ΕΦΗΜΕΡΙΔΑ
ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

5 Ιουλίου 2021 | ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ | Αρ. Φύλλου **2893**

ΑΠΟΦΑΣΕΙΣ

Αριθμ. απόφ. 190/2/16.06.2021

Υιοθέτηση των κατευθυντήριων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών (EBA/GL/2019/04) σχετικά με τη διαχείριση κινδύνων Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ) και Ασφάλειας.

Η ΕΚΤΕΛΕΣΤΙΚΗ ΕΠΙΤΡΟΠΗ
ΤΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ

Αφού έλαβε υπόψη:

α) Τα άρθρα 28 και 55Α του Καταστατικού της Τράπεζας της Ελλάδος (Α' 298),

β) τις διατάξεις του ν. 4261/2014 «Πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων (ενσωμάτωση της Οδηγίας 2013/36/ΕΕ), κατάργηση του ν. 3601/2007 και άλλες διατάξεις» (Α' 107), και ιδίως τα άρθρα 4 και 6, την παρ. 3 του άρθρου 66 και τα άρθρα 77, 102 και 153 αυτού,

γ) τις διατάξεις του ν. 4701/2020 «Πλαίσιο χορήγησης μικροχρηματοδοτήσεων, ρυθμίσεις χρηματοπιστωτικού τομέα και άλλες διατάξεις» (Α' 128), και ιδίως το άρθρο 4 αυτού,

δ) τις διατάξεις του ν. 4537/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2015/2366/ΕΕ για τις υπηρεσίες πληρωμών και άλλες διατάξεις» (Α' 84), και ιδίως τα άρθρα 5, 23, 94 και 95 αυτού,

ε) τις διατάξεις του ν. 4354/2015 «Διαχείριση των μη εξυπηρετούμενων δανείων, μισθολογικές ρυθμίσεις και άλλες επείγουσες διατάξεις εφαρμογής της συμφωνίας δημοσιονομικών στόχων και διαρθρωτικών μεταρρυθμίσεων» (Α' 176), και ιδίως το άρθρο 1 αυτού,

στ) τις διατάξεις του Κεφαλαίου Α' του Δεύτερου Μέρους του ν. 4021/2011 «Ενισχυμένα μέτρα εποπτείας και εξυγίανσης των πιστωτικών ιδρυμάτων - Ρύθμιση θεμάτων χρηματοπιστωτικού χαρακτήρα - Κύρωση της Σύμβασης - Πλαίσιο του Ευρωπαϊκού Ταμείου Χρηματοπιστωτικής Σταθερότητας και των τροποποιήσεών της και άλλες διατάξεις» (Α' 218), και ιδίως το άρθρο 12 και την παρ. 1 του άρθρου 13 αυτού,

ζ) τις διατάξεις του ν. 1905/1990 «Για τη σύμβαση πρακτορείας επιχειρηματικών απαιτήσεων και άλλες διατάξεις» (Α' 147), και ιδίως το άρθρο 5 αυτού,

η) τις διατάξεις του ν. 1665/1986 «Συμβάσεις χρηματοδοτικής μίσθωσης» (Α' 194), και ιδίως το άρθρο 2 αυτού,

θ) τις διατάξεις του ν. 5422/1932 «Περί αναστολής της υποχρεώσεως της Τραπέζης της Ελλάδος προς εξαργύρωσιν των γραμματίων αυτής και περί ρυθμίσεως της αγοράς και πωλήσεως συναλλάγματος» (Α' 133), όπως ισχύει μετά την προσθήκη των παρ. 3 έως 6 με το άρθρο 15 του ν. 2515/1997 «Άσκηση επαγγέλματος Λογιστή Φοροτεχνικού, λειτουργία Σώματος Ορκωτών Εκτιμητών (Σ.Ο.Ε.) και άλλες διατάξεις» (Α' 154), και ιδίως το άρθρο 2 αυτού,

ι) τον Κανονισμό (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 26ης Ιουνίου 2013 σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και επιχειρήσεις επενδύσεων και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176/27.6.2013),

ια) τον Κανονισμό (ΕΕ) αριθ. 1024/2013 του Συμβουλίου της 15ης Οκτωβρίου 2013 για την ανάθεση ειδικών καθηκόντων στην Ευρωπαϊκή Κεντρική Τράπεζα σχετικά με τις πολιτικές που αφορούν την προληπτική εποπτεία των πιστωτικών ιδρυμάτων (ΕΕ L 287/63/29.10.2013), και ιδίως τα άρθρα 4 και 6 αυτού και το στοιχείο 28 του Προοιμίου αυτού,

ιβ) τον Κανονισμό (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Νοεμβρίου 2010 σχετικά με τη σύσταση της Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Τραπεζών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/78/ΕΚ της Επιτροπής (ΕΕ L 331/15.12.2010), και ιδίως την παρ. 2 του άρθρου 4 και την παρ. 3 του άρθρου 16,

ιγ) την Πράξη Εκτελεστικής Επιτροπής της Τράπεζας της Ελλάδος (εφεξής «ΠΕΕ») 178/5/2.10.2020 «Πλαίσιο εξωτερικής ανάθεσης λειτουργιών» (Β' 4410),

ιδ) την ΠΕΕ 157/3/02.04.2019 «Υιοθέτηση των κατευθυντηρίων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών για την αναφορά μειζόνων συμβάντων δυνάμει της Οδηγίας 2015/2366/ΕΕ» (Β' 1646),

ιε) την ΠΕΕ 164/2/13.12.2019 «Όροι και προϋποθέσεις για: α) τη χορήγηση άδειας ίδρυσης και λειτουργίας των

ιδρυμάτων πληρωμών και των ιδρυμάτων ηλεκτρονικού χρήματος και την καταχώριση των παρόχων της υπηρεσίας πληροφοριών λογαριασμού στην Ελλάδα, β) την απόκτηση, την αύξηση ή τη διάθεση ειδικής συμμετοχής, γ) την ανάληψη θέσης μέλους Διοικητικού Συμβουλίου και άλλων, δ) τον καθορισμό ελάχιστου χρηματικού ποσού ασφάλισης επαγγελματικής ευθύνης ή άλλης συγκρίσιμης εγγύησης, ε) τους κανόνες εποπτείας, στ) την τήρηση μητρώου του άρθρου 14 του ν. 4537/2018» (Β’4522),

ιστ) την Πράξη Διοικητή της Τράπεζας Ελλάδος («ΠΔ/ΤΕ») 2577/2006 «Πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης της οργάνωσης και των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών και χρηματοδοτικών ιδρυμάτων και σχετικές αρμοδιότητες των διοικητικών τους οργάνων» (Α’ 59),

ιζ) τις κατευθυντήριες γραμμές της Ευρωπαϊκής Αρχής Τραπεζών σχετικά με την εσωτερική διακυβέρνηση (EBA/GL/2017/11),

ιη) τις κατευθυντήριες γραμμές της Ευρωπαϊκής Αρχής Τραπεζών σχετικά με τη διαχείριση κινδύνων Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ) και Ασφάλειας (EBA/GL/2019/04),

ιθ) ότι από τις διατάξεις της παρούσας Πράξης δεν προκύπτει δαπάνη σε βάρος του κρατικού προϋπολογισμού, αποφασίζει:

Να υιοθετήσει τις κατευθυντήριες γραμμές της Ευρωπαϊκής Αρχής Τραπεζών (EBA/GL/2019/04) σχετικά με τη διαχείριση κινδύνων Τεχνολογίας Πληροφορικής και Επικοινωνιών (εφεξής «ΤΠΕ») και Ασφάλειας, όπως αυτές προσδιορίζουν τα μέτρα διαχείρισης κινδύνου που πρέπει να λαμβάνονται, ως εξής:

ΚΕΦΑΛΑΙΟ Ι. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΚΑΙ ΟΡΙΣΜΟΙ

1. Οι διατάξεις της παρούσας εφαρμόζονται από τα ακόλουθα ιδρύματα (εφεξής «ιδρύματα»):

α. τα πιστωτικά ιδρύματα με έδρα στην Ελλάδα,

β. τα υποκαταστήματα των πιστωτικών ιδρυμάτων με έδρα σε χώρα εκτός του Ε.Ο.Χ. τα οποία λειτουργούν στην Ελλάδα,

γ. τους παρόχους υπηρεσιών πληρωμών του στοιχείου 11 του άρθρου 4 του ν. 4537/2018 (εφεξής «ΠΥΠ»), με έδρα στην Ελλάδα, σε σχέση με τις παρεχόμενες υπηρεσίες πληρωμών, του στοιχείου 3 του άρθρου 4 του ν. 4537/2018, καθώς και σε σχέση με την δραστηριότητα της έκδοσης, εξαργύρωσης και διανομής ηλεκτρονικού χρήματος (για τους σκοπούς της παρούσας, ως υπηρεσίες πληρωμών νοούνται οι δραστηριότητες του στοιχείου 3 του άρθρου 4 του ν. 4537/2018, καθώς και η δραστηριότητα της έκδοσης, εξαργύρωσης και διανομής ηλεκτρονικού χρήματος),

δ. τις εταιρείες χρηματοδοτικής μίσθωσης με έδρα στην Ελλάδα,

ε. τις εταιρείες πρακτορείας επιχειρηματικών απαιτήσεων με έδρα στην Ελλάδα,

στ. τις εταιρείες παροχής πιστώσεων με έδρα στην Ελλάδα,

ζ. τις εταιρείες διαχείρισης απαιτήσεων από δάνεια και πιστώσεις με έδρα στην Ελλάδα οι οποίες προβαίνουν σε αναχρηματοδότηση απαιτήσεων, σύμφωνα με την παρ. 20 του άρθρου 1 του ν. 4354/2015,

η. τα ιδρύματα μικροχρηματοδοτήσεων,

θ. τα ανταλλακτήρια συναλλάγματος με έδρα στην Ελλάδα.

2. Οι διατάξεις της παρούσας εφαρμόζονται από τα πιστωτικά ιδρύματα της περ. α) της παρ. 1 σε ατομική βάση, σε υποενοποιημένη και ενοποιημένη βάση σύμφωνα με το άρθρο 102 του ν. 4261/2014. Τα υπόλοιπα υπόχρεα πρόσωπα της παρ. 1 εφαρμόζουν τις διατάξεις της παρούσας σε ατομική βάση.

3. Η παρούσα Πράξη περιλαμβάνει απαιτήσεις ασφάλειας πληροφοριών, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο, στον βαθμό που οι πληροφορίες φυλάσσονται σε συστήματα ΤΠΕ.

4. Εκτός εάν προβλέπεται διαφορετικά, οι όροι που χρησιμοποιούνται και ορίζονται στον ν. 4261/2014, στον κανονισμό (ΕΕ) αριθ. 575/2013 και στον ν. 4537/2018 έχουν την ίδια έννοια και στην παρούσα Πράξη. Επιπλέον, για τους σκοπούς της παρούσας ισχύουν οι ακόλουθοι ορισμοί:

Κίνδυνος Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ) και Ασφάλειας	Κίνδυνος ζημίας λόγω παραβίασης της εμπιστευτικότητας, αστοχίας της ακεραιότητας συστημάτων και δεδομένων, ακαταλληλότητας ή μη διαθεσιμότητας συστημάτων και δεδομένων, ή αδυναμίας αλλαγής τεχνολογίας πληροφορικής (ΤΠ) εντός εύλογου χρονικού διαστήματος και με εύλογο κόστος όταν οι απαιτήσεις του περιβάλλοντος ή των επιχειρηματικών δραστηριοτήτων μεταβάλλονται (δηλ. ευελιξία). Στο πλαίσιο αυτό περιλαμβάνονται κίνδυνοι ασφάλειας που προκύπτουν λόγω ανεπάρκειας ή αστοχίας εσωτερικών διεργασιών ή εξωτερικών συμβάντων, μεταξύ των οποίων περιλαμβάνονται και οι επιθέσεις στον κυβερνοχώρο ή η ανεπαρκής φυσική ασφάλεια.
Περιστατικό λειτουργικού κινδύνου ή περιστατικό ασφάλειας	Μεμονωμένο συμβάν ή σειρά συνδεόμενων συμβάντων μη προγραμματισμένων από το ίδρυμα, τα οποία έχουν ή ενδέχεται να έχουν δυσμενείς επιπτώσεις στην ακεραιότητα, τη διαθεσιμότητα, την εμπιστευτικότητα και/ή την αυθεντικότητα των υπηρεσιών.
Λειτουργίες εσωτερικού ελέγχου	Οι λειτουργίες του ιδρύματος οι οποίες είναι ανεξάρτητες από τις επιχειρηματικές και τις εταιρικές λειτουργίες των οποίων τις δραστηριότητες και τους κινδύνους ελέγχουν και παρακολουθούν. Οι ανεξάρτητες λειτουργίες εσωτερικού ελέγχου κατά κανόνα περιλαμβάνουν τις λειτουργίες διαχείρισης κινδύνων, κανονιστικής συμμόρφωσης και εσωτερικής επιθεώρησης.

Διάθεση ανάληψης κινδύνου	Το συγκεντρωτικό επίπεδο και τα είδη των κινδύνων που είναι πρόθυμα να αναλάβουν τα ιδρύματα στο πλαίσιο της ικανότητάς τους για ανάληψη κινδύνων, και σύμφωνα με το επιχειρηματικό τους μοντέλο, προκειμένου να επιτύχουν τους στρατηγικούς στόχους τους.
Έργα ΤΠΕ	Κάθε έργο, ή μέρος έργου, στο πλαίσιο του οποίου αλλάζουν, αντικαθίστανται, καταργούνται ή υλοποιούνται συστήματα ΤΠΕ. Τα έργα ΤΠΕ μπορούν να αποτελούν μέρος ευρύτερων ΤΠΕ ή επιχειρηματικών προγραμμάτων μετασχηματισμού.
Τρίτο Μέρος ή Τρίτος	Οργανισμός ο οποίος έχει συνάψει επιχειρηματικές σχέσεις ή συμβάσεις με οντότητα για την παροχή προϊόντος ή υπηρεσίας.
Πληροφοριακός πόρος	Συλλογή πληροφοριών, είτε υλικών είτε άυλων, που αξίζει να προστατεύονται.
Πόρος ΤΠΕ	Πόρος είτε λογισμικού είτε υλισμικού που απαντάται στο επιχειρηματικό περιβάλλον.
Συστήματα ΤΠΕ	Εγκατάσταση ΤΠΕ ως μέρος ενός μηχανισμού ή ενός δικτύου διασύνδεσης το οποίο υποστηρίζει τις λειτουργίες ενός ιδρύματος.
Υπηρεσίες ΤΠΕ	Υπηρεσίες παρεχόμενες από συστήματα ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες. Περιλαμβάνονται, παραδείγματος χάριν, υπηρεσίες εισαγωγής δεδομένων, αποθήκευσης δεδομένων, επεξεργασίας δεδομένων και υποβολής αναφορών, αλλά και υπηρεσίες παρακολούθησης, υποστήριξης επιχειρηματικών δραστηριοτήτων και υποστήριξης λήψης αποφάσεων.

ΚΕΦΑΛΑΙΟ ΙΙ. ΑΝΑΛΟΓΙΚΟΤΗΤΑ - ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΑΙ ΣΤΡΑΤΗΓΙΚΗ

1. Αναλογικότητα

5. Όλα τα ιδρύματα συμμορφώνονται με τις διατάξεις της παρούσας Πράξης με τρόπο αναλογικό και λαμβάνοντας υπόψη το μέγεθός τους, την εσωτερική τους οργάνωση, καθώς και τη φύση, την κλίμακα, την πολυπλοκότητα και τον βαθμό επικινδυνότητας των υπηρεσιών και των προϊόντων που παρέχουν ή προτίθενται να παρέχουν.

2. Διακυβέρνηση και στρατηγική

2.1 Διακυβέρνηση

6. Το Διοικητικό Συμβούλιο διασφαλίζει ότι τα ιδρύματα διαθέτουν επαρκές πλαίσιο εσωτερικής διακυβέρνησης και εσωτερικού ελέγχου για τους οικείους κινδύνους ΤΠΕ και ασφάλειας. Το Διοικητικό Συμβούλιο καθορίζει σαφείς ρόλους και αρμοδιότητες για τη λειτουργία ΤΠΕ, τη διαχείριση κινδύνων ασφάλειας πληροφοριών, καθώς και για την επιχειρησιακή συνέχεια, συμπεριλαμβανομένων και αυτών που αφορούν το ίδιο το Διοικητικό Συμβούλιο και τις επιτροπές του.

7. Το Διοικητικό Συμβούλιο μεριμνά ώστε ο αριθμός και οι δεξιότητες των μελών του προσωπικού των ιδρυμάτων να επαρκούν για την υποστήριξη σε διαρκή βάση των λειτουργικών τους αναγκών στον τομέα των ΤΠΕ και των διεργασιών τους όσον αφορά τη διαχείριση των κινδύνων ΤΠΕ και ασφάλειας, καθώς και για τη διασφάλιση της εφαρμογής της οικείας στρατηγικής ΤΠΕ. Το Διοικητικό Συμβούλιο διασφαλίζει ότι ο διαθέσιμος προϋπολογισμός είναι κατάλληλος για την εκπλήρωση των προαναφερόμενων υποχρεώσεων. Επιπλέον, τα ιδρύματα μεριμνούν ώστε όλα τα μέλη του προσωπικού, συμπεριλαμβανομένων των προσώπων που κατέχουν καίριες θέσεις, να λαμβάνουν κατάλληλη εκπαίδευση σχετικά με τους κινδύνους ΤΠΕ και ασφάλειας, μεταξύ άλλων και όσον αφορά την ασφάλεια πληροφοριών, σε ετήσια βάση ή συχνότερα, εάν απαιτείται.

8. Το Διοικητικό Συμβούλιο υπέχει συνολική υποχρέωση λογοδοσίας για τον καθορισμό, την έγκριση και την επίβλεψη της εφαρμογής της στρατηγικής ΤΠΕ των ιδρυμάτων στο πλαίσιο της συνολικής τους επιχειρηματικής στρατηγικής, καθώς και για τη δημιουργία αποτελεσματικού πλαισίου διαχείρισης κινδύνων ΤΠΕ και ασφάλειας.

2.2 Στρατηγική

9. Η στρατηγική ΤΠΕ εναρμονίζεται με τη συνολική επιχειρηματική στρατηγική των ιδρυμάτων και ορίζει τα εξής:

α) τον τρόπο με τον οποίο εξελίσσεται η ΤΠΕ των ιδρυμάτων ώστε να υποστηρίζει αποτελεσματικά την επιχειρηματική τους στρατηγική και να συμμετέχει σε αυτή, συμπεριλαμβανομένης της εξέλιξης της οργανωτικής δομής, των αλλαγών των συστημάτων ΤΠΕ και των κύριων αλληλεξαρτήσεων με τρίτους,

β) την προγραμματισμένη στρατηγική και εξέλιξη της αρχιτεκτονικής της ΤΠΕ, συμπεριλαμβανομένων των αλληλεξαρτήσεων με τρίτους,

γ) σαφείς στόχους ασφάλειας πληροφοριών, με ιδιαίτερη έμφαση στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ, στο προσωπικό και στις διεργασίες ΤΠΕ.

10. Τα ιδρύματα καταρτίζουν σχέδια δράσης τα οποία περιέχουν τα μέτρα που λαμβάνονται για την επίτευξη του στόχου της στρατηγικής ΤΠΕ. Τα εν λόγω σχέδια δράσης διαβιβάζονται σε όλα τα μέλη του αρμόδιου προσωπικού (συμπεριλαμβανομένων των αναδόχων έργων και των τρίτων παρόχων, κατά περίπτωση και όπου κρίνεται σκόπιμο). Τα σχέδια δράσης επανεξετάζονται σε περιοδική βάση ώστε να διασφαλίζεται η συνάφεια και η καταλληλότητά τους. Τα ιδρύματα δημιουργούν επίσης διαδικασίες για την παρακολούθηση και τη μέτρηση της αποτελεσματικότητας της εφαρμογής της οικείας στρατηγικής ΤΠΕ.

2.3 Χρήση τρίτων παρόχων

11. Με την επιφύλαξη της ΠΕΕ 178/5/2.10.2020 «Πλαίσιο εξωτερικής ανάθεσης λειτουργιών», τα ιδρύματα διασφαλίζουν την αποτελεσματικότητα των μέτρων

μείωσης των κινδύνων, όπως ορίζονται από το οικείο πλαίσιο διαχείρισης κινδύνων, συμπεριλαμβανομένων των μέτρων που προβλέπονται στην παρούσα Πράξη, σε περιπτώσεις εξωτερικής ανάθεσης λειτουργιών των υπηρεσιών πληρωμών και/ή των υπηρεσιών ΤΠΕ και των συστημάτων ΤΠΕ οποιασδήποτε δραστηριότητας, μεταξύ άλλων και σε οντότητες του ομίλου, ή σε περιπτώσεις χρήσης τρίτων.

12. Προκειμένου να διασφαλίζεται η συνέχεια των υπηρεσιών ΤΠΕ και των συστημάτων ΤΠΕ, τα ιδρύματα μεριμνούν ώστε οι συμβάσεις και τα συμβόλαια διασφάλισης επιπέδου ποιότητας (τόσο υπό κανονικές συνθήκες όσο και σε περίπτωση διαταραχής των υπηρεσιών) που συνάπτονται με παρόχους (οντότητες ομίλου ή τρίτους παρόχους) να περιλαμβάνουν τα εξής:

α) κατάλληλους και αναλογικούς στόχους και μέτρα που αφορούν την ασφάλεια πληροφοριών και περιλαμβάνουν απαιτήσεις, όπως ελάχιστες απαιτήσεις ασφάλειας στον κυβερνοχώρο, προδιαγραφές του κύκλου ζωής των δεδομένων του ιδρύματος, τυχόν απαιτήσεις σχετικά με την κρυπτογράφηση δεδομένων, διεργασίες ασφάλειας δικτύου και παρακολούθησης της ασφάλειας, καθώς και την τοποθεσία των μηχανογραφικών κέντρων,

β) διαδικασίες χειρισμού περιστατικών λειτουργικού κινδύνου και περιστατικών ασφάλειας, συμπεριλαμβανομένης της υποβολής αναφορών και της παραπομπής σε ανώτερη βαθμίδα της ιεραρχικής κλίμακας.

13. Τα ιδρύματα παρακολουθούν και ζητούν διαβεβαίωση σχετικά με το επίπεδο συμμόρφωσης των εν λόγω παρόχων με τους αντικειμενικούς σκοπούς, τα μέτρα και τους στόχους επιδόσεων του ιδρύματος όσον αφορά την ασφάλεια.

ΚΕΦΑΛΑΙΟ ΙΙΙ. ΠΛΑΙΣΙΟ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΤΠΕ ΚΑΙ ΑΣΦΑΛΕΙΑΣ

3.1 Οργάνωση και στόχοι

14. Τα ιδρύματα προσδιορίζουν και διαχειρίζονται τους οικείους κινδύνους ΤΠΕ και ασφάλειας. Η υπηρεσιακή/ές μονάδα/ες ΤΠΕ που είναι αρμόδια/ες για τα συστήματα ΤΠΕ, τις διεργασίες και τις λειτουργίες ασφάλειας διαθέτει/ουν κατάλληλες διαδικασίες και δικλείδες ασφάλειας, ώστε να διασφαλίζεται τόσο ο προσδιορισμός, η ανάλυση, η μέτρηση, η παρακολούθηση, η διαχείριση, η αναφορά και η διατήρηση όλων των κινδύνων εντός των ορίων της διάθεσης ανάληψης κινδύνου του ιδρύματος όσο και η συμμόρφωση των έργων και των συστημάτων που παραδίδουν, καθώς και των δραστηριοτήτων που ασκούν με τις εξωτερικές και εσωτερικές απαιτήσεις.

15. Τα ιδρύματα αναθέτουν την ευθύνη για τη διαχείριση και την επίβλεψη των κινδύνων ΤΠΕ και ασφάλειας σε μία λειτουργία εσωτερικού ελέγχου, τηρώντας τις απαιτήσεις της ΠΔ/ΤΕ 2577/2006. Τα ιδρύματα διασφαλίζουν την ανεξαρτησία και την αντικειμενικότητα της εν λόγω λειτουργίας εσωτερικού ελέγχου, διαχωρίζοντάς την δεόντως από τις διεργασίες των λειτουργιών ΤΠΕ. Η εν λόγω λειτουργία εσωτερικού ελέγχου λογοδοτεί απευθείας στο Διοικητικό Συμβούλιο και είναι υπεύθυνη για την παρακολούθηση και τον έλεγχο της τήρησης του πλαισίου διαχείρισης κινδύνων ΤΠΕ και ασφάλειας. Διασφαλίζει τον προσδιορισμό, τη μέτρηση, την αξιολόγηση, τη διαχείριση, την παρακολούθηση και την αναφορά των κινδύνων ΤΠΕ και ασφάλειας. Τα ιδρύματα μεριμνούν ώστε η συγκεκριμένη λειτουργία εσωτερικού ελέγχου να μην είναι υπεύθυνη για τη διενέργεια οποιασδήποτε εσωτερικής επιθεώρησης.

Η λειτουργία εσωτερικής επιθεώρησης, εφαρμόζοντας μια προσέγγιση βάσει κινδύνου, προβαίνει σε ανεξάρτητη αξιολόγηση και παρέχει αντικειμενική διαβεβαίωση αναφορικά με τη συμμόρφωση όλων των δραστηριοτήτων και των μονάδων του ιδρύματος που αφορούν την ΤΠΕ και την ασφάλεια με τις πολιτικές και τις διαδικασίες του ιδρύματος, καθώς και με τις κανονιστικές απαιτήσεις.

16. Τα ιδρύματα ορίζουν και αναθέτουν τους κύριους ρόλους και αρμοδιότητες, μεταξύ των οποίων και του υπεύθυνου ασφάλειας πληροφοριών, καθώς και τις σχετικές γραμμές αναφοράς που απαιτούνται για να είναι αποτελεσματικό το πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας. Το πλαίσιο αυτό εντάσσεται πλήρως στις συνολικές διαδικασίες διαχείρισης κινδύνων των ιδρυμάτων και εναρμονίζεται απόλυτα με αυτές.

17. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας περιλαμβάνει την εφαρμογή διαδικασιών με στόχο:

α) τον καθορισμό της διάθεσης ανάληψης κινδύνου όσον αφορά τους κινδύνους ΤΠΕ και ασφάλειας σύμφωνα με τη διάθεση ανάληψης κινδύνου του ιδρύματος,

β) τον προσδιορισμό και την αξιολόγηση των κινδύνων ΤΠΕ και ασφάλειας στους οποίους εκτίθεται το ίδρυμα,

γ) τον καθορισμό μέτρων μείωσης των κινδύνων, συμπεριλαμβανομένης της εφαρμογής δικλείδων ασφαλείας για τη μείωση των κινδύνων ΤΠΕ και ασφάλειας,

δ) την παρακολούθηση της αποτελεσματικότητας των εν λόγω μέτρων, καθώς και του αριθμού των αναφερθέντων περιστατικών, συμπεριλαμβανομένων — όσον αφορά τους ΠΥΠ — των περιστατικών που αναφέρονται σύμφωνα με το άρθρο 95 του ν. 4537/2018 και επηρεάζουν τις σχετικές με την ΤΠΕ δραστηριότητες, και την ανάληψη δράσης για τη διόρθωση των μέτρων όπου κρίνεται αναγκαίο,

ε) την υποβολή αναφορών στο Διοικητικό Συμβούλιο όσον αφορά τους κινδύνους ΤΠΕ και ασφάλειας και τις αντίστοιχες δικλείδες ασφαλείας,

στ) τον προσδιορισμό και τη διερεύνηση της παρουσίας τυχόν κινδύνων ΤΠΕ και ασφάλειας που προκύπτουν από οποιαδήποτε μείζονα αλλαγή στο σύστημα ΤΠΕ ή στις υπηρεσίες ΤΠΕ, τις διεργασίες ή τις διαδικασίες ΤΠΕ και/ή έπειτα από κάθε σημαντικό περιστατικό λειτουργικού κινδύνου ή περιστατικό ασφάλειας,

18. Τα ιδρύματα μεριμνούν ώστε το πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας να τεκμηριώνεται και να βελτιώνεται διαρκώς, με βάση τα διδάγματα που αντλούνται κατά την εφαρμογή και την παρακολούθησή του. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας εγκρίνεται και επανεξετάζεται, τουλάχιστον μία φορά ετησίως, από το Διοικητικό Συμβούλιο.

3.2 Προσδιορισμός λειτουργιών, διεργασιών και πόρων

19. Τα ιδρύματα προσδιορίζουν, καταρτίζουν και επικαιροποιούν τη χαρτογράφηση των επιχειρηματικών

τους λειτουργιών, ρόλων και υποστηρικτικών διεργασιών ώστε να προσδιορίζεται η σημασία κάθε επιμέρους επιχειρηματικής λειτουργίας, ρόλου και υποστηρικτικής διεργασίας, καθώς και των αλληλεξαρτήσεών τους, σε σχέση με τους κινδύνους ΤΠΕ και ασφάλειας.

20. Επιπλέον, τα ιδρύματα προσδιορίζουν, καταρτίζουν και επικαιροποιούν τη χαρτογράφηση των πληροφοριακών πόρων που υποστηρίζουν τις επιχειρηματικές τους λειτουργίες και υποστηρικτικές διεργασίες, όπως, για παράδειγμα, των συστημάτων ΤΠΕ, του προσωπικού, των αναδόχων έργων, τρίτων μερών, καθώς και των διασυνδέσεων με άλλα εσωτερικά και εξωτερικά συστήματα και διεργασίες, προκειμένου να είναι σε θέση, κατ’ ελάχιστον, να διαχειρίζονται τους πληροφοριακούς πόρους που υποστηρίζουν τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες τους.

3.3 Κατηγοριοποίηση και αξιολόγηση κινδύνων

21. Τα ιδρύματα κατηγοριοποιούν τις ως άνω επιχειρηματικές λειτουργίες, υποστηρικτικές διεργασίες και τους πληροφοριακούς πόρους που αναφέρονται στις παραγράφους 19 και 20 βάσει της κρισιμότητάς τους.

22. Για τον καθορισμό της κρισιμότητας των εν λόγω προσδιοριζόμενων επιχειρηματικών λειτουργιών, υποστηρικτικών διεργασιών και πληροφοριακών πόρων, τα ιδρύματα λαμβάνουν υπόψη, κατ’ ελάχιστον, τις απαιτήσεις εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Επιπλέον, ανατίθενται με σαφήνεια καθήκοντα λογοδοσίας και ευθύνης για τους πληροφοριακούς πόρους.

23. Τα ιδρύματα επανεξετάζουν την επάρκεια της κατηγοριοποίησης των πληροφοριακών πόρων και της σχετικής τεκμηρίωσης κατά τη διενέργεια της αξιολόγησης κινδύνων.

24. Τα ιδρύματα προσδιορίζουν τους κινδύνους ΤΠΕ και ασφάλειας που έχουν αντίκτυπο στις επιχειρηματικές λειτουργίες, στις υποστηρικτικές διεργασίες και στους πληροφοριακούς πόρους, βάσει της κρισιμότητάς τους. Η αξιολόγηση κινδύνων διενεργείται και τεκμηριώνεται σε ετήσια βάση ή σε βραχύτερα διαστήματα, εάν απαιτείται. Οι εν λόγω αξιολογήσεις κινδύνων διενεργούνται επίσης σε περίπτωση τυχόν μείζονος αλλαγής στην υποδομή, τις διεργασίες ή τις διαδικασίες που επηρεάζουν τις επιχειρηματικές λειτουργίες, τις υποστηρικτικές διεργασίες ή τους πληροφοριακούς πόρους και κατ’ αποτέλεσμα επικαιροποιείται η τρέχουσα αξιολόγηση κινδύνων των ιδρυμάτων.

25. Τα ιδρύματα διασφαλίζουν τη συνεχή παρακολούθηση των απειλών και ευπαθειών που αφορούν τις επιχειρηματικές λειτουργίες, τις υποστηρικτικές διεργασίες και τους πληροφοριακούς πόρους τους, ενώ επίσης επανεξετάζουν τακτικά τα σενάρια κινδύνων που τα επηρεάζουν.

3.4 Μείωση των κινδύνων

26. Βάσει των αξιολογήσεων κινδύνων, τα ιδρύματα καθορίζουν τα μέτρα που απαιτούνται για τη μείωση των προσδιορισθέντων κινδύνων ΤΠΕ και ασφάλειας σε αποδεκτά επίπεδα, ενώ επίσης προσδιορίζουν κατά πόσον απαιτούνται αλλαγές στις υφιστάμενες επιχειρηματικές διεργασίες, στα μέτρα ελέγχου, στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ. Τα ιδρύματα λαμβάνουν υπόψη τον χρόνο που απαιτείται για την εφαρμογή των εν λόγω αλλαγών και τον χρόνο λήψης κατάλληλων προσωρινών μέτρων για να ελαχιστοποιήσουν τους κινδύνους ΤΠΕ και ασφάλειας, ώστε να παραμείνουν εντός των ορίων της διάθεσης ανάληψης κινδύνων ΤΠΕ και ασφάλειας του εκάστοτε ιδρύματος.

27. Τα ιδρύματα καθορίζουν και εφαρμόζουν μέτρα για τη μείωση των προσδιοριζόμενων κινδύνων ΤΠΕ και ασφάλειας και για την προστασία των πληροφοριακών πόρων βάσει της κατηγοριοποίησής τους.

3.5 Υποβολή αναφορών

28. Τα ιδρύματα υποβάλλουν εγκαίρως στο Διοικητικό Συμβούλιο σαφείς αναφορές σχετικά με τα αποτελέσματα της αξιολόγησης κινδύνων. Οι εν λόγω αναφορές υποβάλλονται με την επιφύλαξη της υποχρέωσης των ΠΥΠ να παρέχουν στις αρμόδιες αρχές επικαιροποιημένη και ολοκληρωμένη αξιολόγηση κινδύνων, όπως προβλέπεται στην παρ. 2 του άρθρου 94 του ν. 4537/2018.

3.6 Εσωτερική επιθεώρηση

29. Η διακυβέρνηση, τα συστήματα και οι διεργασίες ενός ιδρύματος ως προς τους οικείους κινδύνους ΤΠΕ και ασφάλειας υπόκεινται σε διαδικασία εσωτερικού ελέγχου σε περιοδική βάση από ελεγκτές με επαρκείς γνώσεις, δεξιότητες και εξειδίκευση σε θέματα κινδύνων ΤΠΕ και ασφάλειας, καθώς και σε θέματα πληρωμών (για τους ΠΥΠ), ώστε να παρέχεται στο Διοικητικό Συμβούλιο ανεξάρτητη διαβεβαίωση όσον αφορά την αποτελεσματικότητά τους. Οι ελεγκτές του ιδρύματος, είτε εσωτερικοί είτε εξωτερικοί, απολαμβάνουν ανεξαρτησίας. Η συχνότητα και το σημείο εστίασης των εν λόγω ελέγχων είναι ανάλογα προς τους αντίστοιχους κινδύνους ΤΠΕ και ασφάλειας.

30. Το Διοικητικό Συμβούλιο του ιδρύματος εγκρίνει το πρόγραμμα ελέγχων, συμπεριλαμβανομένων τυχόν ελέγχων ΤΠΕ και κάθε πιθανής σημαντικής τροποποίησής του. Το πρόγραμμα ελέγχων και η εκτέλεσή του, συμπεριλαμβανομένης της συχνότητας των ελέγχων, αντικατοπτρίζει και είναι ανάλογο προς τους εγγενείς κινδύνους ΤΠΕ και ασφάλειας του ιδρύματος και επικαιροποιείται ανά τακτά χρονικά διαστήματα.

31. Στο ίδρυμα θεσπίζεται επίσημη διαδικασία παρακολούθησης, η οποία περιλαμβάνει διατάξεις για την έγκαιρη επαλήθευση των ενεργειών αποκατάστασης των κρίσιμων ευρημάτων ελέγχου ΤΠΕ βάσει του συμφωνηθέντος χρονοδιαγράμματος.

ΚΕΦΑΛΑΙΟ IV. ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

4.1 Πολιτική ασφάλειας πληροφοριών

3.2 Τα ιδρύματα αναπτύσσουν και τεκμηριώνουν πολιτική ασφάλειας πληροφοριών στην οποία καθορίζονται γενικές αρχές και κανόνες για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των πληροφοριών των ιδρυμάτων και των πελατών τους. Όσον αφορά τους ΠΥΠ, η πολιτική αυτή προσδιορίζεται στο έγγραφο που περιγράφει την πολιτική ασφάλειας, το οποίο εγκρίνεται σύμφωνα με το στοιχείο (ι) της παρ. 1 του άρθρου 5 του ν. 4537/2018. Η πολιτική ασφάλειας πληροφοριών συνάδει με τους στόχους της ασφάλειας πληροφοριών του ιδρύματος

και βασίζεται στα σχετικά αποτελέσματα της διαδικασίας αξιολόγησης κινδύνων. Η πολιτική εγκρίνεται από το Διοικητικό Συμβούλιο.

3.3 Η πολιτική περιλαμβάνει περιγραφή των κύριων ρόλων και αρμοδιοτήτων της διαχείρισης ασφάλειας πληροφοριών και καθορίζει τις απαιτήσεις για το προσωπικό και τους αναδόχους έργων, τις διεργασίες και την τεχνολογία σε σχέση με την ασφάλεια πληροφοριών, αναγνωρίζοντας ότι το προσωπικό και οι ανάδοχοι έργων σε όλα τα επίπεδα έχουν ευθύνες όσον αφορά τη διασφάλιση της ασφάλειας πληροφοριών των ιδρυμάτων. Η πολιτική διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα, κατ’ ελάχιστον, των κρίσιμων λογικών και υλικών περιουσιακών στοιχείων, των πόρων, καθώς και των ευαίσθητων δεδομένων των ιδρυμάτων είτε όταν τα στοιχεία αυτά αποθηκεύονται, είτε όταν διαβιβάζονται ή χρησιμοποιούνται. Η πολιτική ασφάλειας πληροφοριών κοινοποιείται στο σύνολο των μελών του προσωπικού και των αναδόχων έργων του ιδρύματος.

34. Βάσει της πολιτικής ασφάλειας πληροφοριών, τα ιδρύματα θεσπίζουν και εφαρμόζουν μέτρα ασφάλειας για τη μείωση των κινδύνων ΤΠΕ και ασφάλειας στους οποίους εκτίθενται. Τα μέτρα αυτά περιλαμβάνουν κατ’ ελάχιστον:

α) την οργάνωση και τη διακυβέρνηση σύμφωνα με τις παραγράφους 14 και 15,

β) τη λογική ασφάλεια (Ενότητα 4.2), γ) τη φυσική ασφάλεια (Ενότητα 4.3),

δ) την ασφάλεια των λειτουργιών ΤΠΕ (Ενότητα 4.4),

ε) την παρακολούθηση της ασφάλειας (Ενότητα 4.5),

στ) επανεξετάσεις, αξιολογήσεις και δοκιμές της ασφάλειας πληροφοριών (Ενότητα 4.6),

ζ) κατάρτιση και ευαισθητοποίηση σε θέματα ασφάλειας πληροφοριών (Ενότητα 4.7).

4.2 Λογική ασφάλεια

35. Τα ιδρύματα καθορίζουν, τεκμηριώνουν και εφαρμόζουν διαδικασίες για τον έλεγχο της λογικής πρόσβασης (διαχείριση στοιχείων ταυτότητας και πρόσβασης). Οι διαδικασίες αυτές εφαρμόζονται, επιβάλλονται, παρακολουθούνται και επανεξετάζονται σε περιοδική βάση. Οι διαδικασίες περιλαμβάνουν επίσης ελέγχους για την παρακολούθηση ασυνήθιστων ενεργειών. Στο πλαίσιο των εν λόγω διαδικασιών πρέπει κατ’ ελάχιστον να εφαρμόζονται τα ακόλουθα στοιχεία, έχοντας υπόψη ότι ο όρος «χρήστης» περιλαμβάνει και τους τεχνικούς χρήστες:

α) Ελάχιστη απαιτούμενη πληροφόρηση, ελάχιστα προνόμια και διαχωρισμός καθηκόντων: τα ιδρύματα διαχειρίζονται τα δικαιώματα πρόσβασης σε πληροφοριακούς πόρους και τα υποστηρικτικά συστήματά τους, συμπεριλαμβανομένης της απομακρυσμένης πρόσβασης, βάσει της αρχής της «ελάχιστης απαιτούμενης πληροφόρησης». Στους χρήστες χορηγούνται ελάχιστα δικαιώματα πρόσβασης, τα οποία είναι απολύτως απαραίτητα για την εκτέλεση των καθηκόντων τους (αρχή των «ελάχιστων προνομίων»), δηλαδή αποτρέπεται η αδικαιολόγητη πρόσβαση σε μεγάλο εύρος δεδομένων ή η χορήγηση συνδυασμένων δικαιωμάτων πρόσβασης που θα μπορούσαν να χρησιμοποιηθούν για την παράκαμψη δικλείδων ασφάλειας (αρχή του «διαχωρισμού των καθηκόντων»).

β) Λογοδοσία χρήστη: τα ιδρύματα περιορίζουν, στο μέτρο του δυνατού, τη χρήση γενικών και κοινών λογαριασμών χρηστών και διασφαλίζουν τη δυνατότητα ταυτοποίησης των χρηστών για τις ενέργειες που πραγματοποιούνται στα συστήματα ΤΠΕ.

γ) Δικαιώματα διαβαθμισμένης πρόσβασης: τα ιδρύματα εφαρμόζουν ισχυρές δικλείδες ασφάλειας για τη διαβαθμισμένη πρόσβαση στα συστήματα ΤΠΕ, περιορίζοντας αυστηρά την πρόσβαση και παρακολουθώντας επισταμένως τους λογαριασμούς με αυξημένα δικαιώματα πρόσβασης στα εν λόγω συστήματα (π.χ. λογαριασμούς διαχειριστών). Για την εξασφάλιση ασφαλούς επικοινωνίας και τη μείωση του κινδύνου ΤΠΕ και ασφάλειας, η απομακρυσμένη διαχειριστική πρόσβαση σε κρίσιμα συστήματα ΤΠΕ επιτρέπεται μόνο με βάση την αρχή της «ελάχιστης απαιτούμενης πληροφόρησης» και εφόσον χρησιμοποιούνται διαδικασίες αυστηρής αυθεντικοποίησης.

δ) Καταγραφή της δραστηριότητας των χρηστών: κατ’ ελάχιστον, καταγράφονται και παρακολουθούνται όλες οι δραστηριότητες των προνομιούχων χρηστών. Τα αρχεία καταγραφής πρόσβασης προστατεύονται από μη εξουσιοδοτημένη τροποποίηση ή διαγραφή και διατηρούνται για χρονικό διάστημα ανάλογο της κρισιμότητας των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων που έχουν προσδιοριστεί, σύμφωνα με την Ενότητα 3.3, με την επιφύλαξη των απαιτήσεων διατήρησης που προβλέπονται στο ενωσιακό και στο εθνικό δίκαιο. Τα ιδρύματα χρησιμοποιούν τις εν λόγω πληροφορίες για να διευκολύνουν την αναγνώριση και τη διερεύνηση ασυνήθιστων δραστηριοτήτων που έχουν εντοπιστεί κατά την παροχή υπηρεσιών.

ε) Διαχείριση πρόσβασης: τα δικαιώματα πρόσβασης χορηγούνται, ανακαλούνται ή τροποποιούνται εγκαίρως, σύμφωνα με προκαθορισμένες εγκριτικές ροές εργασίας στις οποίες συμμετέχει ο επιχειρηματικός ιδιοκτήτης των πληροφοριών οι οποίες συνιστούν αντικείμενο πρόσβασης (ιδιοκτήτης πληροφοριακών πόρων). Σε περίπτωση λύσης της υπαλληλικής σχέσης, τα δικαιώματα πρόσβασης ανακαλούνται άμεσα.

στ) Επανεξέταση πρόσβασης: τα δικαιώματα πρόσβασης επανεξετάζονται σε περιοδική βάση ώστε να διασφαλίζεται ότι οι χρήστες δεν διαθέτουν υπερβολικά προνόμια και ότι τα δικαιώματα πρόσβασης ανακαλούνται όταν δεν είναι πλέον απαραίτητα.

ζ) Μέθοδοι αυθεντικοποίησης: τα ιδρύματα επιβάλλουν μεθόδους αυθεντικοποίησης επαρκώς αξιόπιστες ώστε να διασφαλίζεται με κατάλληλο και αποτελεσματικό τρόπο η συμμόρφωση προς τις πολιτικές και τις διαδικασίες ελέγχου της πρόσβασης. Οι μέθοδοι αυθεντικοποίησης είναι ανάλογες προς τον βαθμό κρισιμότητας των συστημάτων ΤΠΕ, των πληροφοριών ή των διεργασιών που αποτελούν αντικείμενο πρόσβασης. Στο πλαίσιο αυτό περιλαμβάνονται, κατ’ ελάχιστον, σύνθετοι κωδικοί πρόσβασης ή ισχυρότερες μέθοδοι αυθεντικοποίησης

(όπως η αυθεντικοποίηση δύο παραγόντων), βάσει του αντίστοιχου κινδύνου.

36. Η ηλεκτρονική πρόσβαση από εφαρμογές σε δεδομένα και συστήματα ΤΠΕ περιορίζεται στο ελάχιστο επίπεδο που απαιτείται για την παροχή της αντίστοιχης υπηρεσίας.

4.3 Φυσική ασφάλεια

37. Τα μέτρα φυσικής ασφάλειας των ιδρυμάτων καθορίζονται, τεκμηριώνονται και εφαρμόζονται με σκοπό την προστασία των εγκαταστάσεων, των μηχανογραφικών κέντρων και των ευαίσθητων χώρων τους από μη εξουσιοδοτημένη πρόσβαση και από περιβαλλοντικούς κινδύνους.

38. Η φυσική πρόσβαση σε συστήματα ΤΠΕ επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα. Η εξουσιοδότηση παρέχεται ανάλογα με τα καθήκοντα και τις αρμοδιότητες του ατόμου και περιορίζεται σε άτομα που υποβάλλονται σε κατάλληλη εκπαίδευση και παρακολούθηση. Η φυσική πρόσβαση επανεξετάζεται σε περιοδική βάση ώστε να διασφαλίζεται η άμεση ανάκληση μη αναγκαίων δικαιωμάτων πρόσβασης, όταν αυτά δεν είναι απαραίτητα.

39. Τα ενδεδειγμένα μέτρα για την προστασία από περιβαλλοντικούς κινδύνους και κακόβουλες ενέργειες είναι ανάλογα προς τη σημασία των κτιρίων και την κρισιμότητα των λειτουργιών ή των συστημάτων ΤΠΕ που βρίσκονται στα εν λόγω κτίρια.

4.4 Ασφάλεια λειτουργιών ΤΠΕ

40. Τα ιδρύματα εφαρμόζουν διαδικασίες για την πρόληψη της εμφάνισης ζητημάτων ασφάλειας στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ, ενώ ελαχιστοποιούν επίσης τις επιπτώσεις τους στην παροχή υπηρεσιών ΤΠΕ. Στις διαδικασίες αυτές περιλαμβάνονται τα ακόλουθα μέτρα:

α) εντοπισμός πιθανών ευπαθειών, οι οποίες αξιολογούνται και αποκαθίστανται, διασφαλίζοντας ότι το λογισμικό και το υλικολογισμικό των συστημάτων, καθώς και το λογισμικό που παρέχουν τα ιδρύματα στους εσωτερικούς και τους εξωτερικούς χρήστες τους, είναι ενημερωμένα, εγκαθιστώντας κρίσιμες ενημερώσεις ασφάλειας ή εφαρμόζοντας αντισταθμιστικούς ελέγχους,

β) εφαρμογή βασικών γραμμών (baseline) ασφαλούς παραμετροποίησης των δικτυακών στοιχείων,

γ) υλοποίηση κατάτμησης δικτύου (network segmentation), συστημάτων πρόληψης απώλειας δεδομένων (data loss prevention) και κρυπτογράφηση της κίνησης του δικτύου (σύμφωνα με την κατηγοριοποίηση των δεδομένων),

δ) εφαρμογή της προστασίας των τελικών σημείων (endpoint), συμπεριλαμβανομένων διακομιστών, σταθμών εργασίας και φορητών συσκευών. Τα ιδρύματα αξιολογούν αν τα τελικά σημεία πληρούν τα πρότυπα ασφάλειας τα οποία έχουν ορισθεί από τα ίδια τα ιδρύματα πριν χορηγηθεί σε αυτά πρόσβαση στο εταιρικό δίκτυο,

ε) εξασφάλιση της εφαρμογής μηχανισμών για την επαλήθευση της ακεραιότητας του λογισμικού, του υλικολογισμικού και των δεδομένων,

στ) κρυπτογράφηση των δεδομένων όταν αποθηκεύονται και διαβιβάζονται (σύμφωνα με την κατηγοριοποίηση των δεδομένων).

41. Επιπλέον, τα ιδρύματα προσδιορίζουν σε συνεχή βάση αν οι αλλαγές στο υφιστάμενο επιχειρησιακό περιβάλλον επηρεάζουν τα ισχύοντα μέτρα ασφάλειας ή αν απαιτείται η λήψη πρόσθετων μέτρων για τη δέουσα μείωση των σχετικών κινδύνων. Οι αλλαγές αυτές αποτελούν μέρος της επίσημης διαδικασίας διαχείρισης αλλαγών που εφαρμόζεται από τα ιδρύματα και η οποία διασφαλίζει ότι οι αλλαγές προγραμματίζονται, υποβάλλονται σε δοκιμές, τεκμηριώνονται, εγκρίνονται και υλοποιούνται δεόντως.

4.5 Παρακολούθηση της ασφάλειας

42. Τα ιδρύματα αναπτύσσουν και εφαρμόζουν πολιτικές και διαδικασίες για τον εντοπισμό ασυνήθιστων δραστηριοτήτων με ενδεχόμενο αντίκτυπο στην ασφάλεια των πληροφοριών των ιδρυμάτων και για τη δέουσα αντιμετώπιση αυτών των συμβάντων. Στο πλαίσιο αυτής της συνεχούς παρακολούθησης, τα ιδρύματα διαθέτουν κατάλληλες και αποτελεσματικές δυνατότητες για τον εντοπισμό και την αναφορά φυσικής ή λογικής παρείσφρησης καθώς και παραβιάσεων της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών πόρων. Οι διεργασίες συνεχούς παρακολούθησης και εντοπισμού καλύπτουν:

α) συναφείς εσωτερικούς και εξωτερικούς παράγοντες, συμπεριλαμβανομένων διαχειριστικών λειτουργιών τόσο επιχειρηματικών όσο και ΤΠΕ,

β) συναλλαγές, για τον εντοπισμό κατάχρησης πρόσβασης τόσο από τρίτους ή άλλες οντότητες όσο και εσωτερικής κατάχρησης πρόσβασης,

γ) πιθανές εσωτερικές και εξωτερικές απειλές.

43. Τα ιδρύματα δημιουργούν και εφαρμόζουν διαδικασίες και οργανωτικές δομές για τον προσδιορισμό και τη συνεχή παρακολούθηση απειλών για την ασφάλεια που θα μπορούσαν να επηρεάσουν σημαντικά την ικανότητά τους να παρέχουν υπηρεσίες. Τα ιδρύματα παρακολουθούν ενεργά τις τεχνολογικές εξελίξεις προκειμένου να διασφαλίζουν ότι έχουν επίγνωση των κινδύνων ασφάλειας. Τα ιδρύματα εφαρμόζουν μέτρα ανίχνευσης, για παράδειγμα για τον εντοπισμό πιθανών διαρροών πληροφοριών, κακόβουλου κώδικα, λοιπών απειλών για την ασφάλεια και ευρέως γνωστών ευπαθειών λογισμικού και υλισμικού, και ελέγχουν αν υπάρχουν αντίστοιχες ενημερώσεις ασφάλειας.

44. Η διαδικασία παρακολούθησης της ασφάλειας βοηθά επίσης τα ιδρύματα να κατανοούν τη φύση των περιστατικών λειτουργικού κινδύνου ή των περιστατικών ασφάλειας, να αναγνωρίζουν τάσεις και να στηρίζουν τις έρευνες του οργανισμού.

4.6 Επανεξετάσεις, αξιολογήσεις και δοκιμές της ασφάλειας πληροφοριών

45. Τα ιδρύματα διενεργούν ποικίλες επανεξετάσεις, αξιολογήσεις και δοκιμές της ασφάλειας πληροφοριών ώστε να διασφαλίζεται ο αποτελεσματικός εντοπισμός ευπαθειών στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ των ιδρυμάτων. Για παράδειγμα, τα ιδρύματα μπορούν να διενεργούν ανάλυση ελλείψεων (gap analysis) με βάση τα πρότυπα ασφάλειας πληροφοριών, ελέγχους συμμόρφωσης, εσωτερικούς και εξωτερικούς ελέγχους των συστημάτων ΤΠΕ ή ελέγχους φυσικής ασφάλειας.

Επιπλέον, τα ιδρύματα λαμβάνουν υπόψη ορθές πρακτικές, όπως επισκόπηση πηγαίου κώδικα, αξιολογήσεις ευπαθειών, δοκιμές παρείσδυσης (penetration test) και ασκήσεις «κόκκινης ομάδας» (red team exercises).

46. Τα ιδρύματα θεσπίζουν και εφαρμόζουν πλαίσιο δοκιμών ασφάλειας πληροφοριών, το οποίο επικυρώνει την αξιοπιστία και την αποτελεσματικότητα των οικείων μέτρων ασφάλειας πληροφοριών, και διασφαλίζουν ότι στο εν λόγω πλαίσιο λαμβάνονται υπόψη απειλές και ευπάθειες, οι οποίες προσδιορίζονται μέσω της παρακολούθησης απειλών και της διαδικασίας αξιολόγησης κινδύνων ΤΠΕ και ασφάλειας.

47. Το πλαίσιο δοκιμών ασφάλειας πληροφοριών διασφαλίζει ότι οι δοκιμές:

α) διενεργούνται από ανεξάρτητους φορείς διεξαγωγής δοκιμών που διαθέτουν επαρκείς γνώσεις, δεξιότητες και εξειδίκευση στη διενέργεια δοκιμών όσον αφορά μέτρα ασφάλειας πληροφοριών και δεν εμπλέκονται στην ανάπτυξη των μέτρων ασφάλειας πληροφοριών,

β) περιλαμβάνουν επαρκείς ελέγχους ευπαθειών και δοκιμές παρείσδυσης (μεταξύ των οποίων και δοκιμές παρείσδυσης βάσει απειλών όπου κρίνεται αναγκαίο και σκόπιμο) ανάλογα με το επίπεδο κινδύνου που προσδιορίζεται σε σχέση με τις επιχειρηματικές διεργασίες και τα συστήματα.

48. Τα ιδρύματα διενεργούν συνεχείς και επαναλαμβανόμενες δοκιμές των μέτρων ασφάλειας. Οι εν λόγω δοκιμές διενεργούνται τουλάχιστον σε ετήσια βάση για το σύνολο των κρίσιμων συστημάτων ΤΠΕ, σύμφωνα με την παράγραφο 21, ενώ για τις υπηρεσίες πληρωμών εντάσσονται στο πλαίσιο της ολοκληρωμένης αξιολόγησης των κινδύνων ασφάλειας που συνδέονται με τις υπηρεσίες πληρωμών τις οποίες παρέχουν, σύμφωνα με την παρ. 2 του άρθρου 94 του ν. 4537/2018. Τα μη κρίσιμα συστήματα υποβάλλονται τακτικά σε δοκιμή σύμφωνα με μια προσέγγιση βάσει κινδύνου, τουλάχιστον ανά τρία (3) έτη.

49. Τα ιδρύματα διασφαλίζουν ότι οι δοκιμές των μέτρων ασφάλειας διενεργούνται σε περίπτωση αλλαγών στην υποδομή, στις διεργασίες ή στις διαδικασίες, καθώς και σε περίπτωση αλλαγών λόγω μειζόνων περιστατικών λειτουργικού κινδύνου ή μειζόνων περιστατικών ασφάλειας ή λόγω της έκδοσης νέων ή σημαντικά τροποποιημένων κρίσιμων εφαρμογών διαδικτύου.

50. Τα ιδρύματα παρακολουθούν και αξιολογούν τα αποτελέσματα των δοκιμών ασφάλειας και επικαιροποιούν αναλόγως και χωρίς αδικαιολόγητες καθυστερήσεις τα μέτρα ασφάλειάς τους στην περίπτωση των κρίσιμων συστημάτων ΤΠΕ.

51. Για τους ΠΥΠ, το πλαίσιο δοκιμών περιλαμβάνει επίσης τα μέτρα ασφάλειας που αφορούν: 1) τα τερματικά πληρωμών και τις συσκευές που χρησιμοποιούνται για την παροχή υπηρεσιών πληρωμών, 2) τα τερματικά πληρωμών και τις συσκευές που χρησιμοποιούνται για την αυθεντικοποίηση των χρηστών υπηρεσιών πληρωμών και 3) τις συσκευές και το λογισμικό που παρέχουν οι ΠΥΠ στους χρήστες υπηρεσιών πληρωμών για την παραγωγή/λήψη κωδικού αυθεντικοποίησης.

52. Βάσει των απειλών για την ασφάλεια που παρατηρούνται και των αλλαγών που επέρχονται, διενεργούνται δοκιμές σύμφωνα με σενάρια συναφών και γνωστών δυνητικών επιθέσεων.

4.7 Κατάρτιση και ευαισθητοποίηση σε θέματα ασφάλειας πληροφοριών

53. Τα ιδρύματα εφαρμόζουν εκπαιδευτικό πρόγραμμα, συμπεριλαμβανομένων περιοδικών προγραμμάτων ευαισθητοποίησης σε θέματα ασφάλειας, για όλο το προσωπικό και τους αναδόχους έργων προκειμένου να διασφαλίζεται η επαρκής κατάρτισή τους για την άσκηση των καθηκόντων και των αρμοδιοτήτων τους, σύμφωνα με τις σχετικές πολιτικές και διαδικασίες ασφάλειας για τη μείωση των φαινομένων ανθρώπινου σφάλματος, κλοπής, απάτης, κατάχρησης ή απώλειας και για να γνωρίζουν πώς πρέπει να αντιμετωπίζουν τους κινδύνους που συνδέονται με την ασφάλεια των πληροφοριών. Τα ιδρύματα διασφαλίζουν ότι το εκπαιδευτικό πρόγραμμα παρέχει κατάρτιση για το σύνολο των μελών του προσωπικού και των αναδόχων έργων τουλάχιστον σε ετήσια βάση.

ΚΕΦΑΛΑΙΟ V. ΔΙΑΧΕΙΡΙΣΗ ΛΕΙΤΟΥΡΓΙΩΝ ΤΠΕ

54. Τα ιδρύματα διαχειρίζονται τις οικείες λειτουργίες ΤΠΕ βάσει τεκμηριωμένων και εφαρμοζόμενων διεργασιών και διαδικασιών (οι οποίες περιλαμβάνουν, όσον αφορά τους ΠΥΠ, το έγγραφο που περιγράφει την πολιτική ασφάλειας σύμφωνα με το στοιχείο (ι) της παρ. 1 του άρθρου 5 του ν. 4537/2018) που εγκρίνονται από το Διοικητικό Συμβούλιο. Το εν λόγω σύνολο εγγράφων καθορίζει τον τρόπο με τον οποίο τα ιδρύματα διασφαλίζουν τη λειτουργία, την παρακολούθηση και τον έλεγχο των συστημάτων ΤΠΕ και των υπηρεσιών ΤΠΕ τους, συμπεριλαμβανομένης της τεκμηρίωσης των κρίσιμων λειτουργιών ΤΠΕ, ενώ επίσης παρέχει στα ιδρύματα τη δυνατότητα τήρησης ενημερωμένου καταλόγου πόρων ΤΠΕ.

55. Τα ιδρύματα μεριμνούν ώστε οι επιδόσεις των οικείων λειτουργιών ΤΠΕ να συνάδουν με τις απαιτήσεις των επιχειρηματικών δραστηριοτήτων τους. Τα ιδρύματα διατηρούν και βελτιώνουν, όπου είναι εφικτό, την αποτελεσματικότητα των οικείων λειτουργιών ΤΠΕ, συμπεριλαμβανομένης, ενδεικτικά, της ανάγκης εξέτασης του τρόπου ελαχιστοποίησης πιθανών σφαλμάτων που προκύπτουν από την εκτέλεση χειροκίνητων εργασιών.

56. Τα ιδρύματα εφαρμόζουν διαδικασίες καταγραφής και παρακολούθησης για τις κρίσιμες λειτουργίες ΤΠΕ, ώστε να είναι εφικτή η ανίχνευση, η ανάλυση και η διόρθωση σφαλμάτων.

57. Τα ιδρύματα τηρούν πλήρη και ενήμερο κατάλογο των ΤΠΕ πόρων τους (συμπεριλαμβανομένων των συστημάτων ΤΠΕ, των δικτυακών συσκευών, των βάσεων δεδομένων κ.λπ.). Στον κατάλογο πόρων ΤΠΕ αποθηκεύονται οι παράμετροι των πόρων ΤΠΕ, καθώς και οι σύνδεσμοι και οι αλληλεξαρτήσεις μεταξύ των διαφόρων πόρων ΤΠΕ, ώστε να είναι εφικτή η εφαρμογή ορθής διεργασίας παραμετροποίησης και διαχείρισης αλλαγών.

58. Ο κατάλογος πόρων ΤΠΕ είναι επαρκώς λεπτομερής ώστε να παρέχεται η δυνατότητα άμεσου προσδιορισμού του πόρου ΤΠΕ, της θέσης του, της κατηγοριοποίησης ασφάλειας και του καθεστώτος ιδιοκτησίας του. Οι αλληλεξαρτήσεις μεταξύ των πόρων τεκμηριώνονται ώστε να διευκολύνεται η αντιμετώπιση περιστατικών

ασφάλειας και περιστατικών λειτουργικού κινδύνου, συμπεριλαμβανομένων κυβερνο-επιθέσεων.

59. Τα ιδρύματα παρακολουθούν και διαχειρίζονται τους κύκλους ζωής των πόρων ΤΠΕ ώστε να διασφαλίζεται ότι εξακολουθούν να πληρούν και να υποστηρίζουν τις απαιτήσεις διαχείρισης των επιχειρηματικών δραστηριοτήτων και των κινδύνων. Τα ιδρύματα παρακολουθούν αν οι ΤΠΕ πόροι τους υποστηρίζονται από τους εξωτερικούς ή εσωτερικούς τους προμηθευτές και σχεδιαστές εφαρμογών, καθώς και αν όλες οι σχετικές ενημερώσεις και αναβαθμίσεις εφαρμόζονται βάσει τεκμηριωμένων διαδικασιών. Οι κίνδυνοι που απορρέουν από παρωχημένους ή μη υποστηριζόμενους πόρους ΤΠΕ αξιολογούνται και περιορίζονται.

60. Τα ιδρύματα εφαρμόζουν διαδικασίες σχεδιασμού και παρακολούθησης των επιδόσεων και της χωρητικότητας με σκοπό την έγκαιρη πρόληψη, ανίχνευση και αντιμετώπιση σημαντικών ζητημάτων όσον αφορά τις επιδόσεις και τις ελλείψεις χωρητικότητας των συστημάτων ΤΠΕ.

61. Τα ιδρύματα καθορίζουν και εφαρμόζουν διαδικασίες δημιουργίας εφεδρικών αντιγράφων και αποκατάστασης δεδομένων και συστημάτων ΤΠΕ ώστε να διασφαλίζεται η δυνατότητα ανάκτησής τους σύμφωνα με τις απαιτήσεις. Το πεδίο εφαρμογής και η συχνότητα της δημιουργίας εφεδρικών αντιγράφων καθορίζονται σύμφωνα με τις απαιτήσεις επιχειρησιακής ανάκαμψης και την κρισιμότητα των δεδομένων και των συστημάτων ΤΠΕ, και αξιολογούνται με βάση τη διενεργηθείσα αξιολόγηση κινδύνων. Οι δοκιμές των διαδικασιών δημιουργίας εφεδρικών αντιγράφων και αποκατάστασης διενεργούνται σε περιοδική βάση.

62. Τα ιδρύματα διασφαλίζουν ότι τα εφεδρικά αντίγραφα δεδομένων και συστημάτων ΤΠΕ αποθηκεύονται με ασφάλεια και σε αρκετά απομακρυσμένη τοποθεσία από τον κύριο χώρο, ώστε να μην εκτίθενται στους ίδιους κινδύνους.

5.1 Διαχείριση περιστατικών και προβλημάτων ΤΠΕ

63. Τα ιδρύματα δημιουργούν και εφαρμόζουν διαδικασία διαχείρισης περιστατικών και προβλημάτων για την παρακολούθηση και την καταγραφή περιστατικών λειτουργικού κινδύνου και περιστατικών ασφάλειας ΤΠΕ, καθώς και για να εξασφαλίζεται η δυνατότητα των ιδρυμάτων να συνεχίζουν ή να επανεκκινούν εγκαίρως τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες σε περίπτωση εμφάνισης δυσλειτουργιών. Τα ιδρύματα καθορίζουν κατάλληλα κριτήρια και κατώτατα όρια για την κατηγοριοποίηση συμβάντων ως περιστατικών λειτουργικού κινδύνου ή περιστατικών ασφάλειας, καθώς και δείκτες έγκαιρης προειδοποίησης που θα χρησιμεύουν ως ειδοποιήσεις ώστε να καθίσταται δυνατός ο έγκαιρος εντοπισμός των εν λόγω περιστατικών. Όσον αφορά τους ΠΥΠ, τα εν λόγω κριτήρια και κατώτατα όρια εφαρμόζονται με την επιφύλαξη της ταξινόμησης μειζόνων συμβάντων σύμφωνα με το άρθρο 95 του ν. 4537/2018 και την ΠΕΕ 157/3/02.04.2019.

64. Για την ελαχιστοποίηση των επιπτώσεων δυσμενών συμβάντων και την εξασφάλιση της δυνατότητας έγκαιρης ανάκαμψης, τα ιδρύματα εφαρμόζουν κατάλληλες διεργασίες και οργανωτικές δομές για τη διασφάλιση συνεκτικής και ολοκληρωμένης παρακολούθησης, διαχείρισης και επανεξέτασης των περιστατικών λειτουργικού κινδύνου και των περιστατικών ασφάλειας, καθώς και για τη διασφάλιση του προσδιορισμού και της εξάλειψης των βασικών αιτιών, με σκοπό την αποτροπή επαναλαμβανόμενων περιστατικών. Στη διαδικασία διαχείρισης περιστατικών και προβλημάτων καθορίζονται:

α) οι διαδικασίες για τον προσδιορισμό, την ανίχνευση, την καταγραφή, την κατηγοριοποίηση και την ταξινόμηση των περιστατικών βάσει προτεραιοποίησης ανάλογα με την κρισιμότητα των επιχειρησιακών λειτουργιών,

β) οι ρόλοι και οι αρμοδιότητες για διαφορετικά σενάρια περιστατικών (π.χ. σφάλματα, δυσλειτουργίες, κυβερνο-επιθέσεις),

γ) διαδικασίες διαχείρισης προβλημάτων για τον προσδιορισμό, την ανάλυση και την επίλυση των βασικών αιτιών ενός ή περισσότερων περιστατικών: τα ιδρύματα αναλύουν τα περιστατικά λειτουργικού κινδύνου ή τα περιστατικά ασφάλειας που είναι πιθανό να επηρεάζουν το ίδρυμα και έχουν προσδιοριστεί ή έχουν εμφανιστεί εντός και/ή εκτός του οργανισμού, ενώ επίσης λαμβάνουν υπόψη τα κύρια διδάγματα που αντλούνται από τις εν λόγω αναλύσεις και επικαιροποιούν αναλόγως τα μέτρα ασφάλειας,

δ) αποτελεσματικά σχέδια εσωτερικής επικοινωνίας, συμπεριλαμβανομένων διαδικασιών γνωστοποίησης περιστατικών και παραπομπής σε ανώτερη βαθμίδα της ιεραρχικής κλίμακας - οι οποίες καλύπτουν επίσης καταγγελίες πελατών σχετικά με θέματα ασφάλειας- ώστε να διασφαλίζεται ότι:

i) τα περιστατικά με δυνητικά σοβαρές δυσμενείς επιπτώσεις σε συστήματα και υπηρεσίες ΤΠΕ κρίσιμης σημασίας αναφέρονται στα αρμόδια ανώτερα διοικητικά στελέχη και στα ανώτερα διοικητικά στελέχη ΤΠΕ,

ii) το Διοικητικό Συμβούλιο ενημερώνεται εκτάκτως σε περίπτωση σημαντικών περιστατικών και επίσης, κατ’ ελάχιστον, για τις επιπτώσεις, την αντιμετώπιση και τους πρόσθετους ελέγχους που πρέπει να καθοριστούν συνεπεία των περιστατικών,

ε) διαδικασίες αντιμετώπισης περιστατικών για τη μείωση των επιπτώσεων που συνδέονται με αυτά και για την εξασφάλιση της δυνατότητας έγκαιρης και ασφαλούς επαναλειτουργίας της υπηρεσίας,

στ) ειδικά σχέδια εξωτερικής επικοινωνίας για τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες, με στόχο:

i) τη συνεργασία με τους σχετικούς ενδιαφερομένους για την αποτελεσματική αντιμετώπιση του περιστατικού και την ανάκαμψη μετά από αυτό,

ii) την έγκαιρη παροχή πληροφοριών σε εξωτερικά μέρη (π.χ. πελάτες, άλλους συμμετέχοντες στην αγορά, εποπτική αρχή) κατά περίπτωση και σύμφωνα με τις ισχύουσες κανονιστικές διατάξεις.

ΚΕΦΑΛΑΙΟ VI. ΔΙΑΧΕΙΡΙΣΗ ΕΡΓΩΝ ΚΑΙ ΑΛΛΑΓΩΝ ΤΠΕ

6.1 Διαχείριση έργων ΤΠΕ

65. Τα ιδρύματα εφαρμόζουν πρόγραμμα και/ή διαδικασία διακυβέρνησης έργων για τον καθορισμό των ρόλων, των αρμοδιοτήτων και των υποχρεώσεων λογοδοσίας με σκοπό την αποτελεσματική υποστήριξη της υλοποίησης της στρατηγικής ΤΠΕ.

66. Τα ιδρύματα μεριμνούν δεόντως για την παρακολούθηση και τη μείωση των κινδύνων που απορρέουν από το οικείο χαρτοφυλάκιο έργων ΤΠΕ (διαχείριση προγράμματος έργων), λαμβάνοντας επίσης υπόψη τους κινδύνους που ενδέχεται να προκύπτουν από αλληλεξαρτήσεις μεταξύ διαφόρων έργων και από την εξάρτηση πολλαπλών έργων από τους ίδιους πόρους και/ή την ίδια εξειδίκευση.

67. Τα ιδρύματα καταρτίζουν και εφαρμόζουν πολιτική διαχείρισης έργων ΤΠΕ, η οποία περιλαμβάνει τουλάχιστον:

α) στόχους έργου,

β) ρόλους και αρμοδιότητες,

γ) αξιολόγηση κινδύνων έργου,

δ) σχέδιο, χρονοδιάγραμμα και στάδια έργου, ε) βασικά ορόσημα,

στ) απαιτήσεις διαχείρισης αλλαγών.

68. Η πολιτική διαχείρισης έργων ΤΠΕ διασφαλίζει ότι οι απαιτήσεις ασφάλειας πληροφοριών αναλύονται και εγκρίνονται από λειτουργία, η οποία είναι ανεξάρτητη από τη λειτουργία ανάπτυξης.

69. Τα ιδρύματα διασφαλίζουν ότι στην ομάδα έργου εκπροσωπούνται όλοι οι τομείς που επηρεάζονται από το έργο ΤΠΕ και η ομάδα έργου διαθέτει τις γνώσεις που απαιτούνται για την εξασφάλιση της ασφαλούς και επιτυχούς υλοποίησης του έργου.

70. Ο σχεδιασμός και η πρόοδος των έργων ΤΠΕ, καθώς και οι σχετικοί κίνδυνοί τους, αποτελούν αντικείμενο αναφορών που υποβάλλονται στο Διοικητικό Συμβούλιο, είτε μεμονωμένα είτε συγκεντρωτικά, ανάλογα με τη σημασία και το μέγεθος των έργων ΤΠΕ, σε τακτική και έκτακτη βάση, όπως αρμόζει κατά περίπτωση. Τα ιδρύματα συμπεριλαμβάνουν τον κίνδυνο έργου στο πλαίσιο της διαχείρισης κινδύνων τους.

6.2 Απόκτηση και ανάπτυξη συστημάτων ΤΠΕ

71. Τα ιδρύματα αναπτύσσουν και εφαρμόζουν διαδικασία η οποία διέπει την απόκτηση, την ανάπτυξη και τη συντήρηση συστημάτων ΤΠΕ. Η διαδικασία αυτή σχεδιάζεται χρησιμοποιώντας προσέγγιση βάσει κινδύνου.

7.2 Τα ιδρύματα μεριμνούν ώστε, πριν από οποιαδήποτε απόκτηση ή ανάπτυξη συστημάτων ΤΠΕ, να ορίζονται με σαφήνεια και να εγκρίνονται - από την αρμόδια για τη συγκεκριμένη επιχειρηματική δραστηριότητα υπηρεσιακή μονάδα - οι λειτουργικές και μη λειτουργικές απαιτήσεις (συμπεριλαμβανομένων των απαιτήσεων ασφάλειας πληροφοριών).

73. Τα ιδρύματα διασφαλίζουν ότι εφαρμόζονται μέτρα για τη μείωση του κινδύνου ακούσιας τροποποίησης ή εσκεμμένης παραποίησης των συστημάτων ΤΠΕ κατά τη διάρκεια της ανάπτυξης και υλοποίησης του περιβάλλοντος παραγωγής.

74. Τα ιδρύματα διαθέτουν μεθοδολογία για τις δοκιμές και την αποδοχή των συστημάτων ΤΠΕ πριν από την πρώτη χρήση τους. Στην μεθοδολογία αυτή λαμβάνεται υπόψη η κρισιμότητα των επιχειρησιακών διεργασιών και πόρων. Οι δοκιμές εξασφαλίζουν ότι τα νέα συστήματα ΤΠΕ λειτουργούν σύμφωνα με τα προβλεπόμενα. Επίσης, χρησιμοποιούν περιβάλλοντα δοκιμών τα οποία αντικατοπτρίζουν επαρκώς το περιβάλλον παραγωγής.

75. Τα ιδρύματα υποβάλλουν σε δοκιμές τα συστήματα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τα μέτρα ασφάλειας πληροφοριών για τον προσδιορισμό πιθανών αδυναμιών, παραβιάσεων και περιστατικών ασφάλειας.

76. Τα ιδρύματα υλοποιούν χωριστά περιβάλλοντα ΤΠΕ για τη διασφάλιση του κατάλληλου διαχωρισμού καθηκόντων και για τη μείωση των επιπτώσεων των μη επαληθευμένων αλλαγών στα συστήματα παραγωγής. Ειδικότερα, τα ιδρύματα μεριμνούν για τον διαχωρισμό των περιβαλλόντων παραγωγής από τα περιβάλλοντα ανάπτυξης, δοκιμών και από άλλα μη παραγωγικά περιβάλλοντα. Τα ιδρύματα διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων παραγωγής και σε μη παραγωγικά περιβάλλοντα. Η πρόσβαση στα δεδομένα παραγωγής περιορίζεται σε εξουσιοδοτημένους χρήστες.

77. Τα ιδρύματα εφαρμόζουν μέτρα για την προστασία της ακεραιότητας του πηγαίου κώδικα των συστημάτων ΤΠΕ που αναπτύσσονται εσωτερικά. Επίσης, τεκμηριώνουν την ανάπτυξη, την εφαρμογή, τη λειτουργία και/ή την παραμετροποίηση των συστημάτων ΤΠΕ κατά τρόπο ολοκληρωμένο, ώστε να περιορίζεται τυχόν αδικαιολόγητη εξάρτηση από ειδικούς επί του αντικειμένου αυτού. Η τεκμηρίωση του συστήματος ΤΠΕ περιλαμβάνει, κατά περίπτωση, τουλάχιστον την τεκμηρίωση για τον χρήστη, την τεχνική τεκμηρίωση του συστήματος και τις διαδικασίες λειτουργίας.

78. Οι διεργασίες των ιδρυμάτων για την απόκτηση, την ανάπτυξη και την απόσυρση συστημάτων ΤΠΕ εφαρμόζονται επίσης σε συστήματα ΤΠΕ των οποίων η ανάπτυξη ή η διαχείριση πραγματοποιείται από τους τελικούς χρήστες της επιχειρηματικής λειτουργίας εκτός της οργανωτικής δομής ΤΠΕ (π.χ. υπολογιστικές εφαρμογές τελικού χρήστη) με προσέγγιση βάσει κινδύνου. Τα ιδρύματα τηρούν μητρώο των εν λόγω εφαρμογών που υποστηρίζουν κρίσιμες επιχειρηματικές λειτουργίες ή διεργασίες.

6.3 Διαχείριση αλλαγών ΤΠΕ

79. Τα ιδρύματα θεσπίζουν και εφαρμόζουν διαδικασία διαχείρισης αλλαγών ΤΠΕ ώστε να διασφαλίζεται ότι όλες οι αλλαγές στα συστήματα ΤΠΕ καταγράφονται, υποβάλλονται σε δοκιμές, αξιολογούνται, εγκρίνονται, υλοποιούνται και επαληθεύονται με ελεγχόμενο τρόπο. Τα ιδρύματα χειρίζονται τις αλλαγές κατά τη διάρκεια περιπτώσεων έκτακτης ανάγκης (δηλαδή αλλαγές που πρέπει να εφαρμοσθούν το συντομότερο δυνατόν) σύμφωνα με διαδικασίες που παρέχουν επαρκείς διασφαλίσεις.

80. Τα ιδρύματα προσδιορίζουν αν οι αλλαγές στο υφιστάμενο λειτουργικό περιβάλλον επηρεάζουν τα ισχύοντα μέτρα ασφάλειας ή απαιτούν τη λήψη πρόσθετων μέτρων για τη μείωση των αντίστοιχων κινδύνων. Οι αλλαγές αυτές πραγματοποιούνται σύμφωνα με την επίσημη διαδικασία διαχείρισης αλλαγών που εφαρμόζουν τα ιδρύματα.

ΚΕΦΑΛΑΙΟ VII. ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ

81. Τα ιδρύματα καθιερώνουν διαδικασία διαχείρισης της επιχειρησιακής συνέχειας με στόχο τη μεγιστοποίηση της ικανότητάς τους να παρέχουν υπηρεσίες σε συ-

νεχή βάση και τον περιορισμό των ζημιών σε περίπτωση σοβαρής διαταραχής της δραστηριότητάς τους, σύμφωνα με την παρ. 2 του άρθρο 77 του ν. 4261/2014 και τον τίτλο VI των κατευθυντήριων γραμμών της ΕΑΤ σχετικά με την εσωτερική διακυβέρνηση (EBA/GL/2017/11).

7.1 Ανάλυση των επιχειρηματικών επιπτώσεων

82. Στο πλαίσιο της χρηστής διαχείρισης της επιχειρησιακής συνέχειας, τα ιδρύματα διενεργούν ανάλυση των επιχειρηματικών επιπτώσεων, αναλύοντας την έκθεσή τους σε σοβαρές διαταραχές της επιχειρηματικής δραστηριότητάς τους και αξιολογώντας τις πιθανές επιπτώσεις τους (μεταξύ άλλων όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα), βάσει ποσοτικών και ποιοτικών κριτηρίων, χρησιμοποιώντας εσωτερικά και/ή εξωτερικά δεδομένα (π.χ. δεδομένα τρίτου παρόχου που αφορούν επιχειρηματική διεργασία ή δημόσια διαθέσιμα δεδομένα που ενδέχεται να αφορούν την ανάλυση των επιχειρηματικών επιπτώσεων) και ανάλυση σεναρίων. Στην ανάλυση των επιχειρηματικών επιπτώσεων λαμβάνεται επίσης υπόψη η κρισιμότητα των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών, των τρίτων και των πληροφοριακών πόρων που έχουν προσδιοριστεί και κατηγοριοποιηθεί, καθώς και των αλληλεξαρτήσεών τους, σύμφωνα με την Ενότητα 3.3.

83. Τα ιδρύματα διασφαλίζουν ότι τα συστήματα ΤΠΕ και οι υπηρεσίες ΤΠΕ, σχεδιάζονται και συνάδουν με την ανάλυση των επιχειρηματικών επιπτώσεων που διενεργούν, για παράδειγμα εξασφαλίζοντας την εφεδρεία ορισμένων κρίσιμων στοιχείων για την πρόληψη δυσλειτουργιών λόγω συμβάντων που μπορεί να προκαλέσουν επιπτώσεις στα εν λόγω στοιχεία.

7.2 Σχεδιασμός επιχειρησιακής συνέχειας

84. Βάσει των οικείων αναλύσεων των επιχειρηματικών επιπτώσεων, τα ιδρύματα καταρτίζουν σχέδια για τη διασφάλιση της επιχειρησιακής συνέχειας (σχέδια επιχειρησιακής συνέχειας, ΣΕΣ), τα οποία τεκμηριώνονται και στη συνέχεια εγκρίνονται από το Διοικητικό τους Συμβούλιο. Στα σχέδια λαμβάνονται υπόψη ειδικά οι κίνδυνοι οι οποίοι θα μπορούσαν να έχουν δυσμενείς επιπτώσεις στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ. Τα σχέδια υποστηρίζουν τους στόχους για την προστασία και, εφόσον απαιτείται, την αποκατάσταση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων τους. Κατά την κατάρτιση των εν λόγω σχεδίων, τα ιδρύματα συντονίζονται με τους σχετικούς εσωτερικούς και εξωτερικούς ενδιαφερομένους, κατά περίπτωση.

85. Τα ιδρύματα θέτουν σε εφαρμογή σχέδια επιχειρησιακής συνέχειας (ΣΕΣ), ώστε να διασφαλίζεται ότι μπορούν να αντιδράσουν κατάλληλα σε πιθανά σενάρια αστοχίας και ότι είναι σε θέση να ανακτήσουν, έπειτα από διαταραχές, τις λειτουργίες των κρίσιμων επιχειρηματικών δραστηριοτήτων τους στο πλαίσιο ενός στόχου χρόνου ανάκτησης (ΣΧΑ, στόχος χρόνου ανάκαμψης: ο μέγιστος χρόνος εντός του οποίου ένα σύστημα ή μία διεργασία πρέπει να αποκατασταθεί έπειτα από κάποιο περιστατικό) και ενός στόχου σημείου ανάκτησης (ΣΣΑ, στόχος σημείου ανάκαμψης: η μέγιστη χρονική περίοδος κατά τη διάρκεια της οποίας είναι αποδεκτή η απώλεια δεδομένων σε περίπτωση συμβάντος ή περιστατικού). Σε περιπτώσεις σοβαρής διαταραχής της επιχειρηματικής δραστηριότητας, όπου ενεργοποιούνται συγκεκριμένα σχέδια επιχειρησιακής συνέχειας (ΣΕΣ), τα ιδρύματα ιεραρχούν κατά σειρά προτεραιότητας τις ενέργειες επιχειρησιακής συνέχειας, χρησιμοποιώντας μια προσέγγιση βάσει κινδύνου η οποία μπορεί να στηρίζεται στις αξιολογήσεις κινδύνων που διενεργούνται σύμφωνα με την Ενότητα 3.3. Στην περίπτωση των ΠΥΠ, η ενεργοποίηση των ΣΕΣ, μεταξύ άλλων, μπορεί για παράδειγμα να διευκολύνει την περαιτέρω επεξεργασία κρίσιμων συναλλαγών ενόσω συνεχίζονται οι προσπάθειες αποκατάστασης.

86. Τα ιδρύματα εξετάζουν στα σχέδια επιχειρησιακής συνέχειας πληθώρα διαφορετικών σεναρίων, συμπεριλαμβανομένων ακραίων αλλά πιθανών σεναρίων στα οποία ενδέχεται να εκτεθούν, καθώς και σεναρίων επιθέσεων στον κυβερνοχώρο, και αξιολογούν τις δυνητικές επιπτώσεις των εν λόγω σεναρίων. Με βάση τα σενάρια αυτά, τα ιδρύματα περιγράφουν τον τρόπο διασφάλισης της συνέχειας λειτουργίας των συστημάτων και των υπηρεσιών ΤΠΕ, καθώς και της ασφάλειας πληροφοριών του ιδρύματος.

7.3 Σχέδια αντιμετώπισης και ανάκαμψης

87. Βάσει των αναλύσεων των επιχειρηματικών επιπτώσεων της παραγράφου 82 και των εύλογων σεναρίων της παραγράφου 86, τα ιδρύματα καταρτίζουν σχέδια αντιμετώπισης και ανάκαμψης. Στα σχέδια αυτά προσδιορίζονται οι συνθήκες οι οποίες ενδέχεται να προκαλέσουν την άμεση ενεργοποίηση των σχεδίων, καθώς και τα μέτρα που λαμβάνονται για τη διασφάλιση της διαθεσιμότητας, της συνέχειας και της ανάκαμψης, τουλάχιστον, των κρίσιμων συστημάτων ΤΠΕ και υπηρεσιών ΤΠΕ των ιδρυμάτων. Τα σχέδια αντιμετώπισης και ανάκαμψης αποσκοπούν στην επίτευξη των στόχων ανάκαμψης των λειτουργιών των ιδρυμάτων.

88. Στα σχέδια αντιμετώπισης και ανάκαμψης λαμβάνονται υπόψη τόσο βραχυπρόθεσμες όσο και μακροπρόθεσμες επιλογές ανάκαμψης. Τα σχέδια:

α) εστιάζουν στην ανάκαμψη της λειτουργίας των κρίσιμων επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών, των πληροφοριακών πόρων, καθώς και των αλληλεξαρτήσεών τους, ώστε να αποφεύγονται δυσμενείς επιπτώσεις στη λειτουργία των ιδρυμάτων και στο χρηματοπιστωτικό σύστημα, καθώς επίσης και στα συστήματα πληρωμών και στους χρήστες υπηρεσιών πληρωμών, και στη διασφάλιση της εκτέλεσης εκκρεμών συναλλαγών πληρωμών,

β) είναι τεκμηριωμένα, τίθενται στη διάθεση των επιχειρηματικών και υποστηρικτικών μονάδων, και είναι εύκολα προσβάσιμα σε περίπτωση έκτακτης ανάγκης,

γ) επικαιροποιούνται με βάση τα διδάγματα που αντλούνται από τα περιστατικά, τις δοκιμές, τους νέους κινδύνους και τις απειλές που εντοπίζονται, καθώς και τους μεταβαλλόμενους στόχους και προτεραιότητες ανάκαμψης.

89. Στα σχέδια λαμβάνονται επίσης υπόψη εναλλακτικές επιλογές σε περίπτωση που η ανάκαμψη μπορεί

να μην είναι εφικτή σε βραχυπρόθεσμο ορίζοντα λόγω κόστους, κινδύνων, υλικοτεχνικής υποστήριξης ή απρόβλεπτων περιστάσεων.

90. Επιπλέον, στο πλαίσιο των σχεδίων αντιμετώπισης και ανάκαμψης, τα ιδρύματα εξετάζουν και εφαρμόζουν μέτρα συνέχειας για τη άμβλυνση των αστοχιών τρίτων παρόχων, που είναι καίριας σημασίας για τη συνέχεια των υπηρεσιών ΤΠΕ ενός ιδρύματος σύμφωνα με τις διατάξεις της ΠΕΕ 178/5/2.10.2020.

7.4 Δοκιμή των σχεδίων

91. Τα ιδρύματα υποβάλλουν σε δοκιμή τα σχέδια επιχειρησιακής συνέχειάς τους σε περιοδική βάση. Ειδικότερα, διασφαλίζουν ότι διενεργείται δοκιμή των ΣΕΣ των κρίσιμων επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων τους, καθώς και των αλληλεξαρτήσεών τους (συμπεριλαμβανομένων των αλληλεξαρτήσεων με τρίτους, κατά περίπτωση) τουλάχιστον σε ετήσια βάση, σύμφωνα με την παράγραφο 93.

92. Τα σχέδια επιχειρησιακής συνέχειας επικαιροποιούνται τουλάχιστον ετησίως με βάση τα αποτελέσματα των δοκιμών, τις τρέχουσες πληροφορίες σχετικά με απειλές και τα διδάγματα που αντλούνται από προηγούμενα συμβάντα. Κάθε αλλαγή στους στόχους ανάκαμψης (συμπεριλαμβανομένων των στόχων χρόνου ανάκαμψης και των στόχων σημείου ανάκαμψης) και/ή αλλαγή στις επιχειρηματικές λειτουργίες, στις υποστηρικτικές διεργασίες και στους πληροφοριακούς πόρους λαμβάνεται επίσης υπόψη, κατά περίπτωση, ως βάση για την επικαιροποίηση των σχεδίων επιχειρησιακής συνέχειας.

93. Στο πλαίσιο της δοκιμής των σχεδίων επιχειρησιακής συνέχειάς τους, τα ιδρύματα καταδεικνύουν ότι είναι σε θέση να διατηρήσουν τη βιωσιμότητα της επιχειρηματικής δραστηριότητάς τους έως ότου αποκατασταθούν οι κρίσιμες λειτουργίες. Ειδικότερα, η δοκιμή:

α) περιλαμβάνει δοκιμή επαρκούς συνόλου ακραίων αλλά εύλογων σεναρίων, μεταξύ των οποίων συγκαταλέγονται τα σενάρια που εξετάζονται για την κατάρτιση των σχεδίων επιχειρησιακής συνέχειας (καθώς και δοκιμή των υπηρεσιών που παρέχονται από τρίτους, κατά περίπτωση). Στο πλαίσιο αυτό, περιλαμβάνεται η μετάβαση των κρίσιμων επιχειρηματικών λειτουργιών, υποστηρικτικών διεργασιών και πληροφοριακών πόρων στο περιβάλλον ανάκαμψης από καταστροφή και η απόδειξη της δυνατότητας λειτουργίας τους με τον συγκεκριμένο τρόπο για επαρκώς αντιπροσωπευτικό χρονικό διάστημα, καθώς και της δυνατότητας μετέπειτα αποκατάστασης της κανονικής λειτουργίας,

β) είναι σχεδιασμένη κατά τρόπον ώστε να θέτει υπό αμφισβήτηση τις υποθέσεις στις οποίες στηρίζονται τα σχέδια επιχειρησιακής συνέχειας, συμπεριλαμβανομένων των ρυθμίσεων διακυβέρνησης και των σχεδίων επικοινωνίας σε καταστάσεις κρίσεων και

γ) περιλαμβάνει διαδικασίες για την επαλήθευση της ικανότητας του προσωπικού και των αναδόχων έργων, των συστημάτων ΤΠΕ και των υπηρεσιών ΤΠΕ να αντεπεξέρχονται επαρκώς στα σενάρια που ορίζονται στο στοιχείο α) της παρούσας παραγράφου.

94. Τα αποτελέσματα της δοκιμής τεκμηριώνονται από τους εκάστοτε υπεύθυνους και επιβεβαιώνονται από τη λειτουργία εσωτερικής επιθεώρησης, ενώ επίσης τυχόν διαπιστωθείσες ελλείψεις που προκύπτουν από τις δοκιμές αναλύονται, αντιμετωπίζονται και αναφέρονται στο Διοικητικό Συμβούλιο.

7.5 Επικοινωνία σε καταστάσεις κρίσεων

95. Σε περίπτωση διακοπής λειτουργίας, σημαντικού περιστατικού ασφάλειας ή έκτακτης ανάγκης, