

Αριθμός 253

Ο ΠΕΡΙ ΡΥΘΜΙΣΕΩΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΚΑΙ ΤΑΧΥΔΡΟΜΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΝΟΜΟΣ ΤΟΥ 2004

Διάταγμα σύμφωνα με τα άρθρα 2(2)ζ, 18(3)(στ), 19(1), 20 (ιε), 20 (κε), 25, 28, 37(5), 39(2)(ιε) και (ιστ), 42(7), 55(2)(β), 80(α), 97 και 98

Ο Επίτροπος Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων, ασκώντας τις εξουσίες που του παρέχουν τα άρθρα 2(2)ζ, 18(3)(στ), 19(1), 20 (ιε), 20 (κε), 25, 28, 37(5), 39(2)(ιε) και (ιστ), 42(7), 55(2)(β), 80(α), 97 και 98 του περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμου του 2004, εκδίδει το ακόλουθο Διάταγμα:

N.112(I)/2004
N.84(I)/2005
N.149(I)/2005
N.67(I)/2006
N.113(I)/2007
N.134(I)/2007
N.46(I)/2008
N.103(I)/2009.

Συνοπτικός Τίτλος.

1. Το παρόν Διάταγμα θα αναφέρεται ως το Περί Ασφάλειας Δικτύων και Πληροφοριών Διάταγμα του 2011.

ΜΕΡΟΣ Ι
Εισαγωγικές Διατάξεις

Ερμηνεία .

2. (1) Στο παρόν Διάταγμα εκτός εάν από το κείμενο προκύπτει διαφορετική έννοια,

N.112(I)/2004
N.84(I)/2005
N.149(I)/2005
N.67(I)/2006
N.113(I)/2007
N.134(I)/2007
N.46(I)/2008
N.103(I)/2009.

«Νόμος» σημαίνει τον περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμο του 2004 και περιλαμβάνει κάθε Νόμο που τον τροποποιεί ή τον αντικαθιστά.

(2) Εκτός εάν από το κείμενο προκύπτει διαφορετική έννοια οι όροι που χρησιμοποιούνται στο παρόν Διάταγμα έχουν την έννοια που αποδίδει σ' αυτούς ο Νόμος.

(3) «Ακεραιότητα δικτύου» είναι η ικανότητα που παρέχεται σε ένα δίκτυο ηλεκτρονικών επικοινωνιών, στη βάση του σχεδιασμού του, να διατηρεί τη λειτουργικότητα για την οποία έχει σχεδιαστεί και να παρέχει και διατηρεί υψηλό επίπεδο υπηρεσίας κατόπιν βλαβών και αλλαγών στα κανονικά επίπεδα λειτουργίας.

(4) «Διασυνδεδεμένα δίκτυα» θεωρούνται τα δίκτυα τα οποία παρέχουν πρόσβαση το ένα στο άλλο για την ανταλλαγή κίνησης μέσω, ενδεικτικά, διασύνδεσης, μισθωμένων γραμμών, αδεσμοποίητης πρόσβασης στον τοπικό βρόχο, υπηρεσιών χονδρικής ευρυζωνικής πρόσβασης.

(5) «Υποδομές ζωτικής σημασίας» (κρίσιμες υποδομές – critical infrastructures) νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που βρίσκονται εντός της επικράτειας της Κυπριακής Δημοκρατίας και τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών.

Πεδίο Εφαρμογής.

3. Το παρόν Διάταγμα πραγματεύεται το καθορισμό των ελάχιστων υποχρεώσεων σχετικά με την ασφάλεια δικτύων και πληροφοριών τις οποίες πρέπει να τηρούν οι παροχείς οι οποίοι λειτουργούν δημόσια δίκτυα ηλεκτρονικών επικοινωνιών.

Σκοπός.

4. Σκοπός των ρυθμιστικών υποχρεώσεων που επιβάλλονται στους παροχείς που λειτουργούν δημόσια δίκτυα είναι η εξασφάλιση της ακεραιότητας και της επιχειρησιακής συνέχειας των δικτύων και των υπηρεσιών που παρέχονται προς τους καταναλωτές/συνδρομητές σε περίπτωση καταστροφικής βλάβης ή σε περίπτωση ανωτέρας βίας.

