ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)

Έχοντας υπόψη:

1. Τις διατάξεις:

   α. του ν. 3115/2003 «Αρχή διασφάλισης του Απορρήτου των Επικοινωνιών», (ΦΕΚ Α' 47/2003), όπως ισχύει, ιδίως τη διάταξη του άρθρου 6 παρ. 1 αυτού,

   β. του ν. 4727/2020 «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας ΕΕ 2016/2102 και της Οδηγίας 2019/1024) – Ηλεκτρονικές επικοινωνίες (Ενσωμάτωση στο ελληνικό δίκαιο της Οδηγίας ΕΕ 2018/1972) και άλλες διατάξεις», (ΦΕΚ Α' 184/2020), όπως ισχύει, ιδίως τις διατάξεις των άρθρων 148 και 149 αυτού,

   γ. του ν. 3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (ΦΕΚ Α' 136/2008), όπως ισχύει, ιδίως τις διατάξεις του άρθρου 4 παρ. 4 και του άρθρου 5 αυτού,

   δ. του ν. 3959/2011 «Προστασία του ελεύθερου ανταγωνισμού» (ΦΕΚ Α' 93/2011), όπως ισχύει,

   ε. του ν. 3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997» (ΦΕΚ Α' 133/2006), όπως ισχύει,

   στ. της υπ' αριθμ. 165/2011 Απόφασης της ΑΔΑΕ (Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών), (ΦΕΚ Β' 2715/2011), όπως ισχύει,

   ζ. της υπ' αριθμ. 205/2013 Απόφασης της ΑΔΑΕ (Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών), (ΦΕΚ Β' 1742/2013), όπως ισχύει,

   η. της υπ' αριθμ. 991/4/2021 Απόφασης της ΕΕΤΤ (Κανονισμός Γενικών Αδειών), (ΦΕΚ Β' 2265/2021), όπως ισχύει,

2. Την υπ' αριθμ. 251/2022 Απόφαση της ΑΔΑΕ με θέμα: «Σύσταση Ομάδας Εργασίας για την τροποποίηση των Αποφάσεων 165/2011 και 205/2013 της ΑΔΑΕ,
3. Τη διαπίστωση της ανάγκης αναθεώρησης των ως άνω υπ' αριθμ. 165/2011 και 205/2013 Αποφάσεων της Αρχής, ενόψει και της ενσωμάτωσης της Οδηγίας 2018/1972 με το ν. 4727/2020 προς την κατεύθυνση της ενοποίησης των εν λόγω δύο υφιστάμενων κανονιστικών πλαισίων,
4. Τις απαντήσεις των ενδιαφερόμενων μερών, όπως διατυπώθηκαν στο πλαίσιο της δημόσιας διαβούλευσης , η οποία έλαβε χώρα κατά το χρονικό διάστημα από ……,
5. Τα πρακτικά των συνεδριάσεων …..της Ολομέλειας της ΑΔΑΕ,
6. Το γεγονός ότι δεν προκαλείται 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:

ΜΕΡΟΣ Α – ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

ΑΡΘΡΟ 1 – Σκοπός - Πεδίο Εφαρμογής

1.1. Με τον παρόντα Κανονισμό καθορίζονται τα τεχνικά και οργανωτικά μέτρα που πρέπει να λαμβάνουν όλα τα πρόσωπα που παρέχουν δημόσια δίκτυα ηλεκτρονικών επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών (εφεξής καλούμενοι για λόγους συντομίας «οι πάροχοι»), για τη διασφάλιση του απορρήτου των επικοινωνιών και την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών, σύμφωνα με τα οριζόμενα στο άρθρο 148 του ν. 4727/2020. Τα μέτρα αυτά πρέπει να εξασφαλίζουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα και το απόρρητο των δικτύων και των υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία μέσω αυτών, σύμφωνα με την κείμενη νομοθεσία.

1.2. Οι πάροχοι υποχρεούνται να διαθέτουν και να εφαρμόζουν Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών (Networks and Services Security Policy), της οποίας το περιεχόμενο είναι σύμφωνο με τις διατάξεις του παρόντος Κανονισμού.

1.3. Οι πάροχοι που λειτουργούν υπό καθεστώς Γενικής Άδειας, όπως αυτό καθορίζεται από την εκάστοτε ισχύουσα νομοθεσία, υποχρεούνται να υποβάλλουν στην ΑΔΑΕ προς έγκριση την προβλεπόμενη στην προηγούμενη παράγραφο Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών, καθώς και κάθε αναθεώρηση αυτής, όποτε αυτή λαμβάνει χώρα. Εξαιρούνται της υποχρέωσης υποβολής προς έγκριση στην ΑΔΑΕ της εφαρμοζόμενης Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών οι πάροχοι που παρέχουν τις ακόλουθες κατηγορίες δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, όπως προβλέπονται στον Κανονισμό Γενικών Αδειών της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων, όπως εκάστοτε ισχύει:

α) S014: Υπηρεσίες μηχανή με μηχανή (M2M)

β) S015: Δορυφορική συλλογή ειδήσεων (Satellite News Gathering)

γ) S016: Επίγεια συλλογή ειδήσεων (ENG)

δ) S025: Υπηρεσίες ραδιοεπικοινωνιών, όπως τηλεματικής, τηλεμετρίας, ραδιοεντοπισμού

ε) N010: Δίκτυο μετάδοσης σημάτων επίγειας ψηφιακής ευρυεκπομπής, με χρήση ραδιοσυχνοτήτων για την εκπομπή τηλεοπτικού σήματος

ΑΡΘΡΟ 2 – Ορισμοί

Για τους σκοπούς του παρόντος Κανονισμού νοούνται ως:

«Ασφάλεια Δικτύων και Υπηρεσιών (Networks and Services Security)»: η ικανότητα δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών να ανθίστανται, σε δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των εν λόγω δικτύων και υπηρεσιών, των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών.

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

«Περιστατικό Ασφάλειας (Security Incident)»: κάθε συμβάν το οποίο έχει αρνητική επίπτωση στην ασφάλεια των δικτύων ή των υπηρεσιών ηλεκτρονικών επικοινωνιών, με εξαίρεση τις προγραμματισμένες εργασίες συντήρησης ή αναβάθμισης συστημάτων, οι οποίες επηρεάζουν τη λειτουργία των δικτύων και υπηρεσιών, στον βαθμό που αυτές υλοποιούνται σύμφωνα με προγραμματισμένο από τον πάροχο χρονοδιάγραμμα, κάθε περίπτωση παραβίασης ή ιδιαίτερου κινδύνου παραβίασης του απορρήτου των επικοινωνιών και κάθε περίπτωση μη εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών του παρόχου.

«Πληροφοριακά και Επικοινωνιακά Συστήματα (ΠΕΣ) (Information and Communication Systems)»: Ως ΠΕΣ νοούνται:

(α) Τα συστήματα (υλικό και λογισμικό, φυσικά ή εικονικά), με τα οποία πραγματοποιείται η παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών ή/και με τα οποία πραγματοποιούνται εργασίες σε δεδομένα επικοινωνίας.

(β) Τα συστήματα που χρησιμοποιούνται για την υποστήριξη, διαχείριση, εποπτεία, λειτουργία, έλεγχο πρόσβασης και ασφάλεια των ως άνω υπό σημείο (α) συστημάτων.

(γ) Τα συστήματα που περιέχουν πληροφορίες που είναι απαραίτητες για την πραγματοποίηση εργασιών στα ως άνω υπό σημείο (α) συστήματα ή σε δεδομένα επικοινωνίας.

Με βάση τα ανωτέρω, στα ΠΕΣ περιλαμβάνονται, κατ' ελάχιστον, τα μέσα μετάδοσης και διασύνδεσης, οι μεταγωγείς, οι δρομολογητές, συμπεριλαμβανομένων των οικιακών δρομολογητών στο μέτρο κατά το οποίο αυτοί είναι υπό τη διαχειριστική εποπτεία των παρόχων, τα συστήματα για την πρόσβαση στο Διαδίκτυο, τα συστήματα διαχείρισης και εποπτείας, οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου, τα συστήματα για την άρση του απορρήτου των επικοινωνιών (συστήματα νόμιμης επισύνδεσης και διατήρησης δεδομένων), τα συστήματα ελέγχου φυσικής και λογικής (τοπικής και απομακρυσμένης) πρόσβασης, τα τείχη προστασίας (firewalls), τα συστήματα ανίχνευσης/αποτροπής εισβολών, τα συστήματα ανίχνευσης κακόβουλου λογισμικού και ανεπιθύμητης αλληλογραφίας, τα συστήματα καταγραφής και διατήρησης αρχείων καταγραφής, τα συστήματα χρέωσης συνδρομητών, τα συστήματα πωλήσεων και εξυπηρέτησης πελατών, τα συστήματα πρόληψης τηλεπικοινωνιακής απάτης, οι βάσεις δεδομένων που περιέχουν δεδομένα επικοινωνίας ή πληροφορίες σχετικές με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών και τα συστήματα επεξεργασίας αυτών των δεδομένων ή πληροφοριών.

Κατά τα λοιπά, ισχύουν οι ορισμοί που περιλαμβάνονται στο άρθρο 110 του ν. 4727/2020 («Ψηφιακή διακυβέρνηση – Ηλεκτρονικές Επικοινωνίες και άλλες διατάξεις», ΦΕΚ Α'184/2020), όπως ισχύει.

ΜΕΡΟΣ Β – Περιεχόμενο Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών

ΑΡΘΡΟ 3 – Διακυβέρνηση Πολιτικής Ασφάλειας και Διαχείριση Κινδύνου

3.1. Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών

3.1.1. Η Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών αφορά τους χρήστες, συνδρομητές, εργαζόμενους και συνεργάτες του παρόχου, έχει ως σκοπό τον καθορισμό και την υλοποίηση, από τον πάροχο, των κατάλληλων τεχνικών και οργανωτικών μέτρων για την επίτευξη του σκοπού της ασφάλειας δικτύων και υπηρεσιών του και εφαρμόζεται σε όλα τα ΠΕΣ, όπως ορίζονται ανωτέρω.

3.1.2. Η Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών έχει αρθρωτή δομή και αποτελείται από επιμέρους ενότητες, οι οποίες ορίζουν τις απαιτήσεις ασφάλειας που πρέπει να ικανοποιούνται για κάθε επιμέρους κατηγορία ειδικών θεμάτων.

3.1.3. Σε περίπτωση που η Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών εντάσσεται σε ευρύτερη πολιτική ασφάλειας πληροφοριών και επικοινωνιών του παρόχου, αυτός διαθέτει αρχείο με αναλυτική αντιστοίχιση της δομής της ευρύτερης πολιτικής ασφάλειας πληροφοριών και επικοινωνιών με τις απαιτήσεις του παρόντος Κανονισμού. Οι πάροχοι της παραγράφου 1.3 του άρθρου 1 του παρόντος Κανονισμού υποβάλλουν στην ΑΔΑΕ το εν λόγω αρχείο αντιστοίχισης μαζί με την υποβολή προς έγκριση της Πολιτικής τους.

3.1.4. Κάθε αδυναμία συμμόρφωσης με τις απαιτήσεις που ορίζονται στον παρόντα Κανονισμό καταγράφεται και τεκμηριώνεται επαρκώς στην Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών. Ειδικά για τις αδυναμίες συμμόρφωσης που οφείλονται σε τεχνική αδυναμία κάλυψης συγκεκριμένων απαιτήσεων, ο πάροχος καταγράφει, επιπλέον, τις προϋποθέσεις και τις ενέργειες για την κάλυψη αυτών των απαιτήσεων και άρση της αδυναμίας, καθώς και το σχετικό χρονοδιάγραμμα προς τον σκοπό αυτόν.

3.1.5. Για την υλοποίηση των επιμέρους απαιτήσεων της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών, ορίζονται, τεκμηριώνονται, εφαρμόζονται και αναθεωρούνται συγκεκριμένες διαδικασίες ασφάλειας, οδηγίες εργασίας, τεχνικά και άλλα οργανωτικά εγχειρίδια. Τα παραπάνω έγγραφα ορίζουν συγκεκριμένες ενέργειες των εργαζομένων, συνεργατών, χρηστών και συνδρομητών του παρόχου, την αλληλουχία των ενεργειών, τους υπεύθυνους για την εκτέλεσή τους και τον τρόπο και τα μέσα τεκμηρίωσής τους.

3.1.6. Ο πάροχος εξετάζει περιοδικά, κατ’ ελάχιστον κάθε δύο (2) έτη ή μετά από την εκδήλωση σημαντικού περιστατικού ασφάλειας, την ανάγκη τυχόν αναθεώρησης της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών και αποφασίζει σχετικώς, λαμβάνοντας υπόψη κατ’ ελάχιστον τα αποτελέσματα της Αποτίμησης Κινδύνου, τα αποτελέσματα του εσωτερικού ελέγχου και των δοκιμών ασφάλειας στις οποίες έχει προβεί, τα περιστατικά ασφάλειας που τυχόν έχει αντιμετωπίσει, και τις επιχειρησιακές και οργανωτικές αλλαγές που τυχόν έχουν προκύψει. Σε περίπτωση που ο πάροχος αποφασίσει ότι η Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών δεν χρειάζεται αναθεώρηση, τεκμηριώνει εγγράφως την απόφαση αυτή, ενώ, σε περίπτωση που ο πάροχος προβεί σε αναθεώρηση της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών, την υποβάλλει προς έγκριση στην ΑΔΑΕ, σύμφωνα με τα προβλεπόμενα στο άρθρο 13 του παρόντος Κανονισμού.

3.2. Διαχείριση Κινδύνου (Risk Management)

3.2.1. Ο πάροχος διατηρεί και εφαρμόζει Διαδικασία Αποτίμησης Κινδύνου (Risk Assessment) σχετικά με την ασφάλεια δικτύων και υπηρεσιών, βασισμένη σε μεθοδολογία που λαμβάνει υπόψη διεθνείς πρακτικές, με σκοπό την αναγνώριση, την αξιολόγηση και αντιμετώπιση των απειλών (threats) στην ασφάλεια των δικτύων και υπηρεσιών του.

3.2.2. Ο πάροχος αναγνωρίζει και εξετάζει ενδογενείς και εξωγενείς απειλές, όπως, ενδεικτικά αποτελούν οι αστοχίες υλικού και λογισμικού, η πλημμελής εφαρμογή της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών και των συναφών διαδικασιών, οι πράξεις ή παραλείψεις εργαζομένων και συνεργατών, οι απειλές προερχόμενες από άλλα διασυνδεδεμένα δίκτυα, οι κακόβουλες ενέργειες και οι πράξεις δολιοφθοράς, τα ατυχήματα και τα φυσικά φαινόμενα.

3.2.3. Η Αποτίμηση Κινδύνου περιλαμβάνει κατ' ελάχιστον τα παρακάτω:

3.2.3.1. Ο πάροχος καταρτίζει και διατηρεί κατάλογο των πόρων του (ΠΕΣ, εγκαταστάσεις, διαδικασίες, προσωπικό), με συνοπτική περιγραφή τους.

3.2.3.2. Ο πάροχος καταρτίζει και διατηρεί κατάλογο με τις διαφορετικές εκτιμώμενες απειλές που μπορούν να εκδηλωθούν σε πόρους του, καθώς και τις ευπάθειες (vulnerabilities), τα ευάλωτα σημεία και τις αδυναμίες των πόρων του. Επιπρόσθετα, ταξινομεί τους πόρους του ως προς την κρισιμότητά τους, λαμβάνοντας υπόψη τις απειλές που μπορεί να τους επηρεάσουν.

