οι βάσεις δεδομένων που περιέχουν δεδομένα επικοινωνίας και οι εφαρμογές πρόσβασης σε δεδομένα επικοινωνίας.

«Υπόχρεα Πρόσωπα»: τα πρόσωπα που ασχολούνται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Κατά τα λοιπά ισχύουν οι ορισμοί που περιλαμβάνονται στο άρθρο 2 του Ν.3 471/2006 («Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/1999», ΦΕΚ Α΄ 133/28.06.2006), όπως ισχύει.

ΑΡΘΡΟ 3 - Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

3.1. Σκοπός - Εύρος Πολιτικής

3.1.1. Η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, έχει ως στόχο την προστασία των δεδομένων επικοινωνίας και των ΠΕΣ από πιθανούς κινδύνους, ούτως ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών.

3.1.2. Η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών αφορά τους χρήστες, συνδρομητές, εργαζόμενους και συνεργάτες του υπόχρεου προσώπου.

3.2. Γενικές Απαιτήσεις

3.2.1. Η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, έχει αρθρωτή δομή και αποτελείται από επιμέρους πολιτικές, οι οποίες ορίζουν τις απαιτήσεις ασφάλειας που πρέπει να ικανοποιούνται για κάθε επιμέρους κατηγορία ειδικών θεμάτων. Η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών περιλαμβάνει κατ' ελάχιστον τις επιμέρους πολιτικές που αναφέρονται αναλυτικά στα άρθρα 3 έως και 13 του παρόντος Κανονισμού.

3.2.2. Σε περίπτωση που η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών είναι ενταγμένη και συμπεριλαμβάνεται σε ευρύτερη πολιτική ασφάλειας πληροφοριών και επικοινωνιών του υπόχρεου προσώπου, αυτό οφείλει να διαθέτει αρχείο με αναλυτική αντιστοίχιση της δομής της ευρύτερης πολιτικής ασφάλειας πληροφοριών και επικοινωνιών με τις απαιτήσεις του παρόντος Κανονισμού. Τα υπόχρεα πρόσωπα που αναφέρονται στο άρθρο 1 παρ.2 του παρόντος Κανονισμού οφείλουν να υποβάλλουν στην Α.Δ.Α.Ε. το εν λόγω αρχείο με την ευρύτερη πολιτική ασφάλειας πληροφοριών και επικοινωνιών.

3.2.3. 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. Στην περίπτωση των υπόχρεων προσώπων του άρθρου 1 παρ.2 του παρόντος Κανονισμού, προβλέπεται και εφαρμόζεται εσωτερική διαδικασία καταγραφής και τεκμηρίωσης των αδυναμιών της παρούσας παραγράφου.

3.2.4. 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.

3.2.5. 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.

3.2.6. Το υπόχρεο πρόσωπο οφείλει να ορίσει συγκεκριμένο εργαζόμενό 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. Τα

υπόχρεα πρόσωπα που αναφέρονται στο άρθρο 1 παρ.2 του παρόντος Κανονισμού οφείλουν να κοινοποιούν στην Α.Δ.Α.Ε. τα στοιχεία επικοινωνίας του εκάστοτε Υπεύθυνου Διασφάλισης του Απορρήτου των Επικοινωνιών.

3.2.7. Η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών ορίζει συγκεκριμένα στάδια, τα οποία χρησιμοποιούνται και εφαρμόζονται για τη διαχείριση της Πολιτικής. Τα στάδια της παρούσας παραγράφου περιλαμβάνουν τον προσδιορισμό και την αποτίμηση των κινδύνων, το σχεδιασμό και την υλοποίηση των μέτρων ασφάλειας και τον έλεγχο εφαρμογής τους.

3.2.8. Με τα άρθρα 3 έως και 13 του παρόντος Κανονισμού ορίζεται υποχρέωση διατήρησης αρχείων για το σκοπό του ελέγχου της Πολιτικής Διασφάλισης του Απορρήτου των Επικοινωνιών. Με την επιφύλαξη των διατάξεων των ν.3471/2006 (ΦΕΚ Α'133), ν.3783/2009 (ΦΕΚ Α'136) και ν.3917/2011 (ΦΕΚ Α'22), όπως ισχύουν, το υπόχρεο πρόσωπο υποχρεούται να διατηρεί τα εν λόγω αρχεία για χρονικό διάστημα δύο (2) ετών, λαμβάνοντας τα κατάλληλα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς τους. Σε περίπτωση που βρίσκεται σε εξέλιξη έλεγχος της Α.Δ.Α.Ε., το υπόχρεο πρόσωπο, υποχρεούται να διατηρεί τα εν λόγω αρχεία, ακόμα και μετά το πέρας των δύο ετών, και να προβαίνει στη διαγραφή τους μόνο κατόπιν σχετικής απόφασης της Α.Δ.Α.Ε.

3.2.9. Αναφορικά με τα αρχεία καταγραφής των άρθρων 6.2.5 και 8.3.3.2 του παρόντος Κανονισμού, το υπόχρεο πρόσωπο υποχρεούται να εξασφαλίζει ότι οι καταγραφές που προβλέπονται στα εν λόγω άρθρα είναι πλήρεις και συνεχείς. Το υπόχρεο πρόσωπο οφείλει 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. Το υπόχρεο πρόσωπο οφείλει να ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με το άρθρο 9 του παρόντος Κανονισμού, σε περίπτωση διακοπής των καταγραφών που προβλέπονται στα ως άνω άρθρα και σε περίπτωση περιστατικού παραβίασης της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας αυτών.

3.3. Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου

3.3.1. Το υπόχρεο πρόσωπο οφείλει να διατηρεί και να εφαρμόζει διαδικασία αποτίμησης πληροφοριακού κινδύνου σχετικά με το απόρρητο της επικοινωνίας βασισμένη σε μεθοδολογία αποτίμησης κινδύνου που λαμβάνει υπόψη διεθνείς πρακτικές. Η αποτίμηση πληροφοριακού κινδύνου πραγματοποιείται κατ' ελάχιστον κάθε δύο (2) έτη και περιλαμβάνει τουλάχιστον τα παρακάτω:

3.3.1.1. Διατήρηση καταλόγου των ΠΕΣ με συνοπτική περιγραφή της λειτουργίας τους.

3.3.1.2. 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.

3.3.1.3. 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.

ΑΡΘΡΟ 4 - Πολιτική Αποδεκτής Χρήσης

4.1. Σκοπός - Εύρος Πολιτικής

Η Πολιτική Αποδεκτής Χρήσης καθορίζει τις υποχρεώσεις του υπόχρεου προσώπου αλλά και τις αρχές, τους κανόνες και τις συνέπειες για τους εργαζόμενους και συνεργάτες του, στους οποίους εκχωρείται το δικαίωμα πρόσβασης σε ΠΕΣ και δεδομένα επικοινωνίας, και αποβλέπει στην αποτροπή καταχρηστικής άσκησης των δικαιωμάτων τους και της τέλεσης πράξεων που παραβιάζουν ή συνιστούν κίνδυνο παραβίασης του απορρήτου των επικοινωνιών των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών.

4.2. Γενικές Απαιτήσεις - Υποχρεώσεις

4.2.1. Οι εργαζόμενοι και συνεργάτες του υπόχρεου προσώπου 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, το υπόχρεο πρόσωπο οφείλει να καταγράφει στην Πολιτική Αποδεκτής Χρήσης τον τρόπο με τον οποίο εξασφαλίζει ότι οι εργαζόμενοι και συνεργάτες του λαμβάνουν γνώση και έχουν αποδεχτεί την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών ως προς την εργασία τους, προ της απόκτησης πρόσβασης σε ΠΕΣ και σε δεδομένα επικοινωνίας.

4.2.2. Το υπόχρεο πρόσωπο οφείλει να ενημερώνει με πρόσφορα μέσα και να εκπαιδεύει τους εργαζόμενους και συνεργάτες του σχετικά με την εφαρμογή της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και τις τροποποιήσεις αυτής.

4.2.3. Οι εργαζόμενοι και συνεργάτες του υπόχρεου προσώπου, οι οποίοι αποκτούν πρόσβαση στα ΠΕΣ και τα δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών δεν επιτρέπεται να αποκαλύπτουν οποιαδήποτε πληροφορία ή στοιχείο υποπίπτει στην αντίληψή τους ή την κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

4.2.4. Οι εργαζόμενοι και συνεργάτες του υπόχρεου προσώπου υποχρεούνται να ενημερώνουν άμεσα το αρμόδιο προσωπικό του σε περίπτωση που υποπέσει στην αντίληψή τους ένα κενό ασφάλειας ή σχετικό περιστατικό που θέτει σε κίνδυνο το απόρρητο των επικοινωνιών των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών.

4.3. Πρόσθετες Απαιτήσεις Αναφορικά με τους Συνεργάτες

4.3.1. Το υπόχρεο πρόσωπο οφείλει να 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.

4.3.2. Το υπόχρεο πρόσωπο οφείλει να συνάπτει με τους συνεργάτες της προηγούμενης παραγράφου, συμβάσεις, των οποίων το ελάχιστο περιεχόμενο περιλαμβάνει:

4.3.2.1. Όρους εμπιστευτικότητας, μη αποκάλυψης και τήρησης του απορρήτου.

4.3.2.2. 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.

4.3.2.3. Αποδοχή εκ μέρους των συνεργατών της υποχρέωσης για τήρηση των μέτρων ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών, που αναφέρονται στην παράγραφο 4.3.2.2 του παρόντος άρθρου.

4.3.3. Το υπόχρεο πρόσωπο οφείλει να ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με το άρθρο 9 του παρόντος Κανονισμού, για κάθε παραβίαση των συμβατικών όρων που αναφέρονται στις παραγράφους 4.3.2.1, 4.3.2.2 και 4.3.2.3 του παρόντος άρθρου.

4.4. Πρόσθετες Απαιτήσεις Αναφορικά με τους Συνδρομητές ή Χρήστες των Παρεχόμενων Δικτύων ή Υπηρεσιών.

Το υπόχρεο πρόσωπο οφείλει να ενημερώνει τους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών τουλάχιστον κατά τη σύναψη της μεταξύ τους σύμβασης αλλά και σε τακτά χρονικά διαστήματα, με κάθε πρόσφορο τρόπο, σχετικά με τα μέτρα που ενδείκνυται να λαμβάνουν για την προστασία του απορρήτου των επικοινωνιών τους, ιδίως σχετικά με κανόνες ορθής χρήσης των παρεχόμενων δικτύων ή υπηρεσιών αλλά και τους τρόπους χρήσης τεχνολογιών και πόρων σχετικών με την ασφάλεια των πληροφοριών που σχετίζονται με τη διασφάλιση του απορρήτου των επικοινωνιών.

4.5. Διαχείριση Αποθηκευτικών Μέσων

Το υπόχρεο πρόσωπο οφείλει να ορίζει στην Πολιτική και να θέτει σε εφαρμογή μέτρα ή/και διαδικασίες σχετικά με τη χρήση, τη διακίνηση και την καταστροφή των αποθηκευτικών μέσων, ηλεκτρονικών ή εντύπων, που περιέχουν δεδομένα επικοινωνίας ή άλλες πληροφορίες που μπορεί να οδηγήσουν σε αποκάλυψη δεδομένων επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών (ενδεικτικά αναφέρονται κωδικοί πρόσβασης και δεδομένα διάρθρωσης των ΠΕΣ), ώστε να αποτρέπεται η αποκάλυψή τους σε μη εξουσιοδοτημένα πρόσωπα.

ΑΡΘΡΟ 5 - Πολιτική Φυσικής Ασφάλειας

5.1. Σκοπός - Εύρος Πολιτικής

Η Πολιτική Φυσικής Ασφάλειας καθορίζει τα απαιτούμενα μέτρα για την αποτροπή της μη εξουσιοδοτημένης φυσικής πρόσβασης στις εγκαταστάσεις του υπόχρεου προσώπου, στις οποίες είναι εγκατεστημένα ΠΕΣ, εξαιρουμένων εκείνων που χρησιμοποιούνται αποκλειστικά για την εξυπηρέτηση του κοινού, τον έλεγχο της πρόσβασης σε αυτές καθώς και την προστασία των ΠΕΣ.

5.2. Γενικές Απαιτήσεις

5.2.1. Το υπόχρεο πρόσωπο οφείλει να λαμβάνει όλα τα απαραίτητα και πρόσφορα μέτρα για τη φυσική προστασία των εγκαταστάσεών του, ώστε να αποτρέπεται κάθε μη εξουσιοδοτημένη πρόσβαση σε αυτές, καθώς και για τον έλεγχο της φυσικής πρόσβασης, ώστε αυτή να επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα.

5.2.2. Το υπόχρεο πρόσωπο οφείλει να συντάξει και να εφαρμόζει διαδικασία φυσικής πρόσβασης, στην οποία περιγράφονται αναλυτικά όλες οι ενέργειες που απαιτούνται για την πρόσβαση των εργαζομένων και των συνεργατών του σε εγκαταστάσεις και σε χώρους εντός των εγκαταστάσεών του, όπου είναι εγκατεστημένα ΠΕΣ.

5.2.3. Για την παροχή εξουσιοδότησης φυσικής πρόσβασης, στους εργαζόμενους ή τους συνεργάτες του υπόχρεου προσώπου σε εγκαταστάσεις και σε χώρους εντός των εγκαταστάσεών του όπου είναι εγκατεστημένα ΠΕΣ, πρέπει να προβλέπεται υποχρεωτικά η προηγούμενη έγκριση από την αρμόδια διοικητική οντότητα ή το αρμόδιο φυσικό πρόσωπο. Το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο με το ιστορικό όλων των φυσικών προσβάσεων που έχουν εγκριθεί, στο οποίο καταγράφονται όλα τα στοιχεία που αφορούν έκαστη έγκριση (ενδεικτικά, χρονικό διάστημα, εγκατάσταση ή χώρο με δικαίωμα πρόσβασης).

5.2.4. Η φυσική πρόσβαση των εξουσιοδοτημένων προσώπων στις εγκαταστάσεις του υπόχρεου προσώπου πρέπει να καταγράφεται (ονοματεπώνυμο, ιδιότητα, ώρα εισόδου και εξόδου) σε σχετικό αρχείο. 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.

5.2.5. Το υπόχρεο πρόσωπο οφείλει να ορίσει ασφαλείς χώρους εντός των εγκαταστάσεών του, στους οποίους εγκαθίστανται τα ΠΕΣ. Οι χώροι αυτοί, πρέπει να προστατεύονται με ισχυρούς μηχανισμούς ασφάλειας (ενδεικτικά, συστήματα άμεσης ανίχνευσης μη εξουσιοδοτημένης πρόσβασης και συστήματα κλειστού κυκλώματος τηλεόρασης) και ελεγχόμενης πρόσβασης (ενδεικτικά, κάρτες ελεγχόμενης εισόδου) τηρουμένης της κείμενης νομοθεσίας. Η φυσική πρόσβαση στους χώρους της παρούσας παραγράφου καταγράφεται σύμφωνα με τις απαιτήσεις της παραγράφου 5.2.4 του παρόντος άρθρου. Στην περίπτωση πρόσβασης συνεργατών του υπόχρεου προσώπου ή άλλων επισκεπτών στους χώρους της παρούσας παραγράφου, αυτοί θα πρέπει να συνοδεύονται από εξουσιοδοτημένο εργαζόμενο σε όλο το διάστημα παραμονής τους. Οι χώροι της παρούσας παραγράφου, καθώς και οι μηχανισμοί ασφάλειας και ελεγχόμενης πρόσβασης, καταγράφονται σε αρχείο.

5.2.6. Το υπόχρεο πρόσωπο οφείλει να λαμβάνει όλα τα απαραίτητα μέτρα φυσικής προστασίας και ελεγχόμενης πρόσβασης για την προστασία των ΠΕΣ, τα οποία βρίσκονται υπό την εποπτεία του και τοποθετούνται εκτός των εγκαταστάσεών του. Οι μηχανισμοί ασφάλειας για τις περιπτώσεις αυτές πρέπει να περιγράφονται σε αρχείο.

ΑΡΘΡΟ 6 - Πολιτική Λογικής Πρόσβασης

6.1. Σκοπός - Εύρος Πολιτικής

6.1.1. Η Πολιτική Λογικής Πρόσβασης καθορίζει τη διαβάθμιση των επιπέδων πρόσβασης και θέτει τις απαιτήσεις για τον έλεγχο πρόσβασης στα ΠΕΣ του υπόχρεου προσώπου.

6.1.2. Η Πολιτική Λογικής Πρόσβασης ισχύει για τους εργαζόμενους και συνεργάτες του υπόχρεου προσώπου, οι οποίοι στο πλαίσιο της εργασίας τους αποκτούν πρόσβαση στα ΠΕΣ και στα σχετικά δεδομένα και τις πληροφορίες.

6.2. Γενικές Απαιτήσεις

6.2.1. Για την απόκτηση πρόσβασης σε ένα ΠΕΣ χρησιμοποιούνται κατάλληλοι μηχανισμοί ελέγχου πρόσβασης και αυθεντικοποίησης των εργαζομένων και συνεργατών του υπόχρεου προσώπου. Κατ' ελάχιστον, ο έλεγχος πρόσβασης και αυθεντικοποίησης επιτυγχάνεται με τη χρήση ενός λογαριασμού πρόσβασης που αποτελείται από ένα ζεύγος ονόματος χρήστη και κωδικού πρόσβασης, ή άλλου μηχανισμού που εξασφαλίζει αντίστοιχο επίπεδο ασφάλειας. Το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης για κάθε ΠΕΣ.

6.2.2. Σε κάθε εργαζόμενο και συνεργάτη του υπόχρεου προσώπου εκχωρείται προσωπικός λογαριασμός πρόσβασης ανά ΠΕΣ, ούτως ώστε να είναι δυνατή η αντιστοίχιση

συγκεκριμένου προσώπου με τις ενέργειες που τελούνται σε κάθε ΠΕΣ. Το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο με την αντιστοίχιση των λογαριασμών πρόσβασης των εργαζόμενων και συνεργατών στους οποίους αυτοί έχουν αποδοθεί, ούτως ώστε να είναι δυνατό να διαπιστώνεται με βεβαιότητα ποιος είναι ο κάτοχος κάθε λογαριασμού πρόσβασης και για ποιο χρονικό διάστημα.

6.2.3. Η δημιουργία κοινών ή/και προκαθορισμένων λογαριασμών πρόσβασης πρέπει να αποφεύγεται. Σε περίπτωση που αυτό δεν είναι εφικτό, θα πρέπει να δικαιολογείται και, σε κάθε περίπτωση, να εξασφαλίζεται η αντιστοίχιση του συγκεκριμένου φυσικού προσώπου που αποκτά πρόσβαση σε ένα ΠΕΣ με τις ενέργειες που τελούνται σε αυτό, με άλλον κατάλληλο μηχανισμό, ο οποίος θα τεκμηριώνεται σε αρχείο που οφείλει να διατηρεί το υπόχρεο πρόσωπο.

6.2.4. Το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο στο οποίο καταγράφονται οι κατηγορίες των χρηστών και τα δικαιώματα πρόσβασης αυτών για κάθε ΠΕΣ.

6.2.5. Το υπόχρεο πρόσωπο οφείλει να τηρεί αρχείο καταγραφής των προσβάσεων των χρηστών των ΠΕΣ σε αυτά, στο οποίο καταγράφονται, κατ' ελάχιστον, το όνομα χρήστη που απέκτησε την πρόσβαση, και η ημερομηνία και ώρα εκκίνησης και τερματισμού της πρόσβασης.

6.2.6. Το υπόχρεο πρόσωπο οφείλει να 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 πρέπει να καταγράφεται και να αιτιολογείται.

6.3. Γενικές Διαδικασίες Πολιτικής Λογικής Πρόσβασης

Το υπόχρεο πρόσωπο οφείλει να διαμορφώσει και να ακολουθεί τις παρακάτω διαδικασίες:

6.3.1. Διαδικασία Διαχείρισης Χρηστών ΠΕΣ

6.3.1.1. Στη Διαδικασία Διαχείρισης Χρηστών ΠΕΣ πρέπει να περιγράφεται με σαφήνεια ο τρόπος προσθήκης νέων χρηστών ΠΕΣ, η διαγραφή χρηστών ΠΕΣ καθώς και η απονομή και μεταβολή των δικαιωμάτων ή επιπέδων πρόσβασης.

6.3.1.2. Για κάθε μία εκ των ενεργειών που αναφέρονται στην παράγραφο 6.3.1.1 του παρόντος πρέπει να προβλέπεται υποχρεωτικά η προηγούμενη έγκριση από αρμόδιο εργαζόμενο του υπόχρεου προσώπου.

6.3.1.3. Στη Διαδικασία Διαχείρισης Χρηστών ΠΕΣ πρέπει να προβλέπεται η υποχρέωση τήρησης αρχείου των αιτήσεων που αφορούν σε κάθε μεταβολή στην κατάσταση πρόσβασης των χρηστών ΠΕΣ.

6.3.1.4. Στη Διαδικασία Διαχείρισης Χρηστών ΠΕΣ πρέπει να προβλέπεται η υποχρέωση τήρησης αρχείου με το ιστορικό όλων των δικαιωμάτων ή επιπέδων πρόσβασης των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα ΠΕΣ του υπόχρεου προσώπου (ενδεικτικά ανά ΠΕΣ: λογαριασμός πρόσβασης, δικαιώματα/επίπεδο πρόσβασης αυτού, χρονικό διάστημα ισχύος).

6.3.2. Διαδικασία Ελέγχου Ορθής Εφαρμογής της Πολιτικής Λογικής Πρόσβασης

6.3.2.1. Στη Διαδικασία Ελέγχου Ορθής Εφαρμογής της Πολιτικής Λογικής Πρόσβασης πρέπει να περιγράφονται με σαφήνεια οι περιοδικοί έλεγχοι που πραγματοποιούνται, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών του άρθρου 11 του παρόντος Κανονισμού, αναφορικά με:

(α) Τον έλεγχο των δικαιωμάτων πρόσβασης των χρηστών ΠΕΣ, ήτοι, εάν το δικαίωμα πρόσβασης εκάστου χρήστη είναι πράγματι αυτό που του απεδόθη.

(β) Τον έλεγχο των λογαριασμών πρόσβασης, ήτοι, την αντιπαραβολή του αρχείου που περιλαμβάνει τις εγκεκριμένες αιτήσεις (παρ.6.3.1.4 του παρόντος άρθρου) με τους λογαριασμούς που προκύπτουν από έκαστο ΠΕΣ.

(γ) Τον δειγματοληπτικό έλεγχο των αρχείων καταγραφής πρόσβασης (access logs) για την ανακάλυψη ενδεχομένων μη αιτιολογημένων προσβάσεων.

6.4. Δημιουργία και Διαχείριση Λογαριασμών Πρόσβασης

6.4.1. Σχετικά με τη δημιουργία και διαχείριση των λογαριασμών πρόσβασης, το υπόχρεο πρόσωπο οφείλει να διατηρεί (ανά ΠΕΣ ή συγκεντρωτικά) 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 του υπόχρεου προσώπου 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 του άρθρου 11 του παρόντος Κανονισμού.

6.4.2. Για την υλοποίηση των υποχρεώσεων της παραγράφου 6.4.1 του παρόντος, το υπόχρεο πρόσωπο οφείλει να λαμβάνει υπόψη τις παρακάτω απαιτήσεις:

6.4.2.1. 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).

6.4.2.2. Οι χρησιμοποιούμενοι κωδικοί πρόσβασης θα πρέπει να είναι ισχυροί και να έχουν δημιουργηθεί με τρόπο που να αποτρέπει τον προσδιορισμό τους με εύκολο τρόπο. Ειδικότερα, οι κωδικοί πρόσβασης πρέπει να δημιουργούνται με συνδυασμό δύο (2) τουλάχιστον διαφορετικών ειδών χαρακτήρων (αριθμοί, γράμματα, ειδικοί χαρακτήρες). Οι κωδικοί πρόσβασης θα πρέπει να έχουν υποχρεωτικά ένα επαρκές ελάχιστο μήκος, να απαγορεύεται η χρήση πρόσφατων κωδικών στη διαδικασία αλλαγής τους και να μην ακολουθούνται συγκεκριμένα υποδείγματα κατά τη δημιουργία τους.

6.4.2.3. Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν περιοδικά, σε συχνότητα που καθορίζεται ρητά ανά ΠΕΣ και αναφέρεται σε αρχείο που οφείλει να διατηρεί το υπόχρεο πρόσωπο. Το υπόχρεο πρόσωπο οφείλει να χρησιμοποιεί και να 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, θα πρέπει να προβλέπεται η άμεση αλλαγή του αντίστοιχου κωδικού πρόσβασης.

6.4.2.4. Στην περίπτωση επαναλαμβανόμενης εισαγωγής λανθασμένων κωδικών πρόσβασης (ενδεικτικά, μετά από τρεις συνεχόμενες αποτυχημένες απόπειρες εισαγωγής του) ο λογαριασμός πρόσβασης θα αδρανοποιείται ή θα μπορεί να χρησιμοποιηθεί μόνο μετά την πάροδο ενός προκαθορισμένου χρονικού διαστήματος.

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

6.5.1. Το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών του στις υπηρεσίες ή/και τα δίκτυα που παρέχει.

6.5.2. Το υπόχρεο πρόσωπο οφείλει να διαμορφώσει και να ακολουθεί συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών πρόσβασης των συνδρομητών ή χρηστών στις υπηρεσίες ή/και τα δίκτυα που παρέχει, στην οποία θα περιγράφεται κατ' ελάχιστον 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. Κατά τη δημιουργία ή επανέκδοση του κωδικού πρόσβασης, το υπόχρεο πρόσωπο οφείλει να τον δημιουργεί με τρόπο που να αποτρέπει τον εύκολο προσδιορισμό του. Οφείλει επίσης να 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.

6.5.3. Το υπόχρεο πρόσωπο οφείλει να 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, σύμφωνα με την Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών του άρθρου 11 του παρόντος Κανονισμού.

6.5.4. Σε περίπτωση που το υπόχρεο πρόσωπο προσφέρει τη δυνατότητα στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας τους (ενδεικτικά, εξερχόμενες κλήσεις, ηλεκτρονικό ταχυδρομείο) μέσω συγκεκριμένης ιστοθέσης, οφείλει να χρησιμοποιεί τους ευρέως αποδεκτούς μηχανισμούς ασφαλούς αυθεντικοποίησης και κρυπτογράφησης και να περιγράφει αυτούς σε σχετικό αρχείο το οποίο οφείλει να διατηρεί.

6.5.5. Το υπόχρεο πρόσωπο οφείλει να 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. Οι κανόνες αυτοί θα πρέπει να λαμβάνουν υπόψη τις ευρέως αποδεκτές και διεθνείς πρακτικές.

ΑΡΘΡΟ 7 - Πολιτική Απομακρυσμένης Λογικής Πρόσβασης

7.1. Σκοπός - Εύρος Πολιτικής

7.1.1. Η Πολιτική Απομακρυσμένης Λογικής Πρόσβασης καθορίζει τη διαβάθμιση των επιπέδων πρόσβασης και θέτει τις απαιτήσεις για τον έλεγχο απομακρυσμένης πρόσβασης στα ΠΕΣ του υπόχρεου προσώπου.

7.1.2. Η Πολιτική Απομακρυσμένης Λογικής Πρόσβασης ισχύει για τους εργαζόμενους και συνεργάτες του υπόχρεου προσώπου, οι οποίοι στο πλαίσιο της εργασίας τους αποκτούν απομακρυσμένη πρόσβαση στα ΠΕΣ και στα σχετικά δεδομένα και τις πληροφορίες.

7.2. Απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών του υπόχρεου προσώπου.

7.2.1. Η απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών του υπόχρεου προσώπου στα ΠΕΣ του θα πρέπει να περιορίζεται στις περιπτώσεις που αυτό είναι απαραίτητο για τις επιχειρησιακές του ανάγκες.

7.2.2. Το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο στο οποίο καταγράφονται τα ΠΕΣ στα οποία επιτρέπεται η απομακρυσμένη πρόσβαση, και οι τεχνικοί τρόποι απομακρυσμένης πρόσβασης εργαζομένων και συνεργατών του, για κάθε ΠΕΣ στο οποίο έχει επιτραπεί η απομακρυσμένη πρόσβαση.

7.2.3. Θα πρέπει να τηρείται αρχείο με τους εργαζομένους και συνεργάτες (ονοματεπώνυμο και ιδιότητα) του υπόχρεου προσώπου, οι οποίοι έχουν εξουσιοδοτηθεί για χρήση της απομακρυσμένης πρόσβασης. Στο εν λόγω αρχείο καταγράφονται τα δικαιώματα πρόσβασης που τους αντιστοιχούν για κάθε ΠΕΣ.

7.2.4. Η απομακρυσμένη πρόσβαση των εργαζομένων και συνεργατών του υπόχρεου προσώπου πραγματοποιείται με χρήση μηχανισμών ασφαλούς αυθεντικοποίησης και κρυπτογράφησης (π.χ. μέσω VPN).

7.2.5. Το υπόχρεο πρόσωπο πρέπει να 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.

7.2.6. Η απομακρυσμένη πρόσβαση των συνεργατών του υπόχρεου προσώπου θα πρέπει να επιτρέπεται μόνο για συγκεκριμένο χρονικό διάστημα και να γίνεται είτε με τη χρήση προσωρινών κωδικών οι οποίοι θα μεταβάλλονται μετά το πέρας του προκαθορισμένου χρονικού διαστήματος είτε με την απενεργοποίηση των λογαριασμών μετά το πέρας του διαστήματος αυτού.

7.2.7. Το υπόχρεο πρόσωπο οφείλει να επιτρέπει την απομακρυσμένη πρόσβαση των συνεργατών του στα συστήματά του μόνο κατόπιν έγκρισης των σχετικών αιτημάτων, στα οποία θα αναγράφεται ο λόγος της πρόσβασης, το σύστημα στο οποίο θα πραγματοποιηθεί η πρόσβαση καθώς και το χρονικό διάστημα που απαιτείται. Το υπόχρεο πρόσωπο οφείλει να τηρεί αρχείο με όλες τις πληροφορίες της παρούσας παραγράφου.

7.3. Διαδικασία Διαχείρισης Λογαριασμών Απομακρυσμένης Πρόσβασης

7.3.1. Το υπόχρεο πρόσωπο οφείλει να διαμορφώσει και να ακολουθεί συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών απομακρυσμένης πρόσβασης των εργαζομένων και συνεργατών του, η οποία να είναι σύμφωνη με τις απαιτήσεις που αναφέρονται στην παράγραφο 7.2 του παρόντος άρθρου.

7.3.2. Το υπόχρεο πρόσωπο οφείλει να ελέγχει κατ' ελάχιστον κάθε τρεις (3) μήνες α) την αντιστοίχιση των λογαριασμών απομακρυσμένης πρόσβασης και του αρχείου της παρ. 7.2.3 του παρόντος άρθρου, και β) την υλοποίηση των απαιτούμενων μεταβολών των κωδικών και απενεργοποιήσεων των λογαριασμών της παρ. 7.2.6 του παρόντος άρθρου, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών του άρθρου 11 του παρόντος Κανονισμού.

ΑΡΘΡΟ 8 - Πολιτική Διαχείρισης και Εγκατάστασης ΠΕΣ

8.1. Σκοπός - Εύρος Πολιτικής

Σκοπός της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ είναι να προσδιορίσει τις απαιτήσεις που πρέπει να ικανοποιούνται κατά τη σχεδίαση, ανάπτυξη, προμήθεια, εγκατάσταση, λειτουργία, διαχείριση, υποστήριξη, αναβάθμιση, επικαιροποίηση, διαγραφή, απόσυρση των ΠΕΣ, προκειμένου να διασφαλίζεται το απόρρητο των επικοινωνιών.

8.2. Γενικές Απαιτήσεις

8.2.1. Κατά τη διαχείριση και εγκατάσταση ΠΕΣ, το υπόχρεο πρόσωπο θα πρέπει να λαμβάνει όλα τα απαραίτητα μέτρα προκειμένου να ελαχιστοποιείται ο κίνδυνος διαρροής πληροφοριών που σχετίζονται με το απόρρητο των επικοινωνιών των συνδρομητών ή χρηστών των παρεχομένων δικτύων ή υπηρεσιών.

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

8.2.3. Για οποιαδήποτε αλλαγή υλικού ή λογισμικού ΠΕΣ, το υπόχρεο πρόσωπο υποχρεούται να διατηρεί αρχείο στο οποίο καταγράφεται η ημερομηνία, ο τρόπος, η αιτιολόγηση και ο εργαζόμενος ή συνεργάτης που πραγματοποίησε τις αλλαγές. Το αρχείο ενημερώνεται και διατηρείται από συγκεκριμένη διοικητική οντότητα ή εργαζόμενο του υπόχρεου προσώπου.

8.3. Διαδικασίες Διαχείρισης και Εγκατάστασης ΠΕΣ

Το υπόχρεο πρόσωπο υποχρεούται, κατ' ελάχιστον, να διατηρεί και να εφαρμόζει διαδικασίες για τα παρακάτω στάδια:

i. Προμήθεια-Ανάπτυξη Υλικού και Λογισμικού

ii. Εγκατάσταση-Λειτουργία Υλικού και Λογισμικού

iii. Συντήρηση-Υποστήριξη-Λειτουργία Υλικού και Λογισμικού

iv. Διαγραφή-Απόσυρση Υλικού και Λογισμικού

8.3.1. Διαδικασία Προμήθειας-Ανάπτυξης Υλικού και Λογισμικού των ΠΕΣ

8.3.1.1. Το υπόχρεο πρόσωπο πραγματοποιεί αποτίμηση κινδύνου για τον εντοπισμό των πιθανών απειλών, αδυναμιών και κινδύνων αναφορικά με το απόρρητο των επικοινωνιών του υπό προμήθεια/ανάπτυξη ΠΕΣ, σύμφωνα με τα οριζόμενα στην παράγραφο 3.3 «Διαδικασία αποτίμησης πληροφοριακού κινδύνου» του παρόντος Κανονισμού.

8.3.1.2. 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.

8.3.2. Διαδικασία Δοκιμών, Αποδοχής και Ελέγχου Ορθής Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ

8.3.2.1. 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.

8.3.2.2. 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.

8.3.2.3. 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.

8.3.3. Διαδικασία Ελέγχου Συντήρησης-Υποστήριξης-Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ

8.3.3.1. Στις ελάχιστες απαιτήσεις της Διαδικασίας Ελέγχου Συντήρησης-Υποστήριξης-Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ 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.

8.3.3.2. Το υπόχρεο πρόσωπο υποχρεούται να καταγράφει και να διατηρεί σε αρχείο τις ενέργειες στο λειτουργικό σύστημα και στις εφαρμογές των ΠΕΣ, καθώς και τα συμβάντα συστήματος των ΠΕΣ.

8.3.4. Διαδικασία Διαγραφής-Απόσυρσης Υλικού και Λογισμικού των ΠΕΣ

8.3.4.1. Το υπόχρεο πρόσωπο υποχρεούται να ορίζει συγκεκριμένες ενέργειες προκειμένου να διασφαλίζεται ότι, με την επιφύλαξη τήρησης υποχρεώσεων που απορρέουν από άλλες διατάξεις της κείμενης νομοθεσίας, 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.

8.3.4.2. Το υπόχρεο πρόσωπο υποχρεούται να διατηρεί αρχείο στο οποίο καταγράφονται τα ΠΕΣ, τα οποία αποσύρονται.

8.3.4.3. Το υπόχρεο πρόσωπο υποχρεούται να διατηρεί αρχείο καταγραφής των ενεργειών διαγραφής των δεδομένων του ΠΕΣ, στο οποίο κατ' ελάχιστον καταγράφεται το όνομα χρήστη του εργαζομένου ή του συνεργάτη που διενεργεί τη διαγραφή.

ΑΡΘΡΟ 9 - Πολιτική Διαχείρισης Περιστατικών Ασφάλειας

9.1. Σκοπός - Εύρος Πολιτικής

Η Πολιτική Διαχείρισης Περιστατικών Ασφάλειας έχει ως σκοπό (α) να καταγραφούν οι λεπτομέρειες κάθε περιστατικού ασφάλειας, (β) να διερευνηθούν τα αίτια και να προσδιοριστούν οι τεχνικές ή/και οργανωτικές αδυναμίες στις οποίες ενδεχομένως οφείλεται το περιστατικό ασφάλειας, (γ) να καθοριστούν οι συνέπειες και να υλοποιηθούν οι ενέργειες αποκατάστασης με συγκεκριμένο χρονοδιάγραμμα, ανάλογα με την περίπτωση και (δ) να ενημερωθούν: i. ο Υπεύθυνος Διασφάλισης του Απορρήτου των Επικοινωνιών και τα αρμόδια στελέχη του υπόχρεου προσώπου, ii. οι αρμόδιες Αρχές και iii. οι θιγόμενοι συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών, σύμφωνα με την κείμενη νομοθεσία.

9.2. Γενικές Απαιτήσεις

9.2.1. Το υπόχρεο πρόσωπο οφείλει να καταρτίζει και να εφαρμόζει Διαδικασία Διαχείρισης Περιστατικών

Ασφάλειας, η οποία θα ενεργοποιείται αμελλητί σε κάθε περίπτωση περιστατικού ασφάλειας.

9.2.2. Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας προβλέπεται η καταγραφή όλων των στοιχείων που αναφέρονται στην παράγραφο 9.1 του παρόντος άρθρου, καθώς και η σύνταξη και διατήρηση σε αρχείο όλων των εγγράφων που σχετίζονται με τα περιστατικά ασφάλειας, από τα οποία θα τεκμηριώνεται και η εκτέλεση των αντίστοιχων προβλεπόμενων ενεργειών. Κατ' ελάχιστον, καταγράφονται τα ακόλουθα:

α. Ημερομηνία, ώρα εκδήλωσης και περιγραφή του περιστατικού,

β. Ημερομηνία και ώρα που έγινε αντιληπτό το περιστατικό από το υπόχρεο πρόσωπο,

γ. Σημείο στο οποίο εκδηλώθηκε το περιστατικό (ενδεικτικά, σύστημα, υπηρεσία, εφαρμογή, πρωτόκολλα, τύπος δεδομένων),

δ. Εκτιμούμενη αιτία εκδήλωσης του περιστατικού,

ε. Συνέπειες του περιστατικού (ενδεικτικά, πλήθος χρηστών που επηρεάστηκαν, τύπος και όγκος των δεδομένων που επηρεάστηκαν),

στ. Συλλεχθέντα στοιχεία από το υπόχρεο πρόσωπο για τη διερεύνηση του περιστατικού (ενδεικτικά, 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.