Περαιτέρω, μέγιστης σημασίας στην περίπτωση καταστροφικών συμβάντων είναι η εξασφάλιση της αδιάκοπης πρόσβασης σε υπηρεσίες έκτακτης ανάγκης, όπως ενδεικτικά κλήσεις στον αριθμό 112 ή σε αριθμούς της σειράς 116xx.

ΜΕΡΟΣ II

Γενικοί όροι και υποχρεώσεις παροχών δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών

Γενικός όρος.

5. Όλοι οι αδειοδοτημένοι παροχείς οφείλουν να λαμβάνουν τα απαραίτητα μέτρα έτσι ώστε να διασφαλίζεται η ορθή και αποτελεσματική λειτουργία του δικτύου τους σε περίπτωση βλαβών ή/και αλλαγών στα κανονικά επίπεδα λειτουργίας, από φυσικά αίτια ή κακόβουλες ενέργειες.

Υποχρεώσεις παροχών.

6. Κάθε αδειοδοτημένος παροχέας οφείλει να συμμορφώνεται με τις ακόλουθες υποχρεώσεις:

(1) Να προβαίνει σε ετήσια βάση σε αξιολόγηση επικινδυνότητας (risk assessment) των δικτύων του προκειμένου να εντοπίσει σημαντικές αδυναμίες και ευάλωτα σημεία στις δικτυακές του υποδομές. Ο παροχέας υποχρεούται να υποβάλλει στο ΓΕΡΗΕΤ την έκθεση αξιολόγησης επικινδυνότητας και το πλάνο διορθωτικών δράσεων στις οποίες έχει προβεί με στόχο την ενημέρωση του γραφείου για την κατάσταση του δικτύου του.

(2) Να προετοιμάζει σχέδια επιχειρησιακής συνέχειας (business continuity plans) τα οποία πρέπει να βασίζονται στα αποτελέσματα της αξιολόγησης επικινδυνότητας, την οποία έχει πραγματοποιήσει για το δίκτυο και τις υπηρεσίες του.

(3) Ειδικότερα, οφείλει όπως, για ενδεχόμενα εκτάκτων συνθηκών, καταστροφικής βλάβης και ανωτέρας βίας, καταρτίζει και κοινοποιεί στον Επίτροπο σχέδιο αντιμετώπισης εκτάκτων συνθηκών το οποίο να καταγράφει με λεπτομέρεια τη λήψη μέτρων αποκατάστασης.

(4) Να παρακολουθεί συνεχώς και σε πραγματικό χρόνο την κατάσταση των στοιχείων/εξοπλισμού των δικτύων του μέσω της λειτουργίας κατάλληλου Συστήματος Διαχείρισης Δικτύου (Network Management System) ως προς τη λειτουργική τους δυνατότητα και τις πιθανές βλάβες οι οποίες μπορούν να προκύψουν κατά τη λειτουργία του εξοπλισμού. Οι παροχείς οφείλουν επίσης να διατηρούν προσωπικό το οποίο να εργάζεται με ωράριο βάρδιας, ώστε να μπορεί να ανταποκριθεί άμεσα σε βλάβες που πιθανό να επηρεάσουν τις παρεχόμενες υπηρεσίες προς τους συνδρομητές.

(5) Να διασφαλίζει την επιχειρησιακή ακεραιότητα του δικτύου του, διασφαλίζοντας ότι ο εξοπλισμός είναι αξιόπιστος, ασφαλής έναντι εξωτερικών απειλών (π.χ. κακόβουλων επιθέσεων) και διαθέτει δυνατότητα υποβαθμισμένης λειτουργίας ακόμα και στην περίπτωση που υποστεί μερική βλάβη, υπό την επιφύλαξη ανωτέρας βίας. Κατά το σχεδιασμό και την επιλογή της αρχιτεκτονικής του δικτύου τους, οι παροχείς θα πρέπει να λαμβάνουν υπόψη θέματα εφεδρείας (redundancy) και φυσικής ασφάλειας (physical security) του εξοπλισμού τους.