3.2.3.3. Ο πάροχος πραγματοποιεί αξιολόγηση επικινδυνότητας (risk evaluation), ήτοι αξιολογεί την πιθανότητα πραγματοποίησης των απειλών που έχει αναγνωρίσει και εκτιμά την επίδρασή τους στην ασφάλεια των δικτύων και υπηρεσιών του.

3.2.3.4. Ο πάροχος καθορίζει τα κατάλληλα μέτρα ασφάλειας για την αντιμετώπισή των απειλών, συμπληρωματικά ως προς τα μέτρα ασφάλειας που ορίζονται από τον παρόντα Κανονισμό, το χρονοδιάγραμμα υλοποίησης αυτών, καθώς και διαδικασίες αξιολόγησης της αποτελεσματικότητας των επιλεγέντων μέτρων.

3.2.4. Η Αποτίμηση Κινδύνου πραγματοποιείται από τον πάροχο πριν τη σύνταξη της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών και εφεξής, κατ' ελάχιστον κάθε ένα (1) έτος. Για την αναθεώρηση της Αποτίμησης Κινδύνου λαμβάνονται υπόψη: (α) η αποτελεσματικότητα των εφαρμοζόμενων μέτρων, (β) η αναγνώριση νέων απειλών, (γ) η καταγραφή νέων ευπαθειών των ΠΕΣ, (δ) οργανωτικές ή τεχνολογικές αλλαγές, (ε) αλλαγές στο νομοθετικό πλαίσιο, σε εθνικό ή κοινοτικό επίπεδο, (στ) τα αποτελέσματα των ελέγχων που πραγματοποιούνται από τις Ελεγκτικές Αρχές και τις σχετικές υποδείξεις τους και (ζ) κάθε άλλο νέο στοιχείο που πρέπει να λάβει υπόψη του ο πάροχος.

3.2.5. Ο πάροχος διατηρεί καταγεγραμμένη την περιγραφή της εφαρμοσθείσας μεθοδολογίας Αποτίμησης Κινδύνου, καθώς και τα αποτελέσματα της Αποτίμησης Κινδύνου (τα στοιχεία της παραγράφου 3.2.3 του παρόντος άρθρου). Όλα τα ανωτέρω είναι διαθέσιμα κατά τον τακτικό ή έκτακτο έλεγχο της εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών από την ΑΔΑΕ.

3.3. Ρόλοι και Αρμοδιότητες

3.3.1. Ο πάροχος ορίζει, στην Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών, τις διοικητικές οντότητες και τα φυσικά πρόσωπα στα οποία ανατίθενται συγκεκριμένες αρμοδιότητες σχετικά με τη διαχείριση

και εφαρμογή της Πολιτικής. Ο πάροχος αναθέτει τους ρόλους και τις αρμοδιότητες στους εργαζόμενους ή συνεργάτες του, και διατηρεί σχετικό αρχείο με τις εν λόγω αναθέσεις.

3.3.2. Ο πάροχος ορίζει συγκεκριμένο εργαζόμενό του, ως Υπεύθυνο Ασφάλειας Δικτύων και Υπηρεσιών, επιφορτισμένο με την ευθύνη ελέγχου της υλοποίησης των μέτρων και των απαιτήσεων που ορίζονται στην Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών. Οι πάροχοι της παραγράφου 1.3 του άρθρου 1 του παρόντος Κανονισμού κοινοποιούν στην ΑΔΑΕ τα στοιχεία του εκάστοτε Υπεύθυνου Ασφάλειας Δικτύων και Υπηρεσιών (ονοματεπώνυμο, ΑΔΤ, διεύθυνση, τηλέφωνο επικοινωνίας, διεύθυνση ηλεκτρονικού ταχυδρομείου), ιδιαιτέρως δε κατά την υποβολή της Πολιτικής προς έγκριση, καθώς και σε κάθε μεταβολή αυτού.

3.3.3. Ο πάροχος επανεξετάζει περιοδικά, κατ' ελάχιστον κάθε δύο (2) έτη, τις αναθέσεις ρόλων και αρμοδιοτήτων, σύμφωνα με τους όρους και τις προϋποθέσεις της παραγράφου 3.1.6 του παρόντος άρθρου, και διατηρεί εγγράφως τη σχετική τεκμηρίωση.

3.4. Υποχρεώσεις του Παρόχου σχετικά με τους Συνεργάτες

3.4.1. Ο πάροχος ευθύνεται για το σύνολο των πράξεων οποιουδήποτε συνεργάτη, φυσικού ή νομικού προσώπου, τους οποίους χρησιμοποιεί στο πλαίσιο της παροχής των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών του.

3.4.2. Ο πάροχος διατηρεί ενημερωμένο αρχείο στο οποίο καταγράφονται οι συνεργάτες του, φυσικά ή νομικά πρόσωπα, τους οποίους χρησιμοποιεί στο πλαίσιο της παροχής των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών. Σε ειδικό πεδίο του αρχείου της παρούσας παραγράφου καταγράφονται εκείνοι οι συνεργάτες που, προκειμένου να παράσχουν τις υπηρεσίες τους, αποκτούν ή δύνανται να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών, καθώς και οι συνεργάτες που κατέχουν ή διαχειρίζονται ΠΕΣ μέσω των οποίων πραγματοποιείται, αποκλειστικά ή εν μέρει, η παροχή των υπηρεσιών του παρόχου.

3.4.3. Ο πάροχος συνάπτει με τους συνεργάτες της προηγούμενης παραγράφου, συμβάσεις, των οποίων το ελάχιστο περιεχόμενο περιλαμβάνει:

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

3.4.3.2. Απαιτήσεις και μέτρα ασφάλειας που λαμβάνονται για την ασφάλεια των δικτύων και υπηρεσιών του, και επιπρόσθετα, ειδικότερα, μέτρα με τα οποία διασφαλίζεται η εμπιστευτικότητα και ακεραιότητα των δεδομένων επικοινωνίας κατά την επεξεργασία αυτών από τους συνεργάτες του παρόχου, καθώς και η οριστική διαγραφή και καταστροφή αυτών μετά τη λήξη της συνεργασίας.

3.4.3.3. Αποδοχή εκ μέρους των συνεργατών της υποχρέωσης για τήρηση των μέτρων ασφάλειας, που αναφέρονται στην παράγραφο 3.4.3.2 του παρόντος άρθρου.

3.4.3.4. Στην περίπτωση που οι συνεργάτες χρησιμοποιούν τρίτα πρόσωπα προκειμένου να παρέχουν τις υπηρεσίες τους στον πάροχο, τότε στις συμβάσεις τους με τον πάροχο περιλαμβάνεται όρος που προβλέπει την εν λόγω δυνατότητα, καθώς και την παροχή προηγούμενης έγγραφης έγκρισης του παρόχου για την πραγματοποίηση της εκάστοτε εργασίας από το τρίτο πρόσωπο.

3.4.4. Στην περίπτωση κατά την οποία οι συνεργάτες της παραγράφου 3.4.2 του παρόντος άρθρου κατέχουν ή διαχειρίζονται ΠΕΣ μέσω των οποίων πραγματοποιείται, αποκλειστικά ή εν μέρει, η παροχή των υπηρεσιών του παρόχου, τότε ο πάροχος περιλαμβάνει στις συμβάσεις της παραγράφου 3.4.3 του παρόντος άρθρου, την υποχρέωση συμμόρφωσης των εν λόγω συνεργατών με το σύνολο των απαιτήσεων του παρόντος Κανονισμού.

3.4.5. Ο πάροχος ενεργοποιεί τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με την ενότητα 7.1 του άρθρου 7 του παρόντος Κανονισμού, για κάθε παραβίαση των συμβατικών όρων που αναφέρονται στην παράγραφο 3.4.3 του παρόντος άρθρου.

ΑΡΘΡΟ 4 – Μέτρα σχετικά με τους Εργαζόμενους και τους Συνεργάτες

4.1. Εκπαίδευση και Ενημέρωση

4.1.1. Ο πάροχος ενημερώνει και εκπαιδεύει τους εργαζόμενους και συνεργάτες του ως προς την εφαρμογή της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών και επισημαίνει τους κινδύνους που ελλοχεύουν από τυχόν παραβίασή της.

4.1.2. Η ενημέρωση και η εκπαίδευση των εργαζόμενων και συνεργατών διενεργείται σε τακτά χρονικά διαστήματα, κατ' ελάχιστον μία φορά τον χρόνο, με σκοπό την προσήκουσα επιμόρφωσή τους.

4.1.3. Ο πάροχος διατηρεί αρχείο εκπαιδεύσεων στο οποίο αναγράφονται κατ' ελάχιστον αναλυτικά ο χρόνος και η διάρκεια εκπαίδευσης, το εκπαιδευτικό υλικό, τα στοιχεία των εκπαιδευτών και η αξιολόγηση κάθε εκπαιδευόμενου.

4.1.4. Σε περίπτωση τροποποίησης της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών ή των διαδικασιών, τεχνικών οδηγιών ή άλλων δευτερογενών εγγράφων που σχετίζονται με την υλοποίησή της, ο πάροχος προβαίνει αμελλητί σε ενημέρωση των εργαζόμενων και συνεργατών του και διατηρεί εγγράφως τη σχετική τεκμηρίωση πραγματοποίησης της ενημέρωσης.

4.2. Διαχείριση Μεταβολών Εργαζομένων και Συνεργατών

4.2.1. Σε περίπτωση πρόσληψης ή μεταβολής των καθηκόντων εργαζόμενου ή συνεργάτη, ο πάροχος προβαίνει στην ενημέρωση και εκπαίδευσή του ως προς την εφαρμογή της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών.

4.2.2. Σε περίπτωση μεταβολής των καθηκόντων ή αποχώρησης εργαζόμενου ή συνεργάτη, ο πάροχος προβαίνει αμελλητί στην αντίστοιχη τροποποίηση τυχόν δικαιωμάτων που του έχουν αποδοθεί λόγω της φύσης της εργασίας του σύμφωνα με τις απαιτήσεις της εφαρμοζόμενης Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών (πχ. κάρτα εισόδου σε εγκατάσταση, πρόσβαση σε συστήματα ή δεδομένα κ.λπ.).

4.3. Υποχρεώσεις Εργαζομένων και Συνεργατών

4.3.1. Οι εργαζόμενοι και συνεργάτες του παρόχου οφείλουν να συμμορφώνονται με την Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών, συμπεριλαμβανομένων των σχετικών διαδικασιών, μέτρων ασφάλειας και οδηγιών. Για τον σκοπό αυτό, ο πάροχος καταγράφει στην Πολιτική τον τρόπο με

τον οποίο εξασφαλίζει ότι οι εργαζόμενοι και συνεργάτες του λαμβάνουν γνώση και έχουν αποδεχτεί την Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών ως προς την εργασία τους, προ της απόκτησης πρόσβασης σε ΠΕΣ και σε δεδομένα επικοινωνίας.

4.3.2. Οι εργαζόμενοι και συνεργάτες του παρόχου, εφόσον αντιληφθούν κάποιο κενό ασφάλειας ή περιστατικό ασφάλειας, ενημερώνουν άμεσα τον Υπεύθυνο Ασφάλειας Δικτύων και Υπηρεσιών ή άλλο, ρητά εξουσιοδοτημένο για τον σκοπό αυτό, πρόσωπο.

ΑΡΘΡΟ 5 – Ασφάλεια Εγκαταστάσεων και Συστημάτων

5.1. Φυσική Πρόσβαση και Περιβαλλοντική Ασφάλεια

Α. Φυσική Πρόσβαση

5.1.1. Ο πάροχος καθορίζει τα απαιτούμενα μέτρα (α) για την αποτροπή της μη εξουσιοδοτημένης φυσικής πρόσβασης στις εγκαταστάσεις του στις οποίες είναι εγκατεστημένα ΠΕΣ, εξαιρουμένων εκείνων που χρησιμοποιούνται αποκλειστικά για την εξυπηρέτηση του κοινού, (β) για τον έλεγχο της πρόσβασης στις εγκαταστάσεις του και (γ) για την προστασία των ΠΕΣ.

5.1.2. Ο πάροχος διαθέτει και εφαρμόζει διαδικασία φυσικής πρόσβασης, στην οποία περιγράφονται αναλυτικά όλες οι ενέργειες που απαιτούνται για την πρόσβαση των εργαζομένων, συνεργατών και επισκεπτών του σε εγκαταστάσεις και σε χώρους εντός των εγκαταστάσεών του, όπου είναι εγκατεστημένα ΠΕΣ.

5.1.3. Για την παροχή εξουσιοδότησης φυσικής πρόσβασης στους εργαζόμενους ή τους συνεργάτες του παρόχου σε εγκαταστάσεις και σε χώρους εντός των εγκαταστάσεών του όπου είναι εγκατεστημένα ΠΕΣ, προβλέπεται υποχρεωτικά προηγούμενη έγκριση από την αρμόδια διοικητική οντότητα ή το αρμόδιο φυσικό πρόσωπο. Ο πάροχος διατηρεί αρχείο με το ιστορικό όλων των φυσικών προσβάσεων που έχουν εγκριθεί, στο οποίο καταγράφονται όλα τα στοιχεία που αφορούν εκάστη έγκριση (ενδεικτικά, χρονικό διάστημα, εγκατάσταση ή χώρο, είδος δικαιώματος πρόσβασης).

5.1.4. Η φυσική πρόσβαση των εξουσιοδοτημένων προσώπων στις εγκαταστάσεις του παρόχου καταγράφεται (ονοματεπώνυμο, ιδιότητα, ώρα εισόδου και εξόδου) σε σχετικό αρχείο. Σε περίπτωση πρόσβασης συνεργάτη του παρόχου 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.

5.1.5. Ο πάροχος ορίζει ασφαλείς χώρους εντός των εγκαταστάσεών του, στους οποίους εγκαθίστανται τα ΠΕΣ. Οι χώροι αυτοί προστατεύονται με ισχυρούς μηχανισμούς ασφάλειας (ενδεικτικά, συστήματα άμεσης ανίχνευσης μη εξουσιοδοτημένης πρόσβασης και ειδοποίησης, συστήματα βιντεοεπιτήρησης) και ελέγχου πρόσβασης (ενδεικτικά, κάρτες ελεγχόμενης εισόδου) τηρουμένης της κείμενης νομοθεσίας περί προστασίας δεδομένων προσωπικού χαρακτήρα. Η φυσική πρόσβαση στους χώρους της παρούσας παραγράφου καταγράφεται σύμφωνα με τις απαιτήσεις της παραγράφου 5.1.4 του παρόντος άρθρου. Οι χώροι της παρούσας παραγράφου, καθώς και οι μηχανισμοί ασφάλειας και ελέγχου πρόσβασης, καταγράφονται σε αρχείο.

5.1.6. Ο πάροχος λαμβάνει όλα τα απαραίτητα μέτρα φυσικής προστασίας και ελέγχου πρόσβασης για την προστασία των ΠΕΣ, τα οποία βρίσκονται υπό την εποπτεία του και τοποθετούνται εκτός

των εγκαταστάσεών του. Στα ΠΕΣ αυτής της κατηγορίας περιλαμβάνεται ο εξοπλισμός που είναι εγκατεστημένος σε υπαίθριες κατασκευές (ενδεικτικά καμπίνες), σε εγκαταστάσεις άλλης εταιρείας και σε άλλους ιδιωτικούς ή δημόσιους χώρους, εντός ή εκτός της Ελληνικής επικράτειας. Οι μηχανισμοί ασφάλειας για τις περιπτώσεις αυτές περιγράφονται σε αρχείο.

Β. Περιβαλλοντική Ασφάλεια

5.1.7. Ο πάροχος καθορίζει τα απαιτούμενα μέτρα για την προστασία από φυσικές καταστροφές που προκαλούνται από φαινόμενα όπως σεισμός, υγρασία, πλημμύρες, υπερθέρμανση, φωτιά, κεραυνός.

5.1.8. Ο πάροχος λαμβάνει υπόψη του, κατά την επιλογή ή κατασκευή των εγκαταστάσεων στους οποίους εγκαθιστά ΠΕΣ, καθώς και κατά την τοποθέτηση εξοπλισμού και την υλοποίηση μέτρων φυσικής προστασίας, τις ιδιαίτερες φυσικές και άλλες συνθήκες οι οποίες επικρατούν στην περιοχή. Ενδεικτικά αναφέρονται τα ακόλουθα μέτρα: ανιχνευτής φωτιάς, θερμοκρασίας και υγρασίας.

5.1.9. Ο πάροχος επιλέγει, όπου είναι τεχνικά εφικτό, την υπόγεια εγκατάσταση καλωδίων σε σχέση με την εναέρια εγκατάσταση.

5.1.10. Ο πάροχος συνεργάζεται με τις υπηρεσίες οι οποίες ενδεχομένως εκτελούν εργασίες δημόσιου ενδιαφέροντος, όπως, ενδεικτικά, έργα οδοποιίας ή αποχέτευσης, με στόχο την ελαχιστοποίηση της πιθανότητας ζημίας στα ΠΕΣ.

5.1.11. Ο πάροχος μεριμνά για την τακτική συντήρηση των εγκαταστάσεων στις οποίες είναι εγκατεστημένα ΠΕΣ.

5.2. Ασφάλεια Λογικής Πρόσβασης

Α. Λογική Πρόσβαση στα ΠΕΣ

5.2.1. Ο πάροχος καθορίζει τη διαβάθμιση των επιπέδων πρόσβασης και θέτει τις απαιτήσεις για τον έλεγχο πρόσβασης στα ΠΕΣ.

5.2.2. Οι απαιτήσεις της λογικής πρόσβασης ισχύουν για τους εργαζόμενους και συνεργάτες του παρόχου, οι οποίοι στο πλαίσιο της εργασίας τους αποκτούν πρόσβαση στα ΠΕΣ και στα σχετικά δεδομένα και τις πληροφορίες. Η λογική πρόσβαση των εργαζομένων και συνεργατών περιορίζεται στις περιπτώσεις που αυτό είναι απαραίτητο για τις επιχειρησιακές ανάγκες του παρόχου.

5.2.3. Για την απόκτηση πρόσβασης στα ΠΕΣ χρησιμοποιούνται κατάλληλοι μηχανισμοί ελέγχου πρόσβασης και αυθεντικοποίησης. Ο έλεγχος της πρόσβασης και της αυθεντικοποίησης επιτυγχάνεται κατ' ελάχιστον με τη χρήση ενός λογαριασμού πρόσβασης που αποτελείται από ένα ζεύγος ονόματος χρήστη και κωδικού πρόσβασης, ή άλλου μηχανισμού που εξασφαλίζει αντίστοιχο επίπεδο ασφάλειας. Επιπλέον, για τα κρίσιμα ΠΕΣ, όπως αυτά έχουν αποτυπωθεί στην Αποτίμηση Κινδύνου στην οποία έχει προβεί ο πάροχος, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού, καθώς και για τους χρήστες με αυξημένα δικαιώματα διαχείρισης (διαχειριστές) των λοιπών ΠΕΣ, ο πάροχος υλοποιεί λύσεις ελέγχου πρόσβασης και αυθεντικοποίησης δύο παραγόντων (two-factor authentication). Ο πάροχος διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης για κάθε ΠΕΣ.

5.2.4. Σε κάθε εργαζόμενο και συνεργάτη του παρόχου εκχωρείται προσωπικός λογαριασμός πρόσβασης ανά ΠΕΣ, ώστε να είναι δυνατή η αντιστοίχιση συγκεκριμένου προσώπου με τις ενέργειες που τελούνται σε κάθε ΠΕΣ. Ο πάροχος διατηρεί αρχείο με την αντιστοίχιση των λογαριασμών πρόσβασης των εργαζόμενων και συνεργατών στους οποίους αυτοί έχουν αποδοθεί, ώστε να είναι δυνατό να διαπιστώνεται με βεβαιότητα ποιος είναι ο κάτοχος κάθε λογαριασμού πρόσβασης και για ποιο χρονικό διάστημα.

5.2.5. Αναφορικά με τους λογαριασμούς πρόσβασης ισχύουν τα εξής:

5.2.5.α. Αποφεύγεται η δημιουργία κοινών λογαριασμών πρόσβασης. Σε περίπτωση που η δημιουργία τέτοιων λογαριασμών κρίνεται απαραίτητη, δικαιολογείται και τεκμηριώνεται η σχετική ανάγκη.

5.2.5.β. Οι προκαθορισμένοι ή/και συστημικοί λογαριασμοί (system accounts) περιορίζονται στον ελάχιστο δυνατό αριθμό και η ανάγκη διατήρησής τους τεκμηριώνεται επαρκώς. Αποφεύγεται η χρήση των εν λόγω λογαριασμών από φυσικά πρόσωπα.

5.2.5.γ. Σε περίπτωση χρήσης κοινών ή προκαθορισμένων-συστημικών λογαριασμών από φυσικά πρόσωπα, εξασφαλίζεται η αντιστοίχιση του συγκεκριμένου φυσικού προσώπου που αποκτά πρόσβαση σε ΠΕΣ με τις ενέργειες που τελούνται σε αυτό με κατάλληλο μηχανισμό, ο οποίος τεκμηριώνεται επαρκώς.

5.2.5.δ. Το υπόχρεο πρόσωπο διατηρεί αρχείο με την τεκμηρίωση αυτής της παραγράφου.

5.2.6. Για τους λογαριασμούς πρόσβασης των παραγράφων 5.2.4 και 5.2.5 του παρόντος άρθρου, ο πάροχος διατηρεί αρχείο στο οποίο καταγράφεται το ιστορικό όλων των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα ΠΕΣ (ενδεικτικά ανά ΠΕΣ: λογαριασμός πρόσβασης, δικαιώματα/επίπεδο πρόσβασης αυτού, χρονικό διάστημα ισχύος).

5.2.7. Ο πάροχος καταγράφει σε αρχείο τους τρόπους πρόσβασης των εργαζομένων και συνεργατών του σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών (ενδεικτικά αναφέρονται οι τρόποι πρόσβασης μέσω εξειδικευμένων εφαρμογών, βάσεων δεδομένων και του συστήματος αρχείων του λειτουργικού συστήματος).

5.2.8. Ο πάροχος διατηρεί και εφαρμόζει τις παρακάτω διαδικασίες:

5.2.8.1. Διαδικασία Διαχείρισης Χρηστών ΠΕΣ

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

5.2.8.1.2. Για κάθε μία εκ των ενεργειών που αναφέρονται στην παράγραφο 5.2.8.1.1. του παρόντος άρθρου προβλέπεται υποχρεωτικά προηγούμενη έγκριση από αρμόδιο εργαζόμενο του παρόχου.

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

5.2.8.2. Διαδικασία Ελέγχου Ορθής Εφαρμογής των απαιτήσεων της Λογικής Πρόσβασης

5.2.8.2.1. Στη Διαδικασία Ελέγχου Ορθής Εφαρμογής των απαιτήσεων της Λογικής Πρόσβασης περιγράφονται με σαφήνεια οι περιοδικοί έλεγχοι που πραγματοποιούνται, κατ' ελάχιστον κάθε έξι (6) μήνες, σε συμφωνία με τις αρχές του Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών της ενότητας 9.5 του άρθρου 9 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 στο οποίο καταγράφεται το ιστορικό όλων των λογαριασμών (παράγραφος 5.2.6 του παρόντος άρθρου) με τους λογαριασμούς που προκύπτουν από έκαστο ΠΕΣ.

(γ) Τον δειγματοληπτικό έλεγχο των αρχείων καταγραφής πρόσβασης (access logs) της παραγράφου 9.3.1.α του άρθρου 9 του παρόντος Κανονισμού για την ανακάλυψη ενδεχόμενων μη αιτιολογημένων προσβάσεων.

5.2.9. Σχετικά με τη δημιουργία και διαχείριση των λογαριασμών πρόσβασης, ο πάροχος διατηρεί (ανά ΠΕΣ ή συγκεντρωτικά) αρχείο, το οποίο περιλαμβάνει τα ακόλουθα:

(α) περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία ενός ονόματος χρήστη,

(β) περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία ενός κωδικού πρόσβασης,

(γ) τον τρόπο σύμφωνα με τον οποίο αποδίδεται με ασφάλεια σε κάθε εργαζόμενο και συνεργάτη του παρόχου το όνομα χρήστη και ο κωδικός πρόσβασης,

(δ) τον τρόπο σύμφωνα με τον οποίο επιτυγχάνεται η τακτική αλλαγή των κωδικών πρόσβασης και εν γένει η διαχείρισή τους,

(ε) περιγραφή των όρων χρήσης των κωδικών πρόσβασης από τους εργαζόμενους και συνεργάτες του παρόχου,

(στ) τη διαδικασία, σύμφωνα με την οποία διενεργείται έλεγχος για την ορθή εφαρμογή των παραπάνω κανόνων και διαδικασιών, σε συμφωνία με τις αρχές του Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών της ενότητας 9.5 του άρθρου 9 του παρόντος Κανονισμού.

5.2.10. Για την υλοποίηση των υποχρεώσεων της παραγράφου 5.2.9 του παρόντος άρθρου, ο πάροχος λαμβάνει υπόψη τις συνήθεις καλές πρακτικές από την επιστήμη και την τεχνολογία και ιδιαίτερα τις παρακάτω απαιτήσεις:

5.2.10.1. Τα ονόματα χρήστη δεν υποδηλώνουν τον ρόλο των εργαζομένων και συνεργατών του παρόχου στο αντίστοιχο ΠΕΣ (ενδεικτικά, δεν είναι παράγωγα της λέξης admin).

5.2.10.2. Οι χρησιμοποιούμενοι κωδικοί πρόσβασης είναι ισχυροί και έχουν δημιουργηθεί με τρόπο που αποτρέπει τον προσδιορισμό τους με εύκολο τρόπο. Ειδικότερα, οι κωδικοί πρόσβασης δημιουργούνται με συνδυασμό δύο (2) τουλάχιστον διαφορετικών ειδών χαρακτήρων (αριθμοί, γράμματα, ειδικοί χαρακτήρες). Οι κωδικοί πρόσβασης έχουν υποχρεωτικά ένα επαρκές, με βάση τις συνήθεις καλές πρακτικές, ελάχιστο μήκος,

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

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

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

5.2.10.5. Οι κωδικοί πρόσβασης διατηρούνται κρυπτογραφημένοι στα ΠΕΣ.

Β. Πρόσθετες Απαιτήσεις αναφορικά με την Απομακρυσμένη Λογική Πρόσβαση

5.2.11. Ο πάροχος καθορίζει τη διαβάθμιση των επιπέδων πρόσβασης και θέτει τις απαιτήσεις για τον έλεγχο της απομακρυσμένης πρόσβασης στα ΠΕΣ.

5.2.12. Οι απαιτήσεις για την Απομακρυσμένη Λογική Πρόσβαση ισχύουν για τους εργαζόμενους και συνεργάτες του παρόχου, οι οποίοι στο πλαίσιο της εργασίας τους αποκτούν απομακρυσμένη πρόσβαση στα ΠΕΣ και στα σχετικά δεδομένα και τις πληροφορίες.

5.2.13. Η απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών του παρόχου στα ΠΕΣ του περιορίζεται στις περιπτώσεις που αυτό είναι απαραίτητο για τις επιχειρησιακές του ανάγκες.

5.2.14. Ο πάροχος διατηρεί αρχείο, στο οποίο καταγράφονται τα ΠΕΣ στα οποία επιτρέπεται η απομακρυσμένη πρόσβαση και οι τεχνικοί τρόποι απομακρυσμένης ασφαλούς πρόσβασης εργαζομένων και συνεργατών του, για κάθε ΠΕΣ στο οποίο έχει επιτραπεί η απομακρυσμένη πρόσβαση.

5.2.15. Ο πάροχος τηρεί αρχείο με τους εργαζομένους και συνεργάτες του (ονοματεπώνυμο και ιδιότητα), οι οποίοι έχουν εξουσιοδοτηθεί για χρήση της απομακρυσμένης πρόσβασης. Στο εν λόγω αρχείο καταγράφονται τα δικαιώματα πρόσβασης που τους αντιστοιχούν για κάθε ΠΕΣ.

5.2.16. Η απομακρυσμένη πρόσβαση των εργαζομένων και συνεργατών του παρόχου πραγματοποιείται με χρήση μηχανισμών ασφαλούς αυθεντικοποίησης και κρυπτογράφησης (π.χ. μέσω Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks – VPN)).

5.2.17. Ο πάροχος 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.

5.2.18. Η απομακρυσμένη πρόσβαση των συνεργατών του παρόχου επιτρέπεται μόνο για συγκεκριμένο χρονικό διάστημα. Ο πάροχος επιτρέπει κάθε απομακρυσμένη πρόσβαση των συνεργατών του στα συστήματά του μόνο κατόπιν έγκρισης σχετικού αιτήματος, στο οποίο θα αναγράφεται ο λόγος της πρόσβασης, το σύστημα στο οποίο θα πραγματοποιηθεί η πρόσβαση, καθώς και το χρονικό διάστημα που απαιτείται. Ο περιορισμός του χρονικού διαστήματος μπορεί να υλοποιείται με τη χρήση προσωρινών κωδικών, οι οποίοι θα μεταβάλλονται μετά το πέρας του

προκαθορισμένου χρονικού διαστήματος, ή με την απενεργοποίηση των λογαριασμών μετά το πέρας του διαστήματος αυτού ή με άλλον αντίστοιχο μηχανισμό. Ο πάροχος τηρεί αρχείο με όλες τις πληροφορίες της παρούσας παραγράφου.

5.2.19. Ο πάροχος διατηρεί και εφαρμόζει συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών απομακρυσμένης πρόσβασης των εργαζομένων και συνεργατών του, η οποία είναι σύμφωνη με τις απαιτήσεις που αναφέρονται στην ενότητα 5.2.Β του παρόντος άρθρου.

5.2.20. Ο πάροχος ελέγχει, κατ' ελάχιστον, κάθε τρεις (3) μήνες α) την αντιστοίχιση των λογαριασμών απομακρυσμένης πρόσβασης και του αρχείου της παραγράφου 5.2.15 του παρόντος άρθρου, και β) την υλοποίηση των απαιτούμενων μεταβολών των κωδικών και απενεργοποιήσεων των λογαριασμών της παραγράφου 5.2.18 του παρόντος άρθρου, σε συμφωνία με τις αρχές του Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών της ενότητας 9.5 του άρθρου 9 του παρόντος Κανονισμού.

Γ. Ειδικές Απαιτήσεις σχετικά με τους Συνδρομητές ή Χρήστες των Παρεχόμενων Δικτύων ή Υπηρεσιών

5.2.21. Ο πάροχος 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.

5.2.22. Ο πάροχος διατηρεί και εφαρμόζει συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών πρόσβασης των συνδρομητών ή χρηστών στις υπηρεσίες ή/και τα δίκτυα που παρέχει, στην οποία περιγράφεται με σαφήνεια κατ' ελάχιστον ο τρόπος προσθήκης και κατάργησης λογαριασμών πρόσβασης, καθώς και η απόδοση του ονόματος χρήστη και του κωδικού πρόσβασης στους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών. Κατά τη δημιουργία ή επανέκδοση του κωδικού πρόσβασης, ο πάροχος τον δημιουργεί με τρόπο που αποτρέπει τον εύκολο προσδιορισμό του. Ο πάροχος ενημερώνει με κάθε πρόσφορο μέσο τους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών σχετικά με την αναγκαιότητα αλλαγής του κωδικού πρόσβασης, καθώς και σχετικά με ενδεδειγμένους κανόνες δημιουργίας ισχυρών κωδικών πρόσβασης.

5.2.23. Ο πάροχος πραγματοποιεί ελέγχους, κατ' ελάχιστον κάθε δώδεκα (12) μήνες, σχετικά με την αλλαγή του κωδικού πρόσβασης που αποδίδει στους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών και τους ενημερώνει εκ νέου για την αναγκαιότητα αλλαγής των κωδικών πρόσβασης σε περίπτωση που δεν έχουν προβεί στη σχετική αλλαγή, σε συμφωνία με τις αρχές του Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών της ενότητας 9.5 του άρθρου 9 του παρόντος Κανονισμού.

5.2.24. Σε περίπτωση που προσφέρεται στους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών του παρόχου η δυνατότητα να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας τους (ενδεικτικά, εξερχόμενες κλήσεις, ηλεκτρονικό ταχυδρομείο) μέσω συγκεκριμένης ιστοθέσης, ο πάροχος χρησιμοποιεί τους ευρέως αποδεκτούς μηχανισμούς ασφαλούς αυθεντικοποίησης και κρυπτογράφησης, του οποίους και περιγράφει σε σχετικό αρχείο που διατηρεί. Ο πάροχος καταγράφει τις προσβάσεις και τις ενέργειες των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών, σύμφωνα με τις απαιτήσεις της παραγράφου 9.3.1 του άρθρου 9 του παρόντος Κανονισμού.

5.2.25. Οι κωδικοί πρόσβασης των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών διατηρούνται κρυπτογραφημένοι στα ΠΕΣ.

5.3. Ασφάλεια Δικτύου

Α. Γενικές Αρχές Μηχανισμών και Συστημάτων Ασφάλειας Δικτύου

5.3.1. Ο πάροχος καταρτίζει και διατηρεί διαρκώς ενημερωμένο αρχείο στο οποίο ορίζονται οι μηχανισμοί και τα συστήματα που χρησιμοποιούνται σε υλικό και λογισμικό για τους σκοπούς της Ασφάλειας Δικτύου. Οι τρόποι λειτουργίας και τεχνικής διαμόρφωσής τους λαμβάνουν υπόψη τις διεθνείς, ευρέως αποδεκτές πρακτικές και πρότυπα, καθώς και την Αποτίμηση Κινδύνου στην οποία έχει προβεί ο πάροχος, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού. Οι μηχανισμοί και τα συστήματα της Ασφάλειας Δικτύου περιλαμβάνουν, ενδεικτικά και όχι περιοριστικά: τείχη προστασίας, συστήματα ανίχνευσης και αποτροπής εισβολών (intrusion detection and prevention systems), λίστες ελέγχου πρόσβασης (access control lists), εικονικά ιδιωτικά δίκτυα, εικονικά τοπικά δίκτυα.

5.3.2. Η εγκατάσταση, η επικαιροποίηση και η διαχείριση των αναφερόμενων στην παράγραφο 5.3.1 του παρόντος άρθρου μηχανισμών και συστημάτων είναι σύμφωνη με τις αρχές της Διαχείρισης ΠΕΣ της ενότητας 6.2 του άρθρου 6 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 και αποτροπής εισβολών με υπογραφές νέων εισβολών ή επιθέσεων).

5.3.3. Η λειτουργία των αναφερομένων στην παράγραφο 5.3.1 του παρόντος άρθρου μηχανισμών και συστημάτων είναι συνεχής, εξαιρουμένων των περιπτώσεων προγραμματισμένης συντήρησης ή αναβάθμισης, σύμφωνα με τις αρχές της Διαχείρισης ΠΕΣ της ενότητας 6.2 του άρθρου 6 του παρόντος Κανονισμού.

Β. Λογικός Διαχωρισμός και Κατάτμηση Δικτύων του Παρόχου

5.3.4. Ο πάροχος καταρτίζει και διατηρεί διαρκώς ενημερωμένο αρχείο, στο οποίο, με βάση τους αναφερόμενους στην παράγραφο 5.3.1 του παρόντος άρθρου μηχανισμούς και συστήματα (α) περιγράφεται ο λογικός διαχωρισμός και η κατάτμηση των δικτύων του με αντίστοιχη σχηματική απεικόνιση, (β) περιγράφεται η αρχιτεκτονική που έχει υλοποιηθεί και (γ) καταγράφονται όλα τα ΠΕΣ και η ζώνη ασφάλειας στην οποία έχουν τοποθετηθεί. Ο πάροχος διατηρεί τις προηγούμενες εκδόσεις του εν λόγω αρχείου και το χρονικό διάστημα ισχύος εκάστης.

5.3.5. Σε περίπτωση που ο πάροχος 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 τοποθετούνται σε μία ή περισσότερες αποστρατικοποιημένες ζώνες (DeMilitarized Zone, DMZ).

5.3.6. Τα ΠΕΣ του παρόχου που χρησιμοποιούνται από τους εργαζόμενους και συνεργάτες του για την εκτέλεση 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) εντάσσονται σε μία ή περισσότερες εσωτερικές έμπιστες ζώνες, ανάλογα με τις απαιτήσεις ασφάλειας και την κρισιμότητά τους.

5.3.7. Τα ΠΕΣ του παρόχου, ιδίως αυτά που δεν τοποθετούνται σε αποστρατικοποιημένες ή έμπιστες ζώνες (ενδεικτικά, τα δίκτυα πρόσβασης/μετάδοσης, οι συσκευές και κόμβοι διασύνδεσης με τρίτα/εξωτερικά δίκτυα), είναι δυνατό, ανάλογα με την τεχνολογία τους, να υποστηρίζουν την προαιρετική χρήση συγκεκριμένων μηχανισμών ασφάλειας. Στην περίπτωση αυτή, ο πάροχος επιλέγει, ενεργοποιεί και παραμετροποιεί όλους τους κατάλληλους μηχανισμούς ασφάλειας, εκμεταλλευόμενος τις δυνατότητες και μεθόδους ασφάλειας που διαθέτει (ενδεικτικά αναφέρεται η κρυπτογράφηση), τις διεθνείς, ευρέως αποδεκτές πρακτικές και πρότυπα, και τα αποτελέσματα που προκύπτουν από την Αποτίμηση Κινδύνου, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού. Για τα ΠΕΣ της παρούσας παραγράφου, ο πάροχος διατηρεί αρχείο με πλήρη ανάλυση των μέτρων προστασίας και ασφάλειας που έχουν υλοποιηθεί σε αυτά, με σκοπό την ασφάλεια δικτύων και υπηρεσιών του.

5.4. Προστασία από Κακόβουλο Λογισμικό και Ακεραιότητα των ΠΕΣ

5.4.1. Ο πάροχος λαμβάνει όλα τα απαραίτητα οργανωτικά, τεχνικά και άλλα μέτρα ασφάλειας, τα οποία αποσκοπούν στην αποτροπή, ανίχνευση και αντιμετώπιση κακόβουλου λογισμικού. Σε περίπτωση ανίχνευσης κακόβουλου λογισμικού, ο πάροχος ενεργοποιεί τους κατάλληλους μηχανισμούς που διαθέτει για τον περιορισμό της εξάπλωσής του και επιπλέον πραγματοποιεί άμεση αξιολόγηση του περιστατικού και, αναλόγως της κρισιμότητάς του, ενεργοποιεί τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με την ενότητα 7.1 του άρθρου 7 του παρόντος Κανονισμού.

5.4.2. Ο πάροχος ενημερώνει τους εργαζόμενους και συνεργάτες του αναφορικά με τους κινδύνους από κακόβουλο λογισμικό, καθώς και σχετικά με τις υποχρεώσεις τους σε σχέση με τα μέτρα προστασίας έναντι του κακόβουλου λογισμικού.

5.4.3. Ο πάροχος λαμβάνει τα απαραίτητα οργανωτικά και τεχνικά μέτρα, τα οποία αποσκοπούν στην αποτροπή της παραποίησης του λογισμικού των ΠΕΣ, κατά την προμήθεια, εγκατάσταση και λειτουργία τους και ιδιαίτερα στην περίπτωση κατά την οποία πραγματοποιούνται οι αναγκαίες αναβαθμίσεις, ενημερώσεις και διορθώσεις (updates, patches). Ο πάροχος, σε συμφωνία με τις αρχές του Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών της ενότητας 9.5 του άρθρου 9 του παρόντος Κανονισμού, πραγματοποιεί έλεγχο της ακεραιότητας του λογισμικού των ΠΕΣ. Ο έλεγχος αυτός έχει ως σκοπό τη διαπίστωση της μη ύπαρξης στα ΠΕΣ λογισμικού πέραν αυτού που έχει επισήμως προμηθευτεί ο πάροχος.

5.4.4. Ο πάροχος διατηρεί αρχείο στο οποίο καταγράφονται οι λεπτομέρειες εφαρμογής των απαιτήσεων που ορίζονται στην παρούσα ενότητα.

5.5. Χρήση Κρυπτογραφίας

5.5.1. Ο πάροχος χρησιμοποιεί τους κατάλληλους αλγόριθμους και συστήματα κρυπτογράφησης 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 κρυπτογράφησης.

5.5.2. Ο πάροχος εφαρμόζει συστήματα κρυπτογράφησης για την επαρκή προστασία των δεδομένων επικοινωνίας κατά την αποθήκευση και μεταφορά τους μέσω δικτύων.

5.5.3. Η κρυπτογράφηση εφαρμόζεται στα ΠΕΣ με βάση τα αποτελέσματα που προκύπτουν από την Αποτίμηση Κινδύνου, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού.

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

5.5.5. Το μήκος κλειδιού που χρησιμοποιείται λαμβάνει υπόψη τα διεθνώς και ευρέως αποδεκτά πρότυπα, ανάλογα με τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης και με τα αποτελέσματα που προκύπτουν από την Αποτίμηση Κινδύνου, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού.

5.5.6. Ο πάροχος αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση στα κλειδιά τα οποία χρησιμοποιούνται για κρυπτογράφηση, αυθεντικοποίηση ή ψηφιακή υπογραφή.

5.5.7. 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 αντιστοιχεί σε έναν μοναδικό χρήστη και το αντίστοιχο ιδιωτικό κλειδί είναι γνωστό μόνο στον συγκεκριμένο χρήστη, στον οποίο αντιστοιχεί.

5.5.8. Σε περίπτωση που ο πάροχος χρησιμοποιεί ψηφιακά πιστοποιητικά δημόσιων κλειδιών (digital certificates), τα οποία παράγονται από παρόχους υπηρεσιών πιστοποίησης (certification service providers), εξασφαλίζει ότι ο πάροχος υπηρεσιών πιστοποίησης συμμορφώνεται με την κείμενη νομοθεσία.

5.5.9. Σε περίπτωση που ο πάροχος παράγει και διαχειρίζεται κλειδιά κρυπτογράφησης, τα οποία χρησιμοποιούνται σε ΠΕΣ, διατηρεί και εφαρμόζει κατάλληλες διαδικασίες για τη δημιουργία, πιστοποίηση, διανομή και ανάκληση των κρυπτογραφικών κλειδιών.

5.5.10. Ο πάροχος διατηρεί αρχείο, στο οποίο καταγράφονται οι λεπτομέρειες εφαρμογής των απαιτήσεων που ορίζονται στην παρούσα ενότητα.

ΑΡΘΡΟ 6 - Διαχείριση Λειτουργίας

6.1. Παρακολούθηση Δικτύου

6.1.1. Ο πάροχος παρακολουθεί συνεχώς την υφιστάμενη λειτουργία του δικτύου και των υπηρεσιών, καταγράφει και αναλύει τα προβλήματα και προβλέπει τις μελλοντικές ανάγκες, ώστε να προβαίνει έγκαιρα στις απαραίτητες ενέργειες για τη διασφάλιση της ασφάλειας του δικτύου και των υπηρεσιών.

6.1.2. Ο πάροχος προστατεύει το δίκτυο και τις υπηρεσίες από συνθήκες αυξημένης κίνησης. Παρακολουθεί και ελέγχει την κίνηση του δικτύου και των υπηρεσιών και εντοπίζει έγκαιρα την αύξησή της, χρησιμοποιώντας τεχνικές διαχείρισης κίνησης. Προστατεύει, επίσης, το δίκτυο και τις υπηρεσίες από ενδεχόμενη συμφόρηση λόγω αυξημένης κίνησης, εξασφαλίζοντας παράλληλα τη βελτιστοποίηση της απόδοσης.

6.1.3. Ο πάροχος προβαίνει σε προβλέψεις αναφορικά με περιοδικά ή μη γεγονότα, τα οποία ενδέχεται να προκαλέσουν σημαντική αύξηση της κίνησης στο δίκτυο και τις υπηρεσίες, όπως είναι, ενδεικτικά, οι εθνικές ή θρησκευτικές εορτές και οι διαγωνισμοί εθνικής εμβέλειας σε ιδιαίτερα περιορισμένο χρονικό διάστημα. Επίσης, παρακολουθεί την επικαιρότητα, στον βαθμό που αυτή ενδέχεται να επηρεάσει την κίνηση στο δίκτυο και τις υπηρεσίες, όπως, ενδεικτικά, σε περίπτωση καταστροφών ή φυσικών φαινομένων, εθνικής ή τοπικής εμβέλειας.

6.1.4. Ο πάροχος καταγράφει τις τεχνικές διαχείρισης κίνησης και τις συνθήκες υπό τις οποίες τις εφαρμόζει. Καταγράφει, επίσης, τα μέτρα που χρησιμοποιεί προκειμένου να εξασφαλίσει την προτεραιότητα της κίνησης προς τις υπηρεσίες έκτακτης ανάγκης, ιδιαίτερα σε καταστάσεις εκτάκτων συνθηκών.

6.1.5. Ο πάροχος εξετάζει, αξιολογεί και αξιοποιεί πιθανές αναφορές παραπόνων που υποβάλλονται από χρήστες του δικτύου και των υπηρεσιών του σχετικά με προβλήματα που παρουσιάζονται κατά την παροχή της υπηρεσίας.

6.1.6. Ο πάροχος πραγματοποιεί τις εργασίες συντήρησης, αναβάθμισης ή άλλες τεχνικές επεμβάσεις στον εξοπλισμό του, χωρίς να διακόπτεται η λειτουργία του δικτύου και των υπηρεσιών. Όπου αυτό δεν είναι τεχνικά εφικτό, ο πάροχος επιλέγει οι εργασίες αυτές να πραγματοποιούνται σε ώρες χαμηλής κίνησης.

6.2. Διαχείριση ΠΕΣ

6.2.1. Ο πάροχος διατηρεί και εφαρμόζει διαδικασία διαχείρισης ΠΕΣ, η οποία προσδιορίζει τις απαιτήσεις που πρέπει να ικανοποιούνται καθ' όλη τη διάρκεια του κύκλου ζωής των ΠΕΣ. Κατ' ελάχιστον η διαδικασία περιγράφει τα ακόλουθα στάδια: (α) Προμήθειας/Ανάπτυξης Υλικού και Λογισμικού, (β) Εγκατάστασης/Αρχικής Λειτουργίας Υλικού και Λογισμικού, (γ) Λειτουργίας Υλικού και Λογισμικού και (δ) Διαγραφής/Απόσυρσης Υλικού και Λογισμικού

6.2.2. Κατά το στάδιο της Προμήθειας/Ανάπτυξης Υλικού και Λογισμικού των ΠΕΣ, ο πάροχος:

(α) πραγματοποιεί αρχικά Αποτίμηση Κινδύνου για τον εντοπισμό των πιθανών απειλών, ευπαθειών και κινδύνων του υπό προμήθεια/ανάπτυξη ΠΕΣ, αναφορικά με την ασφάλεια δικτύων και υπηρεσιών, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού.

(β) συντάσσει κατάλογο (i) κανόνων ασφάλειας που αφορούν σε ρυθμίσεις ή χαρακτηριστικά του υπό προμήθεια/ανάπτυξη ΠΕΣ σχετικά με την ασφάλεια δικτύων και υπηρεσιών, (ii) ελάχιστων κανόνων που αφορούν στα χαρακτηριστικά διαμόρφωσης και διαχείρισης του υπό προμήθεια/ανάπτυξη ΠΕΣ, καθώς και (iii) παραμέτρων διαμόρφωσης της καταγραφής της πρόσβασης και των ενεργειών, ώστε να επιτυγχάνεται η συμμόρφωση με τις προδιαγραφές ασφάλειας που καθορίζονται από τα αποτελέσματα της Αποτίμησης Κινδύνου και από τις βέλτιστες πρακτικές ασφάλειας. Οι ως άνω κανόνες γίνονται αποδεκτοί από όλα τα εμπλεκόμενα μέρη (π.χ. συνεργαζόμενες εταιρείες, υπαλλήλους του υπόχρεου προσώπου που αναπτύσσουν εσωτερικά στην εταιρεία το λογισμικό) και τηρούνται σε αρχείο από το υπόχρεο πρόσωπο.

6.2.3. Κατά το στάδιο της Εγκατάστασης/Αρχικής Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ, ο πάροχος:

(α) πραγματοποιεί δοκιμές για τον έλεγχο της συμμόρφωσης με τους κανόνες ασφάλειας της προηγούμενης παραγράφου,

(β) καταγράφει και διατηρεί σε αρχείο τις δοκιμές και τα αποτελέσματα αυτών. Το αρχείο αυτό επισυνάπτεται στη συνολική έκθεση αποδοχής του ΠΕΣ και τηρείται αδιάλειπτα.

6.2.4. Κατά το στάδιο Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ, ο πάροχος:

(α) εκτελεί προληπτική συντήρηση του ΠΕΣ, βάσει προδιαγεγραμμένου χρονοδιαγράμματος, προκειμένου να ελαχιστοποιηθεί η πιθανότητα δυσλειτουργίας του δικτύου και των παρεχόμενων υπηρεσιών. Ειδικότερα, ο πάροχος διαθέτει κατάλληλους μηχανισμούς ώστε να προλαβαίνει τυχόν βλάβες ή να τις αποκαθιστά άμεσα σε περίπτωση εμφάνισής τους, όπως, ενδεικτικά, βλαβοληψία, διαχείριση ανταλλακτικών, διαδικασία εσωτερικής κλιμάκωσης αναφοράς προβλημάτων, δείκτες αποκατάστασης βλαβών με τους προμηθευτές,

(β) εξασφαλίζει ότι υπάρχουν, ανά πάσα στιγμή, διαθέσιμα αντίγραφα ασφαλείας της πλέον πρόσφατης διαμόρφωσης του ΠΕΣ, τα οποία είναι απαραίτητα για την αποκατάσταση του δικτύου του και των παρεχόμενων υπηρεσιών. Τα αντίγραφα ασφαλείας φυλάσσονται σε προστατευμένο χώρο,

(γ) πραγματοποιεί στο λογισμικό/υλικό του ΠΕΣ, αμελλητί, τις αλλαγές (εισαγωγή/μεταβολή/διαγραφή) που σχετίζονται με την ασφάλεια δικτύων και υπηρεσιών,

(δ) διατηρεί αρχείο για οποιαδήποτε αλλαγή υλικού ή λογισμικού ΠΕΣ, στο οποίο καταγράφεται η ημερομηνία, ο τρόπος, η αιτιολόγηση και το προσωπικό που πραγματοποίησε τις αλλαγές. Το αρχείο ενημερώνεται και διατηρείται από εξουσιοδοτημένη προς τούτο διοικητική οντότητα ή προσωπικό του παρόχου.

6.2.5. Κατά το στάδιο της Διαγραφής/Απόσυρσης Υλικού και Λογισμικού των ΠΕΣ, ο πάροχος:

(α) ορίζει συγκεκριμένες ενέργειες προκειμένου να διασφαλίζεται ότι, με την επιφύλαξη τήρησης υποχρεώσεων που τυχόν 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 κ.λπ.) διαγράφεται οριστικά και δεν μπορεί να χρησιμοποιηθεί από τρίτους.

(β) διατηρεί αρχείο στο οποίο καταγράφονται τα ΠΕΣ, τα οποία αποσύρονται.

ΑΡΘΡΟ 7 – Διαχείριση Περιστατικών Ασφάλειας

7.1. Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας

7.1.1. Ο πάροχος διατηρεί και εφαρμόζει Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας, η οποία ενεργοποιείται αμελλητί σε κάθε περίπτωση περιστατικού ασφάλειας, με σκοπό τη διαχείριση των περιστατικών.

7.1.2. Η Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας προβλέπει κατ' ελάχιστον τις ακόλουθες ενέργειες: α) την οργάνωση του προσωπικού του παρόχου (ορισμοί ρόλων και αρμοδιοτήτων), με σκοπό την αποτελεσματική διαχείριση των περιστατικών ασφάλειας, β) τον εντοπισμό, την καταγραφή και αρχειοθέτηση των περιστατικών ασφάλειας, γ) τη διερεύνηση των αιτιών και τον προσδιορισμό των τεχνικών ή/και οργανωτικών αδυναμιών στις οποίες ενδεχομένως οφείλεται το

περιστατικό ασφάλειας και την καταγραφή τους, δ) την καταγραφή και υλοποίηση των διορθωτικών μέτρων και ενεργειών με συγκεκριμένο χρονοδιάγραμμα και ε) την ενημέρωση του Υπεύθυνου Ασφάλειας Δικτύων και Υπηρεσιών, των αρμοδίων στελεχών του παρόχου, των αρμοδίων Αρχών και των θιγόμενων συνδρομητών ή χρηστών των παρεχόμενων δικτύων και υπηρεσιών, σύμφωνα με την κείμενη νομοθεσία.

7.1.3. Ο πάροχος ελέγχει σε τακτά χρονικά διαστήματα την ετοιμότητα ενεργοποίησης της Διαδικασίας Διαχείρισης Περιστατικών Ασφάλειας, και αξιολογεί και ανανεώνει την εν λόγω Διαδικασία, με βάση τα αποτελέσματα των ελέγχων και τα προηγούμενα περιστατικά.

7.1.4. Ο πάροχος 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 της ασφάλειας των παρεχόμενων δικτύων ή υπηρεσιών.

7.2 Αναφορά Περιστατικών Ασφάλειας

7.2.1. Ο πάροχος κοινοποιεί το περιστατικό ασφάλειας στην ΑΔΑΕ, σύμφωνα με τις παραμέτρους για την υποχρέωση κοινοποίησης που ορίζονται στο Παράρτημα του παρόντος Κανονισμού, όπως εκάστοτε ισχύει, ως ακολούθως:

Α. Ο πάροχος υποβάλλει αμελλητί στην ΑΔΑΕ την «Έκθεση Αρχικής Αναφοράς Περιστατικού Ασφάλειας», στην οποία καταγράφονται, κατ' ελάχιστον, τα ακόλουθα:
   i. Το είδος του περιστατικού ασφάλειας (ενδεικτικά εάν αφορά στο απόρρητο των επικοινωνιών ή στη διαθεσιμότητα των υπηρεσιών).
   ii. Περιεκτική περιγραφή του περιστατικού ασφάλειας.
   iii. Σύντομη αναφορά των αιτιών οι οποίες προκάλεσαν το περιστατικό και των στοιχείων των παρεχόμενων δικτύων ή υπηρεσιών, τα οποία έχουν επηρεαστεί.

   Ειδικά στην περίπτωση κατά την οποία το περιστατικό ασφάλειας αφορά σε διαθεσιμότητα των παρεχόμενων υπηρεσιών, ο πάροχος ενημερώνει την ΑΔΑΕ άμεσα από την εμφάνιση του περιστατικού, με αυτοματοποιημένο τρόπο εφόσον είναι εφικτό άλλως με κάθε πρόσφορο μέσο (τηλεφωνική κλήση, μήνυμα ηλεκτρονικού ταχυδρομείου). Επιπρόσθετα, στην «Έκθεση Αρχικής Αναφοράς Περιστατικού Ασφάλειας» καταγράφονται, επιπλέον, τα ακόλουθα:

   i. Εκτίμηση αναφορικά με τα δίκτυα ή/και υπηρεσίες ηλεκτρονικών επικοινωνιών, τη γεωγραφική περιοχή και το πλήθος των συνδρομητών/χρηστών που έχουν επηρεαστεί ή/και πρόκειται να επηρεαστούν.
   ii. Εκτίμηση αν επηρεάζονται οι υπηρεσίες εκτάκτου ανάγκης.
   iii. Εκτίμηση του προγραμματισμού ανάκαμψης.

Β. Ο πάροχος υποβάλλει στην ΑΔΑΕ την «Τελική Έκθεση Αναφοράς Περιστατικού Ασφάλειας», το αργότερο ένα μήνα μετά την υποβολή της Έκθεσης Αρχικής Αναφοράς, στην οποία καταγράφονται, κατ' ελάχιστον, τα ακόλουθα:
   i. Ημερομηνία και ώρα εκδήλωσης του περιστατικού.
   ii. Ημερομηνία και ώρα που έγινε αντιληπτό το περιστατικό.

iii. Κατηγορία Δικτύου (π.χ. Σταθερό, Κινητό, Δορυφορικό) και Υπηρεσιών που επηρεάστηκαν [π.χ. Τηλεφωνία, Γραπτά μηνύματα (SMS), Πολυμεσικά μηνύματα (MMS), Περιήγηση στο Διαδίκτυο (Web Browsing)].
iv. Αριθμός χρηστών που επηρεάστηκαν ανά υπηρεσία.
v. Χρονική διάρκεια περιστατικού.
vi. Γεωγραφική κάλυψη (π.χ. διοικητική περιφέρεια, Νομός, Δήμος).
vii. Στοιχεία του Δικτύου που επηρεάστηκαν:
    1. είδος, όνομα κατασκευαστή, σύντομη περιγραφή της βασικής του λειτουργίας,
    2. κατηγορία του κόμβου (π.χ. πρωτεύον PoP, δευτερεύον PoP, ΑΚ),
    3. κατηγορία του δικτύου στο οποίο ανήκει (π.χ. επίπεδο πρόσβασης, συγκέντρωσης, άκρου δικτύου, διανομής, πυρήνα).
viii. Συνέπειες στις υπηρεσίες έκτακτης ανάγκης.
ix. Πρωτεύουσα αιτία του περιστατικού (π.χ. ανθρώπινο λάθος, αστοχία υλικού ή λογισμικού, φυσικά φαινόμενα ή καταστροφές, κακόβουλη ενέργεια, ανεπάρκεια τρίτου μέρους ή εξωτερικού φορέα).
x. Δευτερεύουσα αιτία του περιστατικού.
xi. Εκτίμηση του προγραμματισμού ανάκαμψης.
xii. Ενέργειες διαχείρισης και ανταπόκρισης στο περιστατικό.
xiii. Συλλεχθέντα στοιχεία για τη διερεύνηση του περιστατικού.
xiv. Διορθωτικά μέτρα και σχετικό χρονοδιάγραμμα.
xv. Ενημέρωση θιγόμενων συνδρομητών ή άλλων ατόμων που επηρεάστηκαν από το περιστατικό και γνωστοποίηση στις αρμόδιες αρχές, σύμφωνα με την κείμενη νομοθεσία.
xvi. Ενδεχόμενες συστάσεις σε θιγόμενους συνδρομητές ή άλλα άτομα που επηρεάστηκαν από το περιστατικό, με σκοπό τον μετριασμό των αρνητικών επιπτώσεών του.

Γ. Σε περίπτωση εν εξελίξει περιστατικού κατά τον χρόνο υποχρέωσης υποβολής της Τελικής Έκθεσης, ο πάροχος υποβάλλει Έκθεση Προόδου τη δεδομένη στιγμή και Τελική Έκθεση το αργότερο ένα μήνα μετά την υποβολή της Έκθεσης Προόδου. Η Έκθεση Προόδου καταγράφει τα πεδία της «Τελικής Έκθεσης Αναφοράς Περιστατικού Ασφάλειας» που είναι γνωστά στον πάροχο τη δεδομένη στιγμή.

Δ. Τυχόν πεδία της «Τελικής Έκθεσης Αναφοράς Περιστατικού Ασφάλειας» που είναι γνωστά στον πάροχο ήδη από το αρχικό στάδιο που γίνεται αντιληπτό το περιστατικό, συμπεριλαμβάνονται από τον πάροχο και στην «Έκθεση Αρχικής Αναφοράς Περιστατικού Ασφάλειας».

7.2.2. Η ΑΔΑΕ δύναται να ζητεί συμπληρωματικές πληροφορίες ή διευκρινίσεις σχετικά με τα περιστατικά ασφάλειας, πέραν των αναφερομένων στις εκθέσεις της παραγράφου 7.2.1 του παρόντος άρθρου. Για τον λόγο αυτόν, οι πάροχοι διατηρούν όλες τις διαθέσιμες πληροφορίες σχετικά με τα περιστατικά ασφάλειας, για τα οποία έχουν υποβάλει Έκθεση Αναφοράς Περιστατικού Ασφάλειας, για διάστημα δύο (2) ετών από τον χρόνο υποβολής της Τελικής Έκθεσης Αναφοράς Συμβάντος Ασφάλειας, με την επιφύλαξη τήρησης της κείμενης νομοθεσίας περί προστασίας δεδομένων προσωπικού χαρακτήρα και τυχόν υποχρέωσης διατήρησής τους για μεγαλύτερο χρονικό διάστημα, εφόσον προβλέπεται από άλλες διατάξεις της κείμενης νομοθεσίας.

ΑΡΘΡΟ 8 – Διαχείριση Επιχειρησιακής Συνέχειας

8.1. Στρατηγική Συνέχειας των Παρεχόμενων Υπηρεσιών

Α. Ανάλυση Επιχειρησιακών Επιπτώσεων

8.1.1. Ο πάροχος, βασιζόμενος σε μεθοδολογία που λαμβάνει υπόψη τις διεθνείς πρακτικές, υλοποιεί Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis), με την οποία εντοπίζει και καταγράφει τις επιχειρησιακές λειτουργίες και τους πόρους που υποστηρίζουν τις λειτουργίες αυτές και σχετίζονται ή μπορεί να επηρεάσουν την ακεραιότητα του δικτύου και τη διαθεσιμότητα των υπηρεσιών.

8.1.2. Η Ανάλυση Επιχειρησιακών Επιπτώσεων περιλαμβάνει κατ' ελάχιστον τα παρακάτω:

8.1.2.1. Προσδιορισμό των επιπτώσεων που δύνανται να επέλθουν από γεγονότα που μπορεί να επηρεάσουν τις επιχειρησιακές λειτουργίες της παραγράφου 8.1.1 του παρόντος άρθρου.

8.1.2.2. Κατηγοριοποίηση των επιχειρησιακών λειτουργιών σύμφωνα με την προτεραιότητα αποκατάστασής τους, προκειμένου να επηρεάζεται στο ελάχιστο η λειτουργία του δικτύου και η διαθεσιμότητα των υπηρεσιών. Προς τούτο λαμβάνονται υπόψη, μεταξύ άλλων, ο αριθμός των χρηστών που επηρεάζεται από τη μη διαθεσιμότητα της υπηρεσίας, η γεωγραφική έκταση που εξυπηρετεί κάθε πόρος, καθώς και η γεωγραφική θέση αυτού.

8.1.2.3. Καθορισμός των πόρων (ΠΕΣ, εγκαταστάσεις, διαδικασίες, προσωπικό) που απαιτούνται για τη συνέχιση κάθε επιχειρησιακής λειτουργίας, καθώς και τυχόν εξαρτήσεις αυτών.

8.1.3. Ο πάροχος αναθεωρεί περιοδικά, και κατ' ελάχιστον ανά δύο (2) έτη ή μετά από την εκδήλωση σημαντικού περιστατικού ασφάλειας, την Ανάλυση Επιχειρησιακών Επιπτώσεων λαμβάνοντας υπόψη: α) επιχειρησιακές, οργανωτικές, ή τεχνολογικές αλλαγές, β) αλλαγές στο νομοθετικό πλαίσιο, σε εθνικό ή κοινοτικό επίπεδο, γ) τα αποτελέσματα των διενεργούμενων ελέγχων και δ) άλλα δεδομένα τα οποία οφείλει να λάβει υπόψη του.

8.1.4. Ο πάροχος διατηρεί καταγεγραμμένη την περιγραφή της εφαρμοσθείσας μεθοδολογίας Ανάλυσης Επιχειρησιακών Επιπτώσεων και τα αποτελέσματα εφαρμογής της.

Β. Σχέδιο Επιχειρησιακής Συνέχειας

8.1.5. Για την εξασφάλιση επιχειρησιακής συνέχειας, ο πάροχος διατηρεί και εφαρμόζει Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan), το οποίο βασίζεται στα αποτελέσματα της Αποτίμησης Κινδύνου, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού και της Ανάλυσης Επιχειρησιακών Επιπτώσεων, σε συμφωνία με τις αρχές της ενότητας 8.1.Α του παρόντος άρθρου, και το οποίο περιλαμβάνει:

8.1.5.1. Το προσωπικό που εμπλέκεται στην περίπτωση που απειλείται η επιχειρησιακή συνέχεια του παρόχου, καθώς και τους ρόλους και τις αρμοδιότητες του προσωπικού αυτού.

8.1.5.2. Τις διαδικασίες λήψης απόφασης, καθώς και τις συνθήκες κατά τις οποίες ενεργοποιούνται τα μέτρα για την εξασφάλιση της Επιχειρησιακής Συνέχειας και το εξουσιοδοτημένο για την ενεργοποίησή τους προσωπικό.

8.1.5.3. Τις διαδικασίες διάχυσης πληροφορίας στο αρμόδιο προσωπικό σχετικά με το εκάστοτε πρόβλημα.

8.1.5.4. Τις λειτουργικές διαδικασίες για την ανάλυση και εκτίμηση του προβλήματος.

8.1.5.5. Τις ενέργειες που πρέπει να γίνουν κατά προτεραιότητα, τις διαδικασίες και τους πόρους που απαιτούνται για την αποκατάσταση του δικτύου και των υπηρεσιών και το χρονοδιάγραμμα υλοποίησης.

8.1.5.6. Τους εκτιμώμενους χρόνους αποκατάστασης (Recovery Time Objectives) σε διαφορετικές συνθήκες βλάβης.

8.1.5.7. Τα στοιχεία και τους τρόπους επικοινωνίας του προσωπικού του παρόχου με τεχνικούς, προμηθευτές και εργολάβους του παρόχου, καθώς και με παρόχους άλλων δικτύων, καθώς και διαδικασίες συνεργασίας μεταξύ αυτών για την υλοποίηση των μέτρων για την εξασφάλιση της Επιχειρησιακής Συνέχειας.

8.1.5.8. Τις πληροφορίες σχετικά με τη διαθεσιμότητα εξοπλισμού αντικατάστασης.

8.1.5.9. Την αξιολόγηση των μέτρων που ελήφθησαν για την επίλυση συγκεκριμένου προβλήματος και τις διαδικασίες αναθεώρησης των μέτρων για την εξασφάλιση της Επιχειρησιακής Συνέχειας.

8.1.6. Το Σχέδιο Επιχειρησιακής Συνέχειας αναθεωρείται και αναπροσαρμόζεται από τον πάροχο σε τακτά χρονικά διαστήματα, λαμβάνοντας υπόψη συμβάντα που ενδεχομένως έλαβαν χώρα κατά το παρελθόν και τα αποτελέσματα που προκύπτουν από δοκιμές και ασκήσεις.

Γ. Εφεδρεία

8.1.7. Ο πάροχος εξασφαλίζει ότι υπάρχει στο δίκτυό του η κατάλληλη εφεδρεία, ώστε ενδεχόμενη βλάβη σε κάποιο ΠΕΣ να μην επηρεάσει καθοριστικά τη λειτουργία του δικτύου ή τις παρεχόμενες υπηρεσίες.

8.1.8. Ο πάροχος υλοποιεί λύσεις εφεδρείας, οι οποίες είναι ανάλογες της κρισιμότητας των ΠΕΣ, όπως αυτή έχει προκύψει από την Αποτίμηση Κινδύνου, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού. Για τα κρίσιμα ΠΕΣ, ο πάροχος υλοποιεί λύσεις αυτόματης εφεδρείας, σύμφωνα με τις διεθνείς πρακτικές, οι οποίες επιτρέπουν την αδιάλειπτη λειτουργία του δικτύου και των παρεχόμενων υπηρεσιών.

8.1.9. Σε περιπτώσεις που για κρίσιμα ΠΕΣ δεν είναι δυνατή η ύπαρξη μηχανισμού αυτόματης εφεδρείας, ο πάροχος λαμβάνει όλα τα απαραίτητα μέτρα και προβαίνει στις απαραίτητες ενέργειες για την ταχεία αποκατάσταση των λειτουργιών τους και την ελαχιστοποίηση των επιπτώσεων ενδεχόμενης βλάβης αυτών. Ο πάροχος προβαίνει σε σχεδιασμό, δοκιμή και έγγραφη τεκμηρίωση των μέτρων της παρούσας παραγράφου.

8.1.10. Όπου αυτό είναι εφαρμόσιμο, ο πάροχος υλοποιεί την εφεδρεία κατά τέτοιο τρόπο ώστε τα ΠΕΣ, τα οποία παρέχουν εφεδρεία μεταξύ τους, να είναι τοποθετημένα σε διαφορετικές εγκαταστάσεις. Εάν δεν είναι τεχνικά εφικτό τα εν λόγω ΠΕΣ να τοποθετηθούν σε διαφορετικές εγκαταστάσεις, θα πρέπει, όπου αυτό είναι δυνατόν, να είναι τοποθετημένα σε χώρους με ανεξάρτητα μέσα φυσικής προστασίας.

8.1.11. Ο πάροχος διασφαλίζει ότι υπάρχουν λειτουργικά διαθέσιμοι εφεδρικοί μηχανισμοί εναλλακτικής και φυσικά ανεξάρτητης όδευσης, ιδίως στο δίκτυο κορμού μετάδοσης, μεταγωγής και δρομολόγησης.

Δ. Παροχή Ενέργειας και Ασφάλεια Αναγκαίων Αγαθών

8.1.12. Ο πάροχος μεριμνά για την προστασία των ΠΕΣ από διακοπές ή διαταραχές του δημοσίου δικτύου παροχής ενέργειας, ώστε να εξασφαλίζεται η αδιάλειπτη λειτουργία τους .

8.1.13. Ο πάροχος μεριμνά ώστε η παροχή του δημοσίου δικτύου παροχής ενέργειας προς τα ΠΕΣ να γίνεται βάσει των ενδεδειγμένων προδιαγραφών.

8.1.14. Στην περίπτωση διακοπής του δημοσίου δικτύου παροχής ενέργειας, ο πάροχος εφαρμόζει τρόπους/μέσα εφεδρικής τροφοδοσίας (ενδεικτικά: εφεδρικές συστοιχίες, μπαταρίες, γεννήτριες) που ενεργοποιούνται αυτόματα. Για τον καθορισμό του χρονικού διαστήματος για το οποίο εξασφαλίζεται η συνέχεια λειτουργίας των ΠΕΣ μέσω εφεδρικής τροφοδοσίας λαμβάνονται υπόψη τα αποτελέσματα της Αποτίμησης Κινδύνου, σε συμφωνία με τις αρχές της Διαχείρισης Κινδύνου της ενότητας 3.2 του άρθρου 3 του παρόντος Κανονισμού και της ανάλυσης Επιχειρησιακών Επιπτώσεων της ενότητας 8.1.Α του παρόντος άρθρου.

8.1.15. Όπου αυτό είναι εφικτό, τα ΠΕΣ δεν εξυπηρετούνται από την ίδια πηγή τροφοδοσίας.

8.1.16. Τα μέσα εφεδρικής τροφοδοσίας συντηρούνται σύμφωνα με τις προδιαγραφές του κατασκευαστή και λαμβάνονται όλα τα μέτρα για την εξασφάλιση της εύρυθμης λειτουργίας τους. Σε περίπτωση που για τη λειτουργία των μέσων εφεδρικής τροφοδοσίας απαιτούνται πρώτες ύλες ή άλλα υλικά, ο πάροχος διατηρεί και εφαρμόζει διαδικασίες για την εξασφάλιση της επαρκούς διαθεσιμότητάς τους, ενδεχομένως και σε συνεργασία με τρίτους παρόχους όπου απαιτείται.

8.1.17. Ο πάροχος μεριμνά για την επάρκεια των επιπρόσθετων αναγκαίων αγαθών για την αδιάλειπτη λειτουργία των ΠΕΣ, όπως ενδεικτικά συστήματα κλιματισμού και καύσιμα.

8.2. Ανάκαμψη από Καταστροφή

8.2.1. Σε περίπτωση καταστροφικής βλάβης του δικτύου ή σε περιπτώσεις ανωτέρας βίας, ισχύουν τα οριζόμενα στη διάταξη του άρθρου 216 του ν. 4727/2020 (ΦΕΚ 184/Α/23.09.2020), όπως ισχύει.

8.2.2. Σε περιπτώσεις εκτάκτου ανάγκης, ο πάροχος συνεργάζεται κατά τις κείμενες διατάξεις με τις Αρμόδιες Αρχές και εφαρμόζει, όποτε αυτό είναι αναγκαίο, σχέδιο εκτάκτου ανάγκης, με το οποίο προσδιορίζεται η διαδικασία με την οποία θα παρέχει υπηρεσίες σε περιοχές που έχουν κηρυχτεί σε έκτακτη ανάγκη και για όσο διάστημα αυτή υφίσταται, σύμφωνα με την κείμενη νομοθεσία.

ΑΡΘΡΟ 9 – Διαχείριση Παρακολούθησης και Ελέγχου

9.1. Διαδικασία Διαχείρισης Παρακολούθησης και Ελέγχου

9.1.1. Ο πάροχος διατηρεί και εφαρμόζει Διαδικασία Διαχείρισης Παρακολούθησης και Ελέγχου των ΠΕΣ, των υπηρεσιών/εφαρμογών τους και των εγκαταστάσεών τους, η οποία προβλέπει κατ' ελάχιστον τις ακόλουθες ενέργειες: α) την οργάνωση του προσωπικού του παρόχου (ορισμός ρόλων και αρμοδιοτήτων) με σκοπό την αποτελεσματική εφαρμογή της εν λόγω διαδικασίας, β) την κατηγοριοποίηση των απαραίτητων συμβάντων και συναγερμών, γ) την καταγραφή, διαχείριση και αξιολόγηση των συμβάντων και συναγερμών, με σκοπό τόσο τον προσδιορισμό κακόβουλων ενεργειών, σφαλμάτων και κενών ασφαλείας σε πραγματικό χρόνο όσο και τον εντοπισμό των περιστατικών ασφάλειας, δ) την οργάνωση και κατηγοριοποίηση των ελέγχων εφαρμογής της

Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών και των ασκήσεων και δοκιμών του Σχεδίου Επιχειρησιακής Συνέχειας, ε) την ενημέρωση του Υπεύθυνου Ασφάλειας Δικτύων και Υπηρεσιών και των αρμοδίων στελεχών του παρόχου.

9.1.2. Ο πάροχος αξιολογεί και αναθεωρεί τη Διαδικασία Διαχείρισης Παρακολούθησης και Ελέγχου με βάση προηγούμενη εμπειρία του.

9.2. Παρακολούθηση Συμβάντων και Συναγερμών

9.2.1. Ο πάροχος παρακολουθεί συνεχώς και σε πραγματικό χρόνο τα συμβάντα που λαμβάνουν χώρα στα ΠΕΣ, στις υπηρεσίες/εφαρμογές τους και στις εγκαταστάσεις τους αναφορικά με την ασφάλεια των δικτύων και υπηρεσιών, ώστε να εντοπίζονται εγκαίρως οι τυχόν κακόβουλες ενέργειες, σφάλματα ή κενά ασφάλειας. Ανάλογα με το είδος, τη φύση και τη σοβαρότητα ενός συμβάντος ενεργοποιείται αντίστοιχος συναγερμός. Ενδεικτικά, και όχι περιοριστικά, ως συμβάντα αναφέρονται: i) οι επανειλημμένες ανεπιτυχείς προσπάθειες πρόσβασης σε ΠΕΣ, υπηρεσίες/εφαρμογές και στους χώρους ή τις εγκαταστάσεις αυτών, ii) πρόσβαση ή μεταβολή στη διαμόρφωση των ΠΕΣ και των υπηρεσιών/εφαρμογών τους, iii) πρόσβαση ή μεταβολή σε ευαίσθητα αρχεία, όπως αρχεία που διατηρούν δικτυακά δεδομένα ή αρχεία εντολών για πρόσβαση σε δεδομένα επικοινωνίας συνδρομητών, iv) αλλαγές στην κατάσταση και τη λειτουργία των ΠΕΣ και των υπηρεσιών/εφαρμογών τους, όπως η επανεκκίνηση ή η βίαιη διακοπή λειτουργίας τους, v) κάθε μη σύνηθες συμβάν που εντοπίζεται από τους μηχανισμούς ή τα συστήματα που αναφέρονται στην παράγραφο 5.3.1 του άρθρου 5 του παρόντος Κανονισμού.

9.2.2. Για την παρακολούθηση των συμβάντων και των συναγερμών στα ΠΕΣ, ο πάροχος χρησιμοποιεί σύγχρονα συστήματα και λειτουργίες. Στην κατηγορία αυτή εντάσσονται ενδεικτικά τα Κέντρα Λειτουργίας και Ασφάλειας Δικτύου (Network Operations Center – NOC, Security Operations Center – SOC), τα εργαλεία διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management – SIEM), η παροχή αναφορών/συμβουλών από Ομάδες Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών (Computer Security Incident Response Team – CSIRT) και άλλες δομές και υποστηρικτικά εργαλεία εντοπισμού δικτυακών και πληροφοριακών συμβάντων ή συναγερμών.

9.2.3. Ανάλογα με την κρισιμότητα των συμβάντων και των συναγερμών, ο πάροχος ενεργοποιεί τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας της ενότητας 7.1 του άρθρου 7 του παρόντος Κανονισμού.

9.3. Διατήρηση Αρχείων Καταγραφής των ΠΕΣ και Όροι Διατήρησης Αρχείων

9.3.1. Ο πάροχος τηρεί τα ακόλουθα αρχεία καταγραφής των ΠΕΣ:

(α) αρχείο καταγραφής των προσβάσεων στα ΠΕΣ, στο οποίο καταγράφονται, κατ' ελάχιστον, το όνομα χρήστη που απέκτησε την πρόσβαση και η ημερομηνία και ώρα εκκίνησης και τερματισμού της πρόσβασης.

(β) αρχείο καταγραφής ενεργειών στο λειτουργικό σύστημα, στις βάσεις δεδομένων και στις εφαρμογές των ΠΕΣ. Κάθε πρόσβαση σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών πρέπει επιπλέον να αιτιολογείται.

(γ) αρχείο καταγραφής με τα συμβάντα και τους συναγερμούς των ΠΕΣ.

9.3.2. Αναφορικά με τα αρχεία καταγραφής της παραγράφου 9.3.1 του παρόντος άρθρου:

(α) Ο πάροχος εξασφαλίζει ότι οι καταγραφές που περιλαμβάνονται στα αρχεία καταγραφής είναι πλήρεις και συνεχείς.

(β) Ο πάροχος 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 τις τεχνικές διασφάλισης της ακεραιότητας, της εμπιστευτικότητας, της διαθεσιμότητας και της χρονοσήμανσης (timestamp) των καταγραφών.

(γ) Σε περίπτωση διακοπής των καταγραφών που προβλέπονται στα αρχεία καταγραφής, καθώς και σε περίπτωση περιστατικού παραβίασης της ακεραιότητας, εμπιστευτικότητας, διαθεσιμότητας και χρονοσήμανσης των καταγραφών, ο πάροχος ενεργοποιεί αμελλητί τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας της ενότητας 7.1 του άρθρου 7 του παρόντος Κανονισμού.

9.3.3. Με τα άρθρα 3 έως και 10 του παρόντος Κανονισμού ορίζεται υποχρέωση διατήρησης αρχείων για τον σκοπό του ελέγχου της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών. Με την επιφύλαξη των διατάξεων της κείμενης νομοθεσίας περί προστασίας δεδομένων προσωπικού χαρακτήρα, των ν.3471/2006 (ΦΕΚ Α'133), ν.3783/2009 (ΦΕΚ Α'136), ν.3917/2011 (ΦΕΚ Α'22), όπως ισχύουν, και της τήρησης υποχρεώσεων που τυχόν απορρέουν από άλλες διατάξεις της κείμενης νομοθεσίας, ο πάροχος διατηρεί τα εν λόγω αρχεία για χρονικό διάστημα τουλάχιστον δύο (2) ετών, λαμβάνοντας τα κατάλληλα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς τους. Ειδικά ως προς τα συστήματα για την άρση του απορρήτου των επικοινωνιών (συστήματα νόμιμης επισύνδεσης και διατήρησης δεδομένων), ο πάροχος διατηρεί τα αρχεία καταγραφής της παραγράφου 9.3.1 του παρόντος άρθρου για χρονικό διάστημα τουλάχιστον δέκα (10) ετών. Σε περίπτωση που βρίσκεται σε εξέλιξη έλεγχος της ΑΔΑΕ, ο πάροχος διατηρεί τα αρχεία της παρούσας παραγράφου ακόμα και μετά το πέρας του κατά τα ως άνω προβλεπόμενου χρόνου διατήρησης και προβαίνει στη διαγραφή τους μόνο κατόπιν σχετικής απόφασης της ΑΔΑΕ.

9.4. Ασκήσεις Σχεδίου Επιχειρησιακής Συνέχειας

9.4.1. Ο πάροχος διενεργεί περιοδικά ελέγχους εφαρμογής και δοκιμές του Σχεδίου Επιχειρησιακής Συνέχειας της ενότητας 8.1.Β του άρθρου 8 του παρόντος Κανονισμού, και προβαίνει, άπαξ ετησίως, με τη συμμετοχή των εμπλεκόμενων εργαζομένων και συνεργατών του, σε ασκήσεις ετοιμότητας που αφορούν το σύνολο του δικτύου του, προκειμένου να διασφαλίζεται ότι όλο το εμπλεκόμενο στην εκτέλεση του Σχεδίου προσωπικό έχει την κατάλληλη εκπαίδευση και ότι οι περιγραφόμενες σε αυτό διαδικασίες για την ανάκαμψη των επιχειρησιακών λειτουργιών είναι έγκυρες και αποτελεσματικές.

9.4.2. Ο προγραμματισμός των ως άνω ασκήσεων πραγματοποιείται στην αρχή κάθε έτους και κατά τη διενέργειά τους δύναται να παρίσταται και η ΑΔΑΕ. Για τον σκοπό αυτόν, ο πάροχος ενημερώνει εγκαίρως την ΑΔΑΕ αναφορικά με τη διενέργεια των ασκήσεων. Ειδικώς σε ό,τι αφορά στη διενέργεια των ασκήσεων από τους τρείς μεγαλύτερους τηλεπικοινωνιακούς παρόχους αυτές διεξάγονται με την υποχρεωτική παρουσία της ΑΔΑΕ. Για τον σκοπό αυτό, ο πάροχος ενημερώνει

εγκαίρως την ΑΔΑΕ αναφορικά με τη διενέργεια των εν λόγω ασκήσεων και οριστικοποιεί την ημερομηνία διενέργειάς τους σε συμφωνία με την ΑΔΑΕ.

9.4.3. Ο πάροχος διατηρεί σε αρχείο την τεκμηρίωση αναφορικά με τη διενέργεια των ως άνω ασκήσεων.

9.5. Εσωτερικός Έλεγχος Εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών

9.5.1. Ο πάροχος προβαίνει σε προγραμματισμό εσωτερικού ελέγχου εφαρμογής της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών, με σκοπό την ορθή τήρηση των απαιτήσεων αυτής και τη διαπίστωση της επάρκειας και αποτελεσματικότητας των μηχανισμών ασφάλειας. Ο εσωτερικός έλεγχος βασίζεται σε διεθνείς, βέλτιστες πρακτικές, καταγράφεται σε αρχείο, καλύπτει όλο το εύρος εφαρμογής της Πολιτικής και πραγματοποιείται κατ' ελάχιστον ανά δύο (2) έτη.

9.5.2. Ο εσωτερικός έλεγχος περιλαμβάνει τη χρήση και την εξέταση των αρχείων καταγραφής της παραγράφου 9.3.1 του παρόντος άρθρου, κατά περίπτωση σε συσχετισμό με άλλα αρχεία που προβλέπονται στον παρόντα Κανονισμό. Επιπλέον, ο εσωτερικός έλεγχος περιλαμβάνει τεχνικούς ελέγχους διείσδυσης (penetration tests) στα ΠΕΣ.

9.5.3. Ο εσωτερικός έλεγχος είναι δυνατό να πραγματοποιείται από εξωτερικό φορέα ή από ειδικά εξουσιοδοτημένους προς τούτο, εργαζόμενους του παρόχου, λαμβάνοντας υπόψη τις αρχές της αντικειμενικότητας και της αμεροληψίας. Σε κάθε περίπτωση, λαμβάνεται μέριμνα από τον πάροχο αναφορικά με ζητήματα τήρησης της εμπιστευτικότητας και μη διαρροής πληροφοριών και δεδομένων.

9.5.4. Διαδικασία Εσωτερικού Ελέγχου

9.5.4.1. Ο εσωτερικός έλεγχος εφαρμογής της Πολιτικής περιλαμβάνει τα ακόλουθα στάδια: α) την προετοιμασία του ελέγχου, β) τη διεξαγωγή του ελέγχου και γ) τα αποτελέσματα του ελέγχου. Ο πάροχος διατηρεί σε αρχείο την τεκμηρίωση για κάθε στάδιο του ελέγχου, ακόμη και στην περίπτωση που δεν υπάρχουν ευρήματα από τον έλεγχο.

9.5.4.2. Κατά το στάδιο της προετοιμασίας του εσωτερικού ελέγχου, ο πάροχος καθορίζει τα συστήματα και τις διαδικασίες/μηχανισμούς που θα ελεγχθούν, το χρονοδιάγραμμα και τον ορισμό των προσώπων που απαρτίζουν την Ομάδα Εσωτερικού Ελέγχου.

9.5.4.3. Κατά το στάδιο της διεξαγωγής του εσωτερικού ελέγχου, η απόδοση σε ένα ή περισσότερα μέλη της Ομάδας Εσωτερικού Ελέγχου δικαιωμάτων πρόσβασης σε εργαλεία λογισμικού, συστήματα ή χώρους των εγκαταστάσεων επιτρέπεται μόνο για το χρονικό διάστημα του αντίστοιχου εσωτερικού ελέγχου και πραγματοποιείται σύμφωνα με την Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών του παρόχου.

9.5.4.4. Σε περίπτωση που προκύψουν ευρήματα από τον εσωτερικό έλεγχο, ο πάροχος ορίζει τις απαιτούμενες ενέργειες (όπως, ενδεικτικά, αναθεώρηση διαδικασιών/οδηγιών, επικαιροποίηση λογισμικού, τροποποίηση παραμέτρων τεχνικής διαμόρφωσης, 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.

9.5.4.5. Ανάλογα με τη φύση και την κρισιμότητα των ευρημάτων του εσωτερικού ελέγχου, ο πάροχος ενεργοποιεί τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας της ενότητας 7.1 του άρθρου 7 του παρόντος Κανονισμού.

ΑΡΘΡΟ 10 – Ευαισθητοποίηση σε Θέματα Απειλών και Ενημέρωση Χρηστών/Συνδρομητών

10.1. Συλλογή και Διαχείριση Πληροφοριών για Απειλές

10.1.1. Ο πάροχος διατηρεί και εφαρμόζει Διαδικασία για την Παρακολούθηση, Συλλογή και Διαχείριση πληροφοριών σχετικά με πιθανές απειλές ασφάλειας του δικτύου και των υπηρεσιών του, η οποία περιλαμβάνει κατ' ελάχιστον τα παρακάτω:

10.1.1.1. Ο πάροχος παρακολουθεί τακτικά πληροφορίες και στοιχεία ανάλυσης απειλών (threat intelligence) από σχετικές, τρέχουσες και αξιόπιστες εξωτερικές πηγές πληροφόρησης, όπως ενδεικτικά πληροφορίες διαθέσιμες στο ευρύ κοινό, πληροφορίες ασφαλείας ανοιχτής πηγής, εκθέσεις ανάλυσης απειλών από εμπορικούς φορείς, κατασκευαστές εξοπλισμού και λογισμικού και ακαδημαϊκούς και ερευνητικούς φορείς, καθώς και άτυπες και περιστασιακές κοινοποιήσεις στοιχείων ανάλυσης απειλών από σχετικούς οργανισμούς και φορείς στη βάση διμερών σχέσεων.

10.1.1.2. Ο πάροχος αναλύει, αξιολογεί, συσχετίζει και χαρακτηρίζει τις συλλεχθείσες πληροφορίες για απειλές.

10.1.1.3. Ο πάροχος ορίζει τους τρόπους λήψης απόφασης, καθώς και τις συνθήκες κατά τις οποίες ενεργοποιούνται τα μέτρα για την ελαχιστοποίηση και τον περιορισμό των συνεπειών/επιπτώσεων από απειλές ασφάλειας του δικτύου και των υπηρεσιών του.

10.1.1.4. Ο πάροχος ορίζει τους τρόπους διάχυσης και κοινοποίησης των πληροφοριών και στοιχείων ανάλυσης απειλών σε συνεργασία με σχετικούς οργανισμούς και φορείς στη βάση διμερών σχέσεων, καθώς και τους κανόνες σήμανσης ευαίσθητων πληροφοριών περί απειλών ασφάλειας για την απλούστευση κοινοποίησης και διάδοσης των πληροφοριών περί απειλών.

10.2. Ευαισθητοποίηση και Ενημέρωση Χρηστών/Συνδρομητών

10.2.1. Ο πάροχος 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 ασφάλεια των επικοινωνιών τους, ιδίως σχετικά με τους κανόνες ενδεδειγμένης χρήσης για την προστασία των κωδικών πρόσβασης που κατέχουν, τους κανόνες ορθής χρήσης των παρεχόμενων δικτύων ή υπηρεσιών, αλλά και τους τρόπους χρήσης τεχνολογιών και πόρων σχετικών με την ασφάλεια των πληροφοριών.

10.2.2. Ο πάροχος ενημερώνει τους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών για συγκεκριμένες και σημαντικές απειλές που ενδέχεται να τους επηρεάσουν, σύμφωνα με την κείμενη νομοθεσία. Η ενημέρωση αυτή δύναται να παρέχεται μέσω τακτικών ή/και έκτακτων δελτίων ασφαλείας που εκδίδει ο πάροχος, μέσω ιστοθέσης του δικτυακού τόπου του με

αποκλειστικό θέμα τις απειλές ασφαλείας ή μέσω οποιουδήποτε ευρέως χρησιμοποιούμενου τρόπου παροχής της σχετικής πληροφόρησης.

ΜΕΡΟΣ Γ – Έλεγχος, Υποχρεώσεις Παρόχων, Μεταβατικές και Τελικές Διατάξεις

ΑΡΘΡΟ 11 – Διαδικασία Ελέγχου από την ΑΔΑΕ

11.1. Η ΑΔΑΕ διενεργεί τακτικούς ελέγχους περιοδικά στους παρόχους, προκειμένου να διαπιστώσει τη συμμόρφωσή τους με την εγκριθείσα από την ΑΔΑΕ Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών. Επίσης, η ΑΔΑΕ, στο πλαίσιο των αρμοδιοτήτων της, διενεργεί έκτακτους ελέγχους στους παρόχους, αυτεπαγγέλτως ή κατόπιν καταγγελίας ή περιστατικού ασφάλειας.

11.2. Ο έλεγχος διενεργείται από την ΑΔΑΕ με την παρουσία του Υπεύθυνου Ασφάλειας Δικτύων και Υπηρεσιών, όπως αυτός προβλέπεται στην παράγραφο 3.3.2. του άρθρου 3 του παρόντος Κανονισμού, ή άλλου εξουσιοδοτημένου προς τούτο εργαζόμενου του παρόχου, σύμφωνα με τα ακολούθως οριζόμενα:

11.2.1. Η ΑΔΑΕ με απόφασή της ορίζει ομάδα ελέγχου, με σκοπό τον έλεγχο συγκεκριμένου παρόχου. Με την ίδια απόφαση καθορίζεται η ειδικότερη σύνθεση της ομάδας ελέγχου.

11.2.2. Ο τακτικός έλεγχος διενεργείται με επιτόπια επίσκεψη στις εγκαταστάσεις του παρόχου και συμπληρωματική αλληλογραφία όπου κρίνεται απαραίτητο. Η ομάδα ελέγχου ενημερώνει εγγράφως τον Υπεύθυνο Ασφάλειας Δικτύων και Υπηρεσιών για την ημερομηνία διενέργειας του ελέγχου, ζητώντας του παράλληλα να έχει διαθέσιμα πλήρη αντίγραφα των υφισταμένων διαδικασιών που υλοποιούν την εγκριθείσα από την ΑΔΑΕ Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών, από τα οποία να προκύπτει σαφώς η ημερομηνία έκδοσής τους. Η ομάδα ελέγχου ζητά, κατά την κρίση της, τα απαραίτητα στοιχεία και συνεργάζεται με το προσωπικό του ελεγχόμενου προσώπου.

11.2.3. Ο έκτακτος έλεγχος διενεργείται χωρίς την προηγούμενη ενημέρωση του παρόχου σχετικά με το αντικείμενο του ελέγχου και δύναται να διεξάγεται με επιτόπια επίσκεψη στις εγκαταστάσεις του παρόχου ή εξ αποστάσεως με ψηφιακά μέσα ή δια αλληλογραφίας.

11.2.4. Από τη λήψη της έγγραφης ενημέρωσης του Υπεύθυνου Ασφάλειας Δικτύων και Υπηρεσιών περί της διεξαγωγής τακτικού ελέγχου από την ΑΔΑΕ και εν γένει από την έναρξη κάθε είδους ελέγχου και μέχρι να λάβει έγγραφη ενημέρωση από την Αρχή αναφορικά με το πέρας του ελέγχου, ο πάροχος δεν δύναται να προβεί σε οποιαδήποτε αναθεώρηση του κειμένου της εγκριθείσας Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών ή των συνοδευτικών αρχείων αυτής (διαδικασίες, τεχνικές οδηγίες κ.ά.).

11.2.5. Για κάθε επιτόπιο έλεγχο συντάσσεται ειδικό έγγραφο με τίτλο «Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις του παρόχου», το οποίο συνυπογράφεται από τον Υπεύθυνο Ασφάλειας Δικτύων και Υπηρεσιών ή τον εξουσιοδοτημένο προς τούτο εργαζόμενο του παρόχου που συνέπραξε στον επιτόπιο έλεγχο καθώς και την ομάδα ελέγχου της ΑΔΑΕ.

11.3. Μετά την ολοκλήρωση όλων των αναγκαίων επιμέρους ελέγχων, η ομάδα ελέγχου εξετάζει διεξοδικά το σύνολο των συλλεχθέντων στοιχείων και συντάσσει ειδικό έγγραφο με τίτλο «Έκθεση διενέργειας τακτικού / εκτάκτου ελέγχου στον πάροχο», το οποίο περιλαμβάνει απαραιτήτως τα ακόλουθα στοιχεία:

α) Τα στοιχεία της Απόφασης της ΑΔΑΕ με την οποία αποφασίστηκε η διενέργεια του 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 παρόχου, καθώς και το όνομα του Υπευθύνου Ασφάλειας Δικτύων και Υπηρεσιών,

δ) Τα Πρακτικά Διενέργειας Επιτόπιων Ελέγχων στις εγκαταστάσεις του ελεγχόμενου παρόχου, με αναγραφή των συγκεκριμένων ημερομηνιών που αυτοί έλαβαν χώρα, καθώς και κάθε σχετική έγγραφη επικοινωνία μεταξύ της ΑΔΑΕ και του παρόχου στο πλαίσιο της διεξαγωγής του ελέγχου,

ε) Αναλυτική περιγραφή των ευρημάτων του ελέγχου και διαπίστωση τυχόν παραλείψεων ή αναντιστοιχιών με την εγκριθείσα από την ΑΔΑΕ Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών και την κείμενη νομοθεσία, καθώς και καταγραφή παρατηρήσεων αναφορικά με την εφαρμογή της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών.

στ) Τελικό πόρισμα του ελέγχου.

11.4. Η Απόφαση της Ολομέλειας της ΑΔΑΕ για την έγκριση της «Έκθεσης διενέργειας ελέγχου στον πάροχο», μετά της συνημμένης σε αυτήν έκθεσης, γνωστοποιείται στον ελεγχόμενο πάροχο.

ΑΡΘΡΟ 12 – Υποχρέωση Ενημέρωσης της ΑΔΑΕ

12.1. Οι πάροχοι της παραγράφου 1.3 του άρθρου 1 του παρόντος Κανονισμού υποχρεούνται εντός προθεσμίας δύο (2) μηνών από τη δημοσίευση του παρόντος στην Εφημερίδα της Κυβερνήσεως, να δηλώσουν προς την ΑΔΑΕ με υπεύθυνη δήλωση του νόμιμου εκπροσώπου τους:

α. τις δραστηριότητες για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην ΕΕΤΤ για τη λειτουργία υπό καθεστώς Γενικής Αδείας.

Β. εάν ασκούν εν τοις πράγμασι τις δραστηριότητες για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην ΕΕΤΤ, περιγράφοντας αναλυτικά τις ασκούμενες δραστηριότητες και τα είδη των ΠΕΣ για την άσκηση αυτών των δραστηριοτήτων.

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

12.2. Οι πάροχοι της παραγράφου 1.3 του άρθρου 1 του παρόντος Κανονισμού, οι οποίοι ξεκινούν την άσκηση δραστηριότητας ή δραστηριοτήτων για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην ΕΕΤΤ για τη λειτουργία υπό καθεστώς Γενικής Αδείας μετά την έναρξη ισχύος του παρόντος Κανονισμού, υποχρεούνται να υποβάλουν την ανωτέρω δήλωση εντός προθεσμίας δύο (2) μηνών από την έναρξη των εν λόγω δραστηριοτήτων.

12.3. Οι πάροχοι της παραγράφου 1.3 του άρθρου 1 του παρόντος Κανονισμού οφείλουν να ενημερώνουν αμελλητί την ΑΔΑΕ 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 ΕΕΤΤ καθώς και στην περίπτωση που επέλθει μεταβολή στην εταιρική μορφή, στην επωνυμία και στην έδρα τους.

ΑΡΘΡΟ 13 – Υποβολή και Υλοποίηση Πολιτικής Ασφάλειας

13.1. Οι πάροχοι της παραγράφου 1.3 του άρθρου 1 του παρόντος Κανονισμού, οι οποίοι ασκούν εν τοις πράγμασι τις δραστηριότητες για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην

ΕΕΤΤ, υποχρεούνται να υποβάλουν στην ΑΔΑΕ προς έγκριση Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών, εντός προθεσμίας έξι (6) μηνών από τη δημοσίευση του παρόντος στην Εφημερίδα της Κυβερνήσεως.

13.2. Οι πάροχοι της παραγράφου 1.3 του άρθρου 1 του παρόντος Κανονισμού οι οποίοι ξεκινούν ή μεταβάλλουν την άσκηση δραστηριότητας ή δραστηριοτήτων για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην ΕΕΤΤ μετά την έναρξη ισχύος του παρόντος Κανονισμού, υποχρεούνται να υποβάλουν στην ΑΔΑΕ προς έγκριση Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών, εντός προθεσμίας έξι (6) μηνών από την έναρξη ή μεταβολή των ως άνω δραστηριοτήτων.

13.3. Οι πάροχοι υποχρεούνται εντός προθεσμίας έξι (6) μηνών από τη γνωστοποίηση σε αυτούς της απόφασης της ΑΔΑΕ περί έγκρισης της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών να την υλοποιήσουν και να ενημερώσουν εγγράφως την ΑΔΑΕ. Σε περίπτωση υποβολής αναθεωρημένης Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών, ο χρόνος υλοποίησής της θα ορίζεται κατά περίπτωση από την ΑΔΑΕ και θα γνωστοποιείται στον πάροχο με την απόφαση περί έγκρισης της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών.

13.4. Οι πάροχοι δεν υποβάλουν στην ΑΔΑΕ προς έγκριση τις διαδικασίες ασφάλειας που προβλέπονται στο πλαίσιο του παρόντος Κανονισμού.

ΑΡΘΡΟ 14 – Μεταβατικές Διατάξεις

14.1. Ο Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών (υπ' αριθμ. 165/2011 Απόφαση της ΑΔΑΕ, ΦΕΚ Β΄2715/2011) και ο Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών (υπ' αριθμ. 205/2013 Απόφαση της ΑΔΑΕ, ΦΕΚ Β΄1742/2013) παραμένουν σε ισχύ μέχρι την έναρξη ισχύος του παρόντος Κανονισμού, και καταργούνται από την έναρξη ισχύος του παρόντος.

14.2. Οι πάροχοι εφαρμόζουν την Πολιτική Ασφάλειας που έχουν υποβάλει στην ΑΔΑΕ σε εκπλήρωση της σχετικής υποχρέωσής τους με βάση την καταργούμενη δια του παρόντος υπ' αριθμ. 165/2011 Απόφαση της ΑΔΑΕ, καθώς και τα οριζόμενα στην καταργούμενη δια του παρόντος υπ' αριθμ. 205/2013 Απόφαση της ΑΔΑΕ, μέχρι την υλοποίηση της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών, όπως αυτή εγκρίνεται από την ΑΔΑΕ, σύμφωνα με τον παρόντα Κανονισμό και σε κάθε περίπτωση μέχρι το πέρας της οριζόμενης στην παράγραφο 13.3 του άρθρου 13 του παρόντος Κανονισμού προθεσμίας υλοποίησης της Πολιτικής Ασφάλειας Δικτύων και Υπηρεσιών.

14.3. Οι πάροχοι που έχουν αποστείλει στην ΑΔΑΕ ενημέρωση σχετικά με τις δραστηριότητες για τις οποίες έχουν υποβάλει Δήλωση Καταχώρησης στην ΕΕΤΤ για τη λειτουργία υπό καθεστώς Γενικής Αδείας, σε εκπλήρωση σχετικής υποχρέωσής τους με βάση την καταργούμενη δια του παρόντος υπ' αριθμ. 165/2011 Απόφαση της ΑΔΑΕ, δεν υποχρεούνται να υποβάλουν εκ νέου ενημέρωση, σύμφωνα με τα οριζόμενα στο άρθρο 12 του παρόντος, εφόσον δεν έχουν υπάρξει μεταβολές των εν λόγω δραστηριοτήτων και των ειδών των ΠΕΣ που χρησιμοποιούνται για την άσκησή τους.

14.4. Οι πάροχοι που έχουν υποβάλει στην ΑΔΑΕ Πολιτική Ασφάλειας σε εκπλήρωση σχετικής υποχρέωσής τους με βάση την καταργούμενη δια του παρόντος υπ' αριθμ. 165/2011 Απόφαση της ΑΔΑΕ υποχρεούνται, χωρίς άλλη ειδοποίηση, να υποβάλουν στην ΑΔΑΕ προς έγκριση Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών, σύμφωνα με τις προθεσμίες και τις απαιτήσεις του παρόντος Κανονισμού.

ΑΡΘΡΟ 15 – Έναρξη ισχύος

Η ισχύς του παρόντος Κανονισμού αρχίζει έξι (6) μήνες μετά τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως, υπό την επιφύλαξη των υποχρεώσεων που προβλέπονται στις διατάξεις των παραγράφων 12.1 του άρθρου 12 και 13.1 του άρθρου 13 αυτού, οι οποίες ισχύουν από τη δημοσίευση του παρόντος στην Εφημερίδα της Κυβερνήσεως.

Ο παρών Κανονισμός να δημοσιευτεί στην Εφημερίδα της Κυβερνήσεως.

Παράρτημα – Ορισμός παραμέτρων που καθορίζουν την υποχρέωση κοινοποίησης περιστατικού ασφάλειας

1. Καθορισμός Ποσοτικών παραμέτρων

1.1 Περιστατικά ασφάλειας που αφορούν στην ακεραιότητα, στη διαθεσιμότητα και στην αυθεντικότητα.

Για την περίπτωση περιστατικών ασφάλειας που αφορούν στην ακεραιότητα, στη διαθεσιμότητα και στην αυθεντικότητα δικτύων και υπηρεσιών, ο Πίνακας 1 αποτυπώνει το εκτιμώμενο πλήθος των χρηστών που επηρεάζονται σε συνάρτηση με τη χρονική διάρκεια εκδήλωσης του περιστατικού ασφάλειας, για τους σκοπούς του καθορισμού της υποχρέωσης κοινοποίησης του περιστατικού.

Ως χρονική διάρκεια ορίζεται το χρονικό διάστημα από τη στιγμή που το περιστατικό ασφάλειας έλαβε χώρα ή, στην περίπτωση που αυτό δεν είναι γνωστό, από τη στιγμή που ο πάροχος εκτιμά ότι ξεκίνησε ή αν αυτό δεν είναι εφικτό, από τη στιγμή που αντιλήφθηκε το περιστατικό ασφάλειας, έως την αποκατάσταση της ακεραιότητας του δικτύου ή της συνέχειας των παρεχόμενων υπηρεσιών.

Πίνακας 1: Ποσοτικές παράμετροι για το καθορισμό υποχρέωσης κοινοποίησης περιστατικών διαθεσιμότητας

Χρονική Διάρκεια	1 – 2 ώρες	2 – 4 ώρες	4 – 6 ώρες	6 – 8 ώρες	> 8 ώρες
Χρήστες Υπηρεσίας	>350.000	>200.000	>100.000	>50.000	>30.000

1.2 Περιστατικά ασφάλειας που αφορούν στο απόρρητο.

Για την περίπτωση των περιστατικών ασφάλειας που αφορούν στο απόρρητο, ο παρόχος οφείλει να κοινοποιήσει το περιστατικό ασφάλειας ανεξάρτητα από το πλήθος των χρηστών που επηρεάστηκαν ή τη χρονική του διάρκεια.

2. Καθορισμός Ποιοτικών παραμέτρων

Οι ποιοτικές παράμετροι που λαμβάνονται υπόψη στο πλαίσιο της υποχρέωσης κοινοποίησης περιστατικών είναι οι ακόλουθες :

i) Σημαντικός αντίκτυπος σε συνάρτηση με α) το γεωγραφικό εύρος του περιστατικού (διασυνοριακό περιστατικό, απομακρυσμένες ορεινές/νησιωτικές γεωγραφικές περιοχές) β) τον επηρεαζόμενο πληθυσμό (πλέον του 75% του συνολικού εκτιμώμενου αριθμού χρηστών που εξυπηρετούνται από την υπηρεσία του παρόχου στις απομακρυσμένες γεωγραφικές περιοχές κατά τον χρόνο εκδήλωσης του περιστατικού) και γ) τη χρονική διάρκεια του περιστατικού. (πλέον των 8 ωρών).

ii) Σε περίπτωση βλάβης δικτύου που επηρεάζει την κάλυψη τηλεπικοινωνιακών υπηρεσιών σε κρίσιμες υποδομές και όταν δημιουργείται βλάβη στο Δίκτυο από έκτακτες καταστάσεις (π.χ. πυρκαγιά, πλημμύρα) ο πάροχος οφείλει να ενημερώνει αμελλητί την ΑΔΑΕ.

iii) Σημαντικός αντίκτυπος σε συνάρτηση με τις επιπτώσεις στις οικονομικές και κοινωνικές δραστηριότητες ή στους χρήστες, π.χ. έλλειψη πρόσβασης στο 112 ή/και σε εθνικούς αριθμούς έκτακτης ανάγκης ή δημόσια συστήματα προειδοποίησης, μεγάλες υλικές ζημιές, υψηλός κίνδυνος για τη δημόσια ασφάλεια, αντίκτυπος σε ιδιαίτερα κρίσιμες ημέρες όπως ημέρες εκλογών ή δημοψηφισμάτων.

iv) Σε περίπτωση μη αποκατάστασης βλάβης μετά την παρέλευση 7 ημερολογιακών ημερών, ο πάροχος οφείλει να ενημερώσει την ΑΔΑΕ για την βλάβη με ειδική αιτιολόγηση της καθυστέρησης αποκατάστασης της βλάβης.

v) Η ΑΔΑΕ μπορεί με απόφασή της να ορίζει σε ειδικές καταστάσεις ή σε περιοχές με ιδιαίτερο ενδιαφέρον, πρόσθετες παραμέτρους κοινοποίησης περιστατικών διαθεσιμότητας με προσδιορισμένη χρονική ισχύ της κάθε απόφασης.