9.2.3. Σε περίπτωση περιστατικού ασφάλειας, τα υπόχρεα πρόσωπα που αναφέρονται στο άρθρο 1 παρ.2 του παρόντος Κανονισμού υποχρεούνται να ενημερώνουν αμελλητί την Α.Δ.Α.Ε., υποβάλλοντας, για κάθε περιστατικό, έγγραφο με τίτλο «Έκθεση Άμεσης Αναφοράς Περιστατικού Ασφάλειας». Στην «Έκθεση Άμεσης Αναφοράς Περιστατικού Ασφάλειας» καταγράφονται, κατ' ελάχιστον, οι αναφερόμενες στην παράγραφο 9.2.2 του παρόντος άρθρου πληροφορίες, σύμφωνα με τα δεδομένα που είναι διαθέσιμα κατά τον χρόνο πραγματοποίησης της ενημέρωσης. Μετά την ολοκλήρωση της αντιμετώπισης και της διερεύνησης του περιστατικού, τα υπόχρεα πρόσωπα της παρούσας παραγράφου υποβάλλουν στην Α.Δ.Α.Ε. έγγραφο με τίτλο «Τελική Έκθεση Αναφοράς Περιστατικού Ασφάλειας», στο οποίο καταγράφονται με λεπτομέρεια όλες οι αναφερόμενες στην παράγραφο 9.2.2 του παρόντος άρθρου πληροφορίες, καθώς και κάθε πρόσθετη πληροφορία που τυχόν έχει στη διάθεσή του το υπόχρεο πρόσωπο.

9.2.4. Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας ορίζονται τα αρμόδια στελέχη του υπόχρεου προσώπου, στα οποία θα πρέπει να αναφέρονται άμεσα τα περιστατικά ασφάλειας, καθώς και τα σχετικά στοιχεία επικοινωνίας αυτών.

9.2.5. Το υπόχρεο πρόσωπο οφείλει να παρέχει στους συνδρομητές ή χρήστες των δικτύων ή υπηρεσιών του τη δυνατότητα να καταγγέλλουν με απλά μέσα (π.χ. μέσω της ιστοθέσης του) την ενδεχόμενη παραβίαση του απορρήτου των επικοινωνιών τους.

9.2.6. Το υπόχρεο πρόσωπο οφείλει να ελέγχει σε τακτά χρονικά διαστήματα την ετοιμότητα ενεργοποίησης της Διαδικασίας Διαχείρισης Περιστατικών Ασφάλειας, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών του άρθρου 11 του παρόντος Κανονισμού.

ΑΡΘΡΟ 10 - Πολιτική Ασφάλειας Δικτύου

10.1. Σκοπός - Εύρος Πολιτικής

Ο σκοπός της Πολιτικής Ασφάλειας Δικτύου είναι ο λογικός διαχωρισμός των δικτύων του υπόχρεου προσώπου από εξωτερικά δίκτυα και η κατάτμηση των δικτύων του σε ζώνες ασφάλειας ή υποδίκτυα, ανάλογα με το επίπεδο ασφάλειας που απαιτείται, με στόχο την απομόνωση των ΠΕΣ σε ζώνες ασφάλειας, τον διαχωρισμό αυτών σε δικτυακό επίπεδο, και τον έλεγχο της ροής δεδομένων μεταξύ αυτών.

10.2. Γενικές Αρχές Μηχανισμών και Συστημάτων Πολιτικής Ασφάλειας Δικτύου

10.2.1. Το υπόχρεο πρόσωπο οφείλει να καταρτίζει και να διατηρεί διαρκώς ενημερωμένο αρχείο στο οποίο ορίζονται οι μηχανισμοί και τα συστήματα που χρησιμοποιούνται σε υλικό και λογισμικό για τους σκοπούς της Πολιτικής Ασφάλειας Δικτύου, καθώς και οι τρόποι λειτουργίας και τεχνικής διαμόρφωσης αυτών, οι οποίοι θα πρέπει να λαμβάνουν υπόψη τις διεθνείς, ευρέως αποδεκτές πρακτικές και πρότυπα και την αποτίμηση κινδύνου στην οποία έχει προβεί το υπόχρεο πρόσωπο, σε συμφωνία με τις αρχές του εδαφίου 3.3 του παρόντος Κανονισμού. Οι μηχανισμοί και τα συστήματα της Πολιτικής Ασφάλειας Δικτύου περιλαμβάνουν, ενδεικτικά και όχι περιοριστικά: αναχώματα ασφάλειας, συστήματα ανίχνευσης και αποτροπής εισβολών, λίστες ελέγχου πρόσβασης, ιδεατά ιδιωτικά δίκτυα, ιδεατά τοπικά δίκτυα.

10.2.2. Η εγκατάσταση, η επικαιροποίηση και η διαχείριση των αναφερόμενων στην παράγραφο 10.2.1 του παρόντος άρθρου μηχανισμών και συστημάτων είναι σύμφωνη με τις αρχές της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ του άρθρου 8 του παρόντος Κανονισμού και συμπεριλαμβάνει τους κανόνες πρόσβασης ή ελέγχου που έχουν τεθεί στους εν λόγω μηχανισμούς και συστήματα (ενδεικτικά αναφέρεται η επικαιροποίηση του συστήματος ανίχνευσης/προστασίας εισβολών με υπογραφές νέων εισβολών ή επιθέσεων).

10.2.3. Η λειτουργία των αναφερομένων στην παράγραφο 10.2.1 του παρόντος άρθρου μηχανισμών και συστημάτων πρέπει να είναι συνεχής, με την εξαίρεση των περιπτώσεων προγραμματισμένης συντήρησης ή αναβάθμισης, σύμφωνα με τις αρχές της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ του άρθρου 8 του παρόντος Κανονισμού.

10.2.4. Σε περίπτωση που ένας μηχανισμός ή σύστημα από τους αναφερόμενους στην παράγραφο 10.2.1 του παρόντος άρθρου εντοπίσει κάποιο μη σύνηθες συμβάν, ενεργοποιείται συναγερμός που είναι ενδεικτικός του είδους, της φύσης και σοβαρότητας του συμβάντος και κάθε διαθέσιμη σχετική πληροφορία καταγράφεται και αποθηκεύεται σε ειδικό αρχείο για περαιτέρω επεξεργασία. Αναλόγως της κρισιμότητας του συμβάντος, το υπόχρεο πρόσωπο ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με το άρθρο 9 του παρόντος Κανονισμού.

10.3. Λογικός Διαχωρισμός και Κατάτμηση Δικτύων του Υπόχρεου Προσώπου.

10.3.1. Το υπόχρεο πρόσωπο οφείλει να καταρτίζει και να διατηρεί διαρκώς ενημερωμένο αρχείο, στο οποίο περιγράφεται αναλυτικά, με βάση τους αναφερόμενους στην παράγραφο 10.2.1 του παρόντος άρθρου μηχανισμούς και συστήματα, ο λογικός διαχωρισμός και η κατάτμηση των δικτύων του με αντίστοιχη σχηματική απεικόνιση, περιγράφεται η αρχιτεκτονική που έχει υλοποιηθεί και καταγράφονται όλα τα ΠΕΣ και η ζώνη ασφάλειας στην οποία έχουν τοποθετηθεί. Το υπόχρεο πρόσωπο οφείλει να διατηρεί τις προηγούμενες εκδόσεις του εν λόγω αρχείου.

10.3.2. Σε περίπτωση που το υπόχρεο πρόσωπο διαθέτει στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών που απαιτούν πρόσβαση σε εξυπηρετητές από εξωτερικά δίκτυα (αναφέρονται ενδεικτικά οι υπηρεσίες ηλεκτρονικού ταχυδρομείου), τα ΠΕΣ που προσφέρουν τις εν λόγω υπηρεσίες πρέπει να τοποθετούνται σε μία ή περισσότερες αποστρατικοποιημένες ζώνες.

10.3.3. Τα ΠΕΣ του υπόχρεου προσώπου που χρησιμοποιούνται από τους εργαζόμενους και συνεργάτες του για την τέλεση των επιχειρησιακών διαδικασιών και λειτουργιών (ενδεικτικά, τα συστήματα διαχείρισης και εποπτείας, τα συστήματα καταγραφής, τα συστήματα χρέωσης συνδρομητών, οι βάσεις δεδομένων που περιέχουν δεδομένα επικοινωνίας και οι εφαρμογές πρόσβασης σε δεδομένα επικοινωνίας), πρέπει να εντάσσονται σε μία ή περισσότερες εσωτερικές έμπιστες ζώνες, ανάλογα με τις απαιτήσεις ασφάλειας και την κρισιμότητά τους.

10.3.4. Τα ΠΕΣ του υπόχρεου προσώπου, και ιδιαίτερα αυτά που δεν τοποθετούνται σε αποστρατικοποιημένες ή έμπιστες ζώνες, (ενδεικτικά, τα δίκτυα πρόσβασης/μετάδοσης, οι συσκευές και κόμβοι διασύνδεσης με τρίτα/εξωτερικά δίκτυα), ανάλογα με την τεχνολογία τους, είναι δυνατό να υποστηρίζουν την προαιρετική χρήση συγκεκριμένων μηχανισμών ασφάλειας. Στην περίπτωση αυτή, το υπόχρεο πρόσωπο οφείλει να επιλέγει, να ενεργοποιεί και να παραμετροποιεί όλους τους κατάλληλους μηχανισμούς ασφάλειας, εκμεταλλευόμενο τις δυνατότητες και μεθόδους ασφάλειας που διαθέτουν (αναφέρεται ενδεικτικά η κρυπτογράφηση), τις διεθνείς, ευρέως αποδεκτές πρακτικές και πρότυπα, και τα αποτελέσματα που προκύπτουν από την αποτίμηση κινδύνου, σε συμφωνία με τις αρχές του άρθρου 3.3 του παρόντος Κανονισμού. Για τα ΠΕΣ της παρούσας παραγράφου, το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο με πλήρη ανάλυση των μέτρων προστασίας και ασφάλειας που έχουν υλοποιηθεί σε αυτά, με σκοπό την προστασία του απορρήτου των επικοινωνιών.

ΑΡΘΡΟ 11 - Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

11.1. Σκοπός - Εύρος Πολιτικής

Η Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών καθορίζει τις απαιτήσεις και το πλαίσιο διεξαγωγής ελέγχων που διενεργεί το υπόχρεο πρόσωπο, με σκοπό την ορθή τήρηση των επιμέρους πολιτικών και διαδικασιών, τη διαπίστωση της επάρκειας και αποτελεσματικότητας των μηχανισμών ασφάλειας και τον έλεγχο των τεχνικών ευπαθειών στα ΠΕΣ.

11.2. Γενικές Απαιτήσεις

11.2.1. Το υπόχρεο πρόσωπο οφείλει να προβαίνει σε προγραμματισμό ελέγχου εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, ο οποίος καταγράφεται σε αρχείο, καλύπτει όλο το εύρος εφαρμογής της Πολιτικής και πραγματοποιείται κατ' ελάχιστον ανά δύο (2) έτη.

11.2.2. Ο έλεγχος περιλαμβάνει τη χρήση και την εξέταση των αρχείων καταγραφής κάθε ΠΕΣ, κατά περίπτωση σε συσχετισμό με άλλα αρχεία που προβλέπονται στον παρόντα Κανονισμό.

11.2.3. Οι έλεγχοι είναι δυνατό να πραγματοποιούνται από εξωτερικό φορέα ή από ειδικά εξουσιοδοτημένους προς τούτο, εργαζόμενους του υπόχρεου προσώπου.

11.2.3.1. Στην περίπτωση διεξαγωγής ελέγχου εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών από εξωτερικό φορέα, θα πρέπει να λαμβάνεται μέριμνα από το υπόχρεο πρόσωπο 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, θα πρέπει να παρίσταται ειδικά εξουσιοδοτημένος προς τούτο εργαζόμενος του υπόχρεου προσώπου.

11.2.3.2. Στην περίπτωση διεξαγωγής ελέγχου εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών από ειδικά εξουσιοδοτημένους προς τούτο εργαζόμενους του υπόχρεου προσώπου, αυτοί θα πρέπει να είναι κατάλληλα εκπαιδευμένοι και να λαμβάνονται υπόψη παράγοντες αντικειμενικότητας και αμεροληψίας. Ενδεικτικά αναφέρεται ότι οι ελεγκτές δεν θα πρέπει να ανήκουν στο Τμήμα ή τη Διεύθυνση της οποίας τα συστήματα ελέγχονται ή να έχουν συμμετάσχει στην ανάπτυξη κώδικα και στην εγκατάσταση ή τη λειτουργία του υπό έλεγχο συστήματος.

11.2.4. Οι αρμοδιότητες των εργαζομένων του υπόχρεου προσώπου, οι οποίοι διενεργούν τους ελέγχους, πρέπει να είναι εκ των προτέρων καθορισμένες και να περιγράφονται αναλυτικά σε σχετικό αρχείο, το οποίο τηρείται από το υπόχρεο πρόσωπο.

11.3. Προετοιμασία Ελέγχου

Τα στάδια προετοιμασίας κάθε ελέγχου περιλαμβάνουν κατ' ελάχιστον τα ακόλουθα:

i. Τον καθορισμό του συστήματος και των διαδικασιών/μηχανισμών διασφάλισης του απορρήτου που θα ελεγχθούν και των ελέγχων για την εύρεση τεχνικών ευπαθειών

ii. Το χρονοδιάγραμμα διεξαγωγής του ελέγχου

iii. Τη συλλογή των απαιτούμενων πληροφοριών και δεδομένων και

iv. Τον ορισμό των προσώπων που απαρτίζουν την Ομάδα Ελέγχου.

Τα στοιχεία της παρούσας παραγράφου καταγράφονται σε σχετικό αρχείο, το οποίο διατηρείται από το υπόχρεο πρόσωπο.

11.4. Διεξαγωγή Ελέγχου

11.4.1. Τα στάδια διεξαγωγής κάθε ελέγχου, τα σχετικά ευρήματα και οι προτεινόμενες βελτιώσεις ή τροποποιήσεις καταγράφονται σε ειδικό αρχείο, το οποίο διατηρείται από το υπόχρεο πρόσωπο, ακόμη και στην περίπτωση που δεν υπάρχουν ευρήματα από τον έλεγχο.

11.4.2. Η απόδοση σε ένα ή περισσότερα μέλη της Ομάδας Ελέγχου δικαιωμάτων πρόσβασης σε εργαλεία λογισμικού, συστήματα (αναφέρονται ενδεικτικά τα συστήματα ανίχνευσης επισυνδέσεων) ή χώρους των εγκαταστάσεων, θα πρέπει να επιτρέπεται μόνο για το χρονικό διάστημα του αντίστοιχου ελέγχου και να γίνεται σύμφωνα με τις αντίστοιχες Πολιτικές Ασφάλειας του υπόχρεου προσώπου.

11.5. Αποτελέσματα Ελέγχου

Σε περίπτωση που προκύψουν ευρήματα από τον έλεγχο, το υπόχρεο πρόσωπο ορίζει τις απαιτούμενες ενέργειες (όπως είναι ενδεικτικά η αναθεώρηση διαδικασιών/οδηγιών, η επικαιροποίηση λογισμικού, η τροποποίηση παραμέτρων τεχνικής διαμόρφωσης, η μερική ή ολική αντικατάσταση συστήματος ή εφαρμογής), το χρονοδιάγραμμα πραγματοποίησής τους, τις αρμοδιότητες των εργαζομένων ή των συνεργατών του για την πραγματοποίηση των διορθωτικών ενεργειών και τα πρόσωπα που θα είναι ειδικά εξουσιοδοτημένα να ελέγχουν την ορθή υλοποίηση των ενεργειών της παρούσας παραγράφου. Αναλόγως της φύσης και της κρισιμότητας των ευρημάτων, το υπόχρεο πρόσωπο ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με το άρθρο 9 του παρόντος Κανονισμού.

11.6. Διαδικασία Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

11.6.1. Το υπόχρεο πρόσωπο πρέπει να διαθέτει και να 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.

ΑΡΘΡΟ 12 - Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού.

12.1. Σκοπός - Εύρος Πολιτικής

Η Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού καθορίζει τις απαιτήσεις και περιγράφει τα τεχνικά και οργανωτικά μέτρα που απαιτούνται προκειμένου να προστατεύονται τα ΠΕΣ του υπόχρεου προσώπου έναντι του κακόβουλου λογισμικού.

12.2. Απαιτήσεις - Υποχρεώσεις

12.2.1. Το υπόχρεο πρόσωπο οφείλει να λαμβάνει όλα τα απαραίτητα οργανωτικά και τεχνικά μέτρα ασφάλειας, τα οποία αποσκοπούν στην αποτροπή, ανίχνευση και αντιμετώπιση του κακόβουλου λογισμικού.

12.2.2. Το υπόχρεο πρόσωπο οφείλει να ενημερώνει τους εργαζόμενους αναφορικά με τους κινδύνους από το κακόβουλο λογισμικό καθώς και για τις υποχρεώσεις τους σε σχέση με τα μέτρα προστασίας έναντι του κακόβουλου λογισμικού.

12.2.3. Το υπόχρεο πρόσωπο οφείλει, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών του άρθρου 11 του παρόντος Κανονισμού, να πραγματοποιεί έλεγχο της ακεραιότητας του λογισμικού των ΠΕΣ. Ο έλεγχος αυτός έχει ως σκοπό τη διαπίστωση της μη ύπαρξης λογισμικού στα ΠΕΣ πέραν αυτού που έχει επισήμως προμηθευτεί το υπόχρεο πρόσωπο.

12.2.4. Το υπόχρεο πρόσωπο οφείλει να ορίσει τους κατάλληλους μηχανισμούς για τον περιορισμό της εξάπλωσης του κακόβουλου λογισμικού, σε περίπτωση ανίχνευσής του. Στην περίπτωση αυτή θα πρέπει να πραγματοποιείται άμεση αξιολόγηση του περιστατικού και αναλόγως της κρισιμότητάς του, το υπόχρεο πρόσωπο ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με το άρθρο 9 του παρόντος Κανονισμού.

12.2.5. Το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο στο οποίο καταγράφονται οι λεπτομέρειες εφαρμογής των απαιτήσεων που ορίζονται στην παράγραφο 12.2 του παρόντος.

ΑΡΘΡΟ 13 - Πολιτική Χρήσης Κρυπτογραφίας

13.1. Σκοπός - Εύρος Πολιτικής

Η Πολιτική Χρήσης Κρυπτογραφίας ορίζει την υποχρέωση του υπόχρεου προσώπου να χρησιμοποιεί κατάλληλους αλγόριθμους και συστήματα κρυπτογραφίας για την επαρκή προστασία των δεδομένων επικοινωνίας ή άλλων πληροφοριών που μπορεί να οδηγήσουν σε αποκάλυψη δεδομένων επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών (ενδεικτικά αναφέρονται κωδικοί πρόσβασης και δεδομένα διάρθρωσης των ΠΕΣ) κατά την αποθήκευση και μεταφορά τους σε ΠΕΣ, καθώς και τα ελάχιστα χαρακτηριστικά ασφάλειας των συστημάτων κρυπτογραφίας. Η Πολιτική Χρήσης Κρυπτογραφίας εφαρμόζεται σε όλα τα ΠΕΣ του υπόχρεου προσώπου.

13.2. Γενικές Απαιτήσεις

13.2.1. Το υπόχρεο πρόσωπο πρέπει να εφαρμόζει συστήματα κρυπτογράφησης για την επαρκή προστασία των δεδομένων επικοινωνίας κατά την αποθήκευση και μεταφορά τους μέσω δικτύων.

13.2.2. Η κρυπτογράφηση πρέπει να εφαρμόζεται στα ΠΕΣ με βάση τα αποτελέσματα που προκύπτουν από την αποτίμηση κινδύνου σε συμφωνία με τις αρχές του άρθρου 3.3 του παρόντος Κανονισμού.

13.2.3. Σε περίπτωση που χρησιμοποιούνται αλγόριθμοι και συστήματα κρυπτογράφησης, συμπεριλαμβανομένων και των αλγορίθμων ψηφιακής υπογραφής, λαμβάνονται υπόψη τα διεθνώς ευρέως αποδεκτά πρότυπα.

13.2.4. Το μήκος κλειδιού που χρησιμοποιείται θα πρέπει να λαμβάνει υπόψη τα διεθνώς και ευρέως αποδεκτά πρότυπα, ανάλογα με τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης και με τα αποτελέσματα της αποτίμησης κινδύνου, σε συμφωνία με τις αρχές του άρθρου 3.3 του παρόντος Κανονισμού.

13.2.5. Το υπόχρεο πρόσωπο οφείλει να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση στα κλειδιά τα οποία χρησιμοποιούνται για κρυπτογράφηση, αυθεντικοποίηση ή ψηφιακή υπογραφή.

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

13.2.7. Σε περίπτωση που το υπόχρεο πρόσωπο χρησιμοποιεί ψηφιακά πιστοποιητικά δημόσιων κλειδιών, τα οποία παράγονται από παρόχους υπηρεσιών πιστοποίησης, οφείλει να εξασφαλίζει ότι ο πάροχος υπηρεσιών πιστοποίησης συμμορφώνεται με την κείμενη νομοθεσία.

13.2.8. Σε περίπτωση που το υπόχρεο πρόσωπο παράγει και διαχειρίζεται κλειδιά κρυπτογράφησης τα οποία χρησιμοποιούνται σε ΠΕΣ, θα πρέπει να καταρτίζει και να τηρεί κατάλληλες διαδικασίες για τη δημιουργία, πιστοποίηση, διανομή και ανάκληση των κρυπτογραφικών κλειδιών.

13.2.9. Το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο στο οποίο καταγράφονται οι λεπτομέρειες εφαρμογής των απαιτήσεων που ορίζονται στην παράγραφο 13.2.

ΑΡΘΡΟ 14 - Διαδικασία Ελέγχου από την Α.Δ.Α.Ε.

14.1. Τακτικός Έλεγχος

14.1.1. Η Α.Δ.Α.Ε. σε τακτά χρονικά διαστήματα διενεργεί έλεγχο στα υπόχρεα πρόσωπα που εμπίπτουν στις διατάξεις του παρόντος Κανονισμού κατά τα οριζόμενα

στο άρθρο 1 αυτού. Η συχνότητα των ελέγχων καθορίζεται από την Α.Δ.Α.Ε. με απόφασή της.

14.1.2. Ο έλεγχος διενεργείται από τις αρμόδιες Υπηρεσίες της Α.Δ.Α.Ε. με την παρουσία του Υπεύθυνου Διασφάλισης του Απορρήτου των Επικοινωνιών ή άλλου εξουσιοδοτημένου προς τούτο εργαζόμενου του υπόχρεου προσώπου, σύμφωνα με τα ακολούθως οριζόμενα:

14.1.2.1. Η Α.Δ.Α.Ε. με απόφασή της ορίζει ομάδα ελέγχου που αποτελείται από τρία (3) τουλάχιστον άτομα, με σκοπό τον έλεγχο συγκεκριμένου υπόχρεου προσώπου. Με την ίδια απόφαση καθορίζεται η ειδικότερη σύνθεση της ομάδας ελέγχου.

14.1.2.2. Σε χρόνο που αποφασίζει η ομάδα ελέγχου ενημερώνει τον Υπεύθυνο Διασφάλισης του Απορρήτου των Επικοινωνιών σύμφωνα με τα οριζόμενα στο άρθρο 3.2.6 του παρόντος για την ημερομηνία διενέργειας επιτόπιου ελέγχου, ζητώντας του παράλληλα να έχει διαθέσιμα πλήρη αντίγραφα των υφισταμένων διαδικασιών που υλοποιούν την εγκριθείσα από την Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, από τα οποία να προκύπτει σαφώς η ημερομηνία έκδοσής τους. Από τη λήψη της αναφερόμενης στο προηγούμενο εδάφιο έγγραφης ενημέρωσης του Υπεύθυνου Διασφάλισης του Απορρήτου των Επικοινωνιών περί της διεξαγωγής τακτικού ελέγχου από την Α.Δ.Α.Ε. και μέχρι να λάβει έγγραφη ενημέρωση από την Αρχή αναφορικά με το πέρας του ελέγχου, το υπόχρεο πρόσωπο δεν δύναται να προβεί σε οποιαδήποτε αναθεώρηση του κειμένου της εγκριθείσας Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών ή των συνοδευτικών αρχείων αυτής (διαδικασίες, τεχνικές οδηγίες κ.ά.).

14.1.2.3. Η ομάδα ελέγχου προβαίνει σε επιτόπιο έλεγχο στις εγκαταστάσεις του υπόχρεου προσώπου, προκειμένου να διαπιστώσει εάν συμμορφώνεται με την εγκριθείσα από την Α.Δ.Α.Ε. Πολιτική Ασφάλειας μέσω της εφαρμογής των διαδικασιών του. Κατά τον επιτόπιο έλεγχο, στον οποίο πρέπει να παρίσταται απαραιτήτως ο Υπεύθυνος Διασφάλισης του Απορρήτου των Επικοινωνιών, η ομάδα ελέγχου ζητά κατά την κρίση της συμπληρωματικά στοιχεία και συνεργάζεται με το προσωπικό του ελεγχόμενου προσώπου. Η ομάδα ελέγχου προβαίνει σε αναλυτική εξέταση των αρχείων που αφορούν στην Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και στην εφαρμογή αυτής, προκειμένου να διαπιστωθούν ενδεχόμενες παραλείψεις ή αναντιστοιχίες με τις διατάξεις της εγκριθείσας από την Α.Δ.Α.Ε. Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

14.1.2.4. Για κάθε επιτόπιο έλεγχο συντάσσεται ειδικό έγγραφο με τίτλο «Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις του υπόχρεου προσώπου», το οποίο υπογράφεται από τον Υπεύθυνο Διασφάλισης του Απορρήτου των Επικοινωνιών.

14.1.3. Μετά την ολοκλήρωση των επιτόπιων ελέγχων, η ομάδα ελέγχου εξετάζει διεξοδικά το σύνολο των συλλεχθέντων στοιχείων και συντάσσει ειδικό έγγραφο με τίτλο «Έκθεση διενέργειας τακτικού ελέγχου στο υπόχρεο πρόσωπο», το οποίο περιλαμβάνει απαραιτήτως τα ακόλουθα στοιχεία:

α) Τα στοιχεία της Απόφασης της Α.Δ.Α.Ε. με την οποία αποφασίστηκε η διενέργεια τακτικού ελέγχου,

β) Το ονοματεπώνυμο και την ιδιότητα των προσώπων που απαρτίζουν την ομάδα ελέγχου και την ημερομηνία σύστασης της τελευταίας,

γ) Την επωνυμία του ελεγχόμενου υπόχρεου προσώπου, καθώς και το όνομα του Υπευθύνου Διασφάλισης του Απορρήτου των Επικοινωνιών,

δ) Τα Πρακτικά Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις του ελεγχόμενου προσώπου καθώς και κάθε σχετική έγγραφη επικοινωνία μεταξύ της Α.Δ.Α.Ε. και του ελεγχόμενου προσώπου στο πλαίσιο της διεξαγωγής του τακτικού ελέγχου,

ε) Αναλυτική περιγραφή των ευρημάτων του ελέγχου και διαπίστωση τυχόν παραλείψεων ή αναντιστοιχιών με την εγκριθείσα από την Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών,

στ) Την ημερομηνία έναρξης και περάτωσης του ελέγχου,

ζ) Τελικό πόρισμα του ελέγχου.

14.1.4. Το ελεγχόμενο υπόχρεο πρόσωπο καλείται να παραλάβει από την Α.Δ.Α.Ε. την απόφαση της Ολομέλειας της Α.Δ.Α.Ε. για την έγκριση της «Έκθεσης διενέργειας τακτικού ελέγχου στο υπόχρεο πρόσωπο» μετά της συνημμένης σε αυτήν έκθεσης.

14.2. Έκτακτος Έλεγχος

14.2.1. Η Α.Δ.Α.Ε. διενεργεί έκτακτους ελέγχους αυτεπαγγέλτως ή κατόπιν καταγγελίας.

14.2.2. Ο έκτακτος έλεγχος διενεργείται χωρίς προηγούμενη ενημέρωση του ελεγχόμενου υπόχρεου προσώπου, κατόπιν σχετικής απόφασης της Α.Δ.Α.Ε. που ορίζει και τα στελέχη της Α.Δ.Α.Ε. που απαρτίζουν την ομάδα ελέγχου. Από την έναρξη του έκτακτου ελέγχου από την Α.Δ.Α.Ε. και μέχρι να λάβει έγγραφη ενημέρωση αναφορικά με το πέρας του ελέγχου, το υπόχρεο πρόσωπο δεν δύναται να προβεί σε οποιαδήποτε αναθεώρηση του κειμένου της εγκριθείσας Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών ή των συνοδευτικών αρχείων αυτής (διαδικασίες, τεχνικές οδηγίες κ.ά.).

14.2.3. Η ομάδα ελέγχου προς εκτέλεση της ως άνω απόφασης της Α.Δ.Α.Ε. δύναται να προβαίνει σε επιτόπιο έλεγχο στις εγκαταστάσεις του υπόχρεου προσώπου.

14.2.4. Για κάθε επιτόπιο έλεγχο συντάσσεται ειδικό έγγραφο με τίτλο «Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις του υπόχρεου προσώπου», το οποίο υπογράφεται από τους εργαζόμενους του ελεγχόμενου προσώπου, οι οποίοι αρμοδίως συνέπραξαν στον επιτόπιο έλεγχο.