(6) Οι παροχείς υποχρεούνται όπως διαθέτουν ή εξασφαλίζουν τη διαθεσιμότητα κατάλληλων και επαρκών αποθεμάτων (ανταλλακτικών) εξοπλισμού και διατηρούν κατάλληλα καταρτισμένο προσωπικό έτσι ώστε σε περιπτώσεις βλαβών που επηρεάζουν την λειτουργικότητα του δικτύου να μπορούν να αποκαταστήσουν τη λειτουργία του δικτύου και των παρεχόμενων υπηρεσιών καθ' όλη τη διάρκεια του εικοσιτετράωρου.

(7) Οι παροχείς καλούνται να συμμορφώνονται, με πρότυπα ή προδιαγραφές που θεσπίζονται σε κοινοτικό επίπεδο, χαρακτηρίζονται ως υποχρεωτικά και έχουν δημοσιευθεί σε κατάλογο προτύπων ή και προδιαγραφών στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, για την παροχή υπηρεσιών, τεχνικών διεπαφών ή και λειτουργιών δικτύων. Σε περίπτωση τεχνικών δυσκολιών συμμόρφωσης με την παραπάνω υποχρέωση, οι παροχείς, σε εύλογο χρόνο κατόπιν συμφωνίας με τον Επίτροπο, προβαίνουν στα αναγκαία μέτρα για τη συμμόρφωση με τις παραπάνω υποχρεώσεις τους..

Στην απουσία τέτοιων προτύπων ή και προδιαγραφών, οι παροχείς καλούνται να εφαρμόζουν τις τελευταίες εκδόσεις των διεθνών προτύπων ή συστάσεων που εγκρίνονται από τη Διεθνή Ένωση Τηλεπικοινωνιών (ITU), τον Διεθνή Οργανισμό Τυποποίησης (ISO) ή τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC).

ΜΕΡΟΣ III

Αξιολόγηση επικινδυνότητας

Άσκηση αξιολόγησης επικινδυνότητας .

7. (1) Οι παροχείς, στο πλαίσιο των λαμβανόμενων μέτρων για προστασία του δικτύου τους, υποχρεούνται να διενεργούν σε τακτά χρονικά διαστήματα άσκηση αξιολόγησης επικινδυνότητας με στόχο την εξακρίβωση των στοιχείων του δικτύου τα οποία δύνανται να επηρεάσουν την ακεραιότητα και τη διαθεσιμότητά του και να προκαλέσουν υποβάθμιση ή

απώλεια των παρεχομένων υπηρεσιών. Υποχρεούνται επίσης να συμμετέχουν σε εθνικές ή πανευρωπαϊκές ασκήσεις αξιολόγησης επικινδυνότητας.

(2) Το αποτέλεσμα της άσκησης επικινδυνότητας κοινοποιείται στον Επίτροπο, κατά τα διαλαμβανόμενα στο άρθρο 6 (1). Ως αποτέλεσμα της άσκησης επικινδυνότητας, ο Επίτροπος δύναται να επιβάλει, ή να συμφωνήσει με τους παροχείς, τηλήψη διορθωτικών μέτρων/δράσεων σύμφωνα με το πλαίσιο αξιολόγησης επικινδυνότητας, όπως αυτό περιγράφεται στο Παράρτημα 1.

Καταρτισμός Σχεδίου Επιχειρησιακής Συνέχειας.

8. Όλοι οι παροχείς δικτύων ηλεκτρονικών επικοινωνιών θα πρέπει να καταρτίζουν σχέδιο επιχειρησιακής συνέχειας, το οποίο αποσκοπεί στη διασφάλιση της αδιάλειπτης/απρόσκοπτης λειτουργίας των δικτύων και των παρεχομένων υπηρεσιών.

Το σχέδιο καταρτίζεται αφού προηγηθεί η άσκηση αξιολόγησης επικινδυνότητας και στη βάση των ευρημάτων/αποτελεσμάτων αυτής. Περιέχει περιγραφή των μέτρων που λαμβάνει ο παροχέας για την αποκατάσταση της λειτουργίας των στοιχείων του δικτύου του και την αποκατάσταση της πληροφωρίας η οποία έχει αλλοιωθεί ή χαθεί και η οποία απαιτείται για την παροχή υπηρεσίας. Το ελάχιστο περιεχόμενο του σχεδίου επιχειρησιακής συνέχειας περιγράφεται στο Παράρτημα 2.

Καταρτισμός Σχεδίου Εκτάκτων Συνθηκών.

9. Οι παροχείς υποχρεούνται να καταρτίζουν Σχέδιο Εκτάκτων Συνθηκών, στο πλαίσιο του οποίου καταγράφονται οι απαραίτητες δράσεις που αποσκοπούν στη διατήρηση της διαθεσιμότητας του δικτύου και των υπηρεσιών που παρέχονται στο κοινό και στη διατήρηση του υψηλότερου δυνατού επιπέδου υπηρεσιών για την ανταπόκριση στις απαιτήσεις οποιασδήποτε δημόσιας αρχής, σε περίπτωση καταστρεπτικής βλάβης ή ανωτέρας βίας.

Το Σχέδιο Εκτάκτων Συνθηκών θα πρέπει να αναθεωρείται στη βάση καθορισμένων διαδικασιών από προσωπικό του παροχέα το οποίο είναι υπεύθυνο για τον καταρτισμό και την αναγκαία αναθεώρηση του Σχεδίου.

Έλεγχοι.

10. Οι παροχείς οφείλουν να ελέγχουν την αποτελεσματικότητα του Σχεδίου Επιχειρησιακής Συνέχειας και του Σχεδίου Εκτάκτων Συνθηκών συστηματικά και τουλάχιστον σε ετήσια βάση. Οι παροχείς υποχρεούνται να διαθέτουν καταγεγραμμένες διαδικασίες βάσει των οποίων πραγματοποιούνται οι συγκεκριμένοι έλεγχοι. Η συχνότητα και το εύρος των ελέγχων καθορίζεται από τους κινδύνους που έχουν αναγνωρισθεί και τα εφαρμοζόμενα μέτρα ασφάλειας.

ΜΕΡΟΣ IV

Διατήρηση βασικών λειτουργιών δικτύου

Εφεδρεία.

11.(1) Οι παροχείς υποχρεούνται να εξασφαλίζουν την κατάλληλη εφεδρεία των κρίσιμων στοιχείων του δικτύου, έτσι ώστε πιθανή βλάβη να μην προκαλέσει σημαντική αλλοίωση της λειτουργίας του δικτύου και των παρεχομένων υπηρεσιών στους συνδρομητές τους.

(2) Οι παροχείς οφείλουν να σχεδιάζουν λύσεις εφεδρείας στα μέρη του δικτύου τους, με την εφεδρεία να αντανάκλα την κρίσιμότητα των μερών του δικτύου, στη βάση των αποτελεσμάτων της άσκησης αξιολόγησης επικινδυνότητας του δικτύου την οποία έχουν διενεργήσει προηγουμένως.

Ο σχεδιασμός του δικτύου θα πρέπει να προνοεί για την υλοποίηση λύσεων αυτόματης εφεδρείας που επιτρέπουν την αδιάλειπτη λειτουργία του δικτύου. Στις περιπτώσεις που δεν είναι τεχνικώς δυνατή η υλοποίηση σχεδιασμού αυτόματων λύσεων εφεδρείας – αυτόματη δρομολόγηση κίνησης μέσω εναλλακτικών διαδεύσεων –, τότε οι παροχείς οφείλουν να προβαίνουν στις απαραίτητες ενέργειες για την ταχεία επιδιόρθωση της βλάβης.

(3) Οι παροχείς οφείλουν να σχεδιάζουν τα δίκτυα τους ώστε η εφεδρεία των κρίσιμων στοιχείων των δικτύων να επιτυγχάνεται με τρόπο που να επιτρέπει την εγκατάσταση των κρίσιμων στοιχείων σε διαφορετικά υποστατικά του παροχέα, με τρόπο ώστε να εξασφαλίζεται η εφεδρεία μέσω της γεωγραφικής διασποράς. Οι παροχείς δύναται να αφίστανται της υποχρέωσης αυτής, όταν αντικειμενικοί λόγοι επιβάλουν διαφορετική σχεδίαση του δικτύου τους. Σε κάθε περίπτωση, οι παροχείς οφείλουν να ενημερώνουν τον Επίτροπο για τους λόγους της αδυναμίας αυτής, ώστε να αξιολογήσει τη βασιμότητά τους και να επιβάλει αναλογικές υποχρεώσεις.

Φυσική ασφάλεια.

12.(1) Οι παροχείς θα πρέπει να μεριμνούν για τη φυσική ασφάλεια των εγκαταστάσεων όπου βρίσκεται εγκατεστημένος ο εξοπλισμός των δικτύων τους, λαμβάνοντας μέτρα φυσικής ασφάλειας για κάθε υποστατικό ανάλογα με την κρίσιμότητα του εξοπλισμού που φιλοξενούν. Σε περίπτωση συνεγκατάστασης, η κατανομή της ευθύνης για τη φυσική ασφάλεια των εγκαταστάσεων καθώς και για τον έλεγχο της πρόσβασης γίνεται με τη σχετική συμφωνία πλαίσιο των μερών, σύμφωνα με το άρθρο 9(1)(δ) του Περὶ Παροχής Συνεγκατάστασης και

από Κοινού Χρήσης Διευκολύνσεων Διατάγματος του 2006 (Κ.Δ.Π.338/2006), όπως ισχύει.

Ενδεικτικά μέτρα φυσικής ασφάλειας περιλαμβάνουν τον έλεγχο πρόσβασης σε υποστατικά, προστασία από σεισμούς, πλημμύρες, υπερθέρμανση, φωτιά, κεραυνούς και άλλες φυσικές καταστροφές.

(2) Οι παροχείς οφείλουν να ακολουθούν σχεδιασμούς που εγγυώνται ότι τα στοιχεία του δικτύου τα οποία έχουν αξιολογηθεί ως ζωτικής σημασίας είναι εγκατεστημένα σε διαφορετικές εγκαταστάσεις ή σε χώρους φυσικά ανεξάρτητους. Στις περιπτώσεις όπου τα στοιχεία του δικτύου δεν μπορούν να εγκατασταθούν σε διαφορετικά υποστατικά θα πρέπει να λαμβάνεται πρόνοια ώστε ο εξοπλισμός να προστατεύεται από ανεξάρτητα μέσα φυσικής προστασίας.

(3) Σχετικά με τον έλεγχο πρόσβασης σε υποστατικά όπου βρίσκεται εγκατεστημένος εξοπλισμός του δικτύου, ο οποίος έχει προηγουμένως χαρακτηριστεί ως ζωτικής σημασίας, θα πρέπει να εγκαθίστανται ειδικά συστήματα τα οποία να αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση και να καθορίζονται διαδικασίες ασφάλειας μέσω των οποίων να ελέγχεται η πρόσβαση στους παραπάνω χώρους.

(4) Οι παροχείς οφείλουν να μεριμνούν για τη φυσική ακεραιότητα και την τακτική συντήρηση των υποστατικών/εγκαταστάσεων στα οποία είναι εγκατεστημένος ο εξοπλισμός του δικτύου τους, καθώς επίσης και για την εύρυθμη λειτουργία των μέτρων φυσικής ασφάλειας.

(5) Οι παροχείς οφείλουν να διαθέτουν μηχανισμούς και διαδικασίες για την άμεση πληροφόρηση τους ως προς γεγονότα που απειλούν την φυσική ασφάλεια των στοιχείων του δικτύου τους και των χώρων όπου αυτά είναι εγκατεστημένα.

(6) Οι παροχείς οφείλουν να συνεργάζονται με τους αρμόδιους φορείς και υπηρεσίες (κρατικές και ιδιωτικές) με στόχο την ελαχιστοποίηση της πιθανότητας ζημίας στα στοιχεία του δικτύου τους στις περιπτώσεις όπου διενεργούνται εργασίες που πιθανό να επηρεάζουν το δίκτυο τους.

Τροφοδοσία ισχύος.

13.(1) Οι παροχείς θα πρέπει να εξασφαλίζουν ότι η παροχή της κύριας τροφοδοσίας του εξοπλισμού γίνεται στη βάση των ενδεδειγμένων προδιαγραφών του.

(2) Σε περίπτωση διακοπής της κύριας τροφοδοσίας σε υποστατικό όπου στεγάζονται κρίσιμα σημεία του δικτύου λόγω βλάβης, θα πρέπει να εξασφαλίζουν την αδιάλειπτη παροχή τροφοδοσίας.

(3) Οι παροχείς οφείλουν να μεριμνούν ώστε η παροχή τροφοδοσίας στα κρίσιμα στοιχεία του δικτύου να μην διακόπτεται στην περίπτωση διακοπής της κύριας τροφοδοσίας.

(4) Κοινές πρακτικές που εφαρμόζονται σε περιπτώσεις απώλειας της κύριας πηγής τροφοδοσίας περιλαμβάνονται στο Παράρτημα 3 του παρόντος Διατάγματος.

Εξοπλισμός.

14. Οι παροχείς οφείλουν να λαμβάνουν όλα τα απαραίτητα μέτρα για την επαρκή προστασία του εξοπλισμού που χρησιμοποιείται στα δίκτυα τους.

Η προστασία του εξοπλισμού αφορά ιδίως την τήρηση μέτρων για τη φυσική προστασία του εξοπλισμού, την τήρηση των προδιαγραφών λειτουργίας του εξοπλισμού καθώς και την τήρηση των απαιτήσεων συντήρησής του.

Σε περίπτωση που διαπιστωθεί ότι εξοπλισμός ή στοιχείο δικτύου προκαλεί υποβάθμιση της λειτουργικής ικανότητας του δικτύου, οι παροχείς οφείλουν να λαμβάνουν αμέσως μέτρα αποκατάστασης της εύρυθμης λειτουργίας του δικτύου, αποκαθιστώντας το συντομότερο δυνατό την κανονική λειτουργία του εξοπλισμού ή αποσυνδέοντάς τον από το δίκτυο, ως τελευταίο μέτρο.

ΜΕΡΟΣ V

Ασφάλεια πληροφοριών

Ασφάλεια πληροφοριών
(Data Integrity – Packet losses).

15. Οι παροχείς οφείλουν να λαμβάνουν όλα τα απαραίτητα μέτρα για να διασφαλίσουν έναντι μη επιτρεπόμενης πρόσβασης την ακεραιότητα και τη διαθεσιμότητα της πληροφορίας στο δίκτυό τους, εξασφαλίζοντας ότι τα δεδομένα/πληροφορία (information data) τα οποία έχουν αποσταλεί, έχουν παραληφθεί ή έχουν αποθηκευθεί είναι πλήρη, ορθά και αμετάβλητα.

Οι παροχείς οφείλουν να μεριμνούν κατ'ελάχιστον για τα ακόλουθα:

(1) Τον προσδιορισμό της κρισιμότητας της πληροφορίας που σχετίζεται με την παροχή των υπηρεσιών.

(2) Την ύπαρξη καταγεγραμμένων διαδικασιών για την ασφαλή διαχείριση της πληροφορίας και μεθόδων αντιμετώπισης πιθανών κινδύνων και των επιπτώσεων τους, τόσο σε κανονικές όσο και σε έκτακτες συνθήκες.

(3) Την καταγραφή των μέτρων που λαμβάνει ο παροχέας για την αποφυγή πρόσβασης μη