14.2.5. Μετά την ολοκλήρωση και των τυχόν επιτόπιων ελέγχων, η ομάδα ελέγχου εξετάζει διεξοδικά το σύνολο των συλλεχθέντων στοιχείων και συντάσσει ειδικό έγγραφο με τίτλο «Έκθεση διενέργειας έκτακτου ελέγχου στο υπόχρεο πρόσωπο», το οποίο περιλαμβάνει απαραιτήτως τα ακόλουθα στοιχεία:

α) Τα στοιχεία της Απόφασης της Α.Δ.Α.Ε. με την οποία αποφασίστηκε η διενέργεια έκτακτου ελέγχου,

β) Το ονοματεπώνυμο και την ιδιότητα των προσώπων που απαρτίζουν την ομάδα ελέγχου και την ημερομηνία σύστασης της τελευταίας,

γ) Την επωνυμία του ελεγχόμενου υπόχρεου προσώπου, καθώς και το όνομα του Υπευθύνου Διασφάλισης του Απορρήτου των Επικοινωνιών,

δ) Τα πρακτικά Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις του ελεγχόμενου προσώπου καθώς και κάθε σχετική έγγραφη επικοινωνία μεταξύ της Α.Δ.Α.Ε. και του ελεγχόμενου προσώπου στο πλαίσιο της διεξαγωγής του έκτακτου ελέγχου,

ε) Αναλυτική περιγραφή των ευρημάτων του ελέγχου και διαπίστωση τυχόν παραλείψεων ή αναντιστοιχιών με

την εγκριθείσα από την Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών,

στ) Την ημερομηνία διενέργειας του επιτόπιου ελέγχου,

ζ) Τελικό πόρισμα του ελέγχου.

14.2.6. Το ελεγχόμενο υπόχρεο πρόσωπο καλείται να παραλάβει από την Α.Δ.Α.Ε. την απόφαση της Ολομέλειας της Α.Δ.Α.Ε. για την έγκριση της «Έκθεσης διενέργειας έκτακτου ελέγχου στο υπόχρεο πρόσωπο» μετά της συνημμένης σε αυτήν έκθεσης.

ΑΡΘΡΟ 15 - Υποχρέωση Ενημέρωσης της Α.Δ.Α.Ε.

15.1 Τα υπόχρεα πρόσωπα του άρθρου 1 παρ.2 του παρόντος Κανονισμού υποχρεούνται εντός προθεσμίας δύο (2) μηνών από τη δημοσίευση του παρόντος στην Εφημερίδα της Κυβερνήσεως, να δηλώσουν προς την Α.Δ.Α.Ε., με υπεύθυνη δήλωση του νομίμου εκπροσώπου τους:

α. Τις δραστηριότητες για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) για τη λειτουργία υπό καθεστώς Γενικής Άδειας.

β. Εάν ασκούν εν τοις πράγμασι τις δραστηριότητες για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην Ε.Ε.Τ.Τ., περιγράφοντας αναλυτικά τις ασκούμενες δραστηριότητες και τα είδη των ΠΕΣ για την άσκηση αυτών των δραστηριοτήτων.

γ. Εάν δεν ασκούν εν τοις πράγμασι δραστηριότητες για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην Ε.Ε.Τ.Τ., επισημαίνοντας εάν τις έχουν ασκήσει στο παρελθόν και για ποιο χρονικό διάστημα.

15.2. Τα υπόχρεα πρόσωπα του άρθρου 1 παρ.2 του παρόντος Κανονισμού οφείλουν να ενημερώνουν αμελλητί την Α.Δ.Α.Ε. σε περίπτωση που επέλθει οποιαδήποτε μεταβολή ως προς τις δραστηριότητες παροχής δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών που ασκούν εν τοις πράγμασι, ανεξαρτήτως της υποβολής αντίστοιχης Δήλωσης Καταχώρησης στην Ε.Ε.Τ.Τ., καθώς και στην περίπτωση που επέλθει μεταβολή στην εταιρική μορφή, στην επωνυμία και στην έδρα τους.

15.3. Τα υπόχρεα πρόσωπα ενημερώνουν αμελλητί την Α.Δ.Α.Ε. σε περίπτωση περιστατικού ασφάλειας, σύμφωνα με το άρθρο 9 του παρόντος Κανονισμού, καθώς και σε κάθε περίπτωση που προβλέπεται ενημέρωση της Αρχής σύμφωνα με την κείμενη νομοθεσία.

ΑΡΘΡΟ 16 - Υποβολή και Υλοποίηση Πολιτικής Ασφάλειας

16.1. Τα υπόχρεα πρόσωπα του άρθρου 1 παρ. 2 του παρόντος Κανονισμού, τα οποία ασκούν εν τοις πράγμασι τις δραστηριότητες για τις οποίες έχουν υποβάλει δήλωση καταχώρησης στην Ε.Ε.Τ.Τ., υποχρεούνται να υποβάλουν στην Α.Δ.Α.Ε. προς έγκριση Πολιτική Ασφάλειας για τη διασφάλιση του Απορρήτου των Επικοινωνιών εντός προθεσμίας έξι (6) μηνών από τη δημοσίευση του παρόντος στην Εφημερίδα της Κυβερνήσεως.

16.2. Τα υπόχρεα πρόσωπα του άρθρου 1 παρ. 2 του παρόντος Κανονισμού, τα οποία ξεκινούν ή μεταβάλλουν την άσκηση δραστηριότητας ή δραστηριοτήτων για τις οποίες έχουν υποβάλει δήλωση καταχώρησης στην Ε.Ε.Τ.Τ. μετά την έναρξη ισχύος του παρόντος Κανονισμού, υποχρεούνται να υποβάλουν στην Α.Δ.Α.Ε. προς έγκριση Πολιτική Ασφάλειας για τη διασφάλιση του Απορρήτου των Επικοινωνιών για τις αντίστοιχες δραστηριότητες εντός προθεσμίας έξι (6) μηνών από την έναρξη των ως άνω δραστηριοτήτων.

16.3. Τα υπόχρεα πρόσωπα του παρόντος άρθρου υποχρεούνται εντός προθεσμίας έξι (6) μηνών από τη γνωστοποίηση σε αυτά της απόφασης της Α.Δ.Α.Ε. περί έγκρισης της Πολιτικής Ασφάλειας για τη διασφάλιση του Απορρήτου των Επικοινωνιών να την υλοποιήσουν. Σε περίπτωση υποβολής αναθεωρημένης Πολιτικής Ασφάλειας για τη διασφάλιση του Απορρήτου των Επικοινωνιών, ο χρόνος υλοποίησής της θα ορίζεται κατά περίπτωση από την Α.Δ.Α.Ε. και θα γνωστοποιείται στο υπόχρεο πρόσωπο με την απόφαση περί έγκρισης της Πολιτικής Ασφάλειας.

16.4. Τα υπόχρεα πρόσωπα του παρόντος άρθρου δεν υποβάλλουν στην Α.Δ.Α.Ε. προς έγκριση τις διαδικασίες ασφάλειας που προβλέπονται στο πλαίσιο του παρόντος Κανονισμού.

ΑΡΘΡΟ 17 - Μεταβατικές Διατάξεις

17.1. Οι υπ' αριθμ. 629α/2004 («Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών» , ΦΕΚ Β΄ 87/2005), 630α/2004 («Κανονισμός για τη Διασφάλιση του Απορρήτου κατά την Παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών», ΦΕΚ Β΄ 87/2005), 631α/2004 («Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Τηλεπικοινωνιακών Υπηρεσιών μέσω Ασυρμάτων Δικτύων», ΦΕΚ Β΄ '87/2005), 632α/2005 («Κανονισμός για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές», ΦΕΚ Β΄ 88/2005), 633α/2005 («Κανονισμός για την Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών», ΦΕΚ Β΄ 88/2005), και 634α/2005 («Κανονισμός για την Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου», ΦΕΚ Β΄ 88/2005) Αποφάσεις της Α.Δ.Α.Ε. παραμένουν σε ισχύ μέχρι την έναρξη ισχύος του παρόντος Κανονισμού.

17.2. Τα υπόχρεα πρόσωπα που έχουν υποβάλει στην Α.Δ.Α.Ε. Πολιτική Ασφάλειας σε εκπλήρωση της σχετικής υποχρέωσής τους με βάση τους καταργούμενους διά του παρόντος Κανονισμούς της Α.Δ.Α.Ε., υποχρεούνται, χωρίς άλλη ειδοποίηση, να υποβάλουν στην Α.Δ.Α.Ε. προς έγκριση Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των επικοινωνιών σύμφωνα με τις απαιτήσεις του παρόντος Κανονισμού.

17.3. Τα υπόχρεα πρόσωπα του παρόντος άρθρου εφαρμόζουν την πολιτική ασφάλειας που έχουν υποβάλει στην Α.Δ.Α.Ε. σε εκπλήρωση της σχετικής υποχρέωσής τους με βάση τους καταργούμενους διά του παρόντος Κανονισμούς της Α.Δ.Α.Ε., μέχρι την υλοποίηση της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των επικοινωνιών όπως εγκρίνεται από την Α.Δ.Α.Ε. σύμφωνα με τον παρόντα Κανονισμό και, σε κάθε περίπτωση, το αργότερο μέχρι το πέρας της οριζόμενης στο άρθρο 16.3 του παρόντος Κανονισμού προθεσμίας υλοποίησης της Πολιτικής Ασφάλειας για τη διασφάλιση του Απορρήτου των Επικοινωνιών.

ΑΡΘΡΟ 18 - Έναρξη Ισχύος

Η ισχύς του παρόντος Κανονισμού αρχίζει 6 μήνες μετά τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως, υπό την επιφύλαξη των διατάξεων των άρθρων 15 παρ. 1 και 16 παρ. 1 αυτού.

Ο παρών Κανονισμός να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Μαρούσι, 10 Νοεμβρίου 2011

Ο Πρόεδρος

ΑΝΔΡΕΑΣ ΛΑΜΠΡΙΝΟΠΟΥΛΟΣ

ΑΠΟ ΤΟ ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ
ΚΑΠΟΔΙΣΤΡΙΟΥ 34 * ΑΘΗΝΑ 104 32 * ΤΗΛ. 210 52 79 000 * FAX 210 52 21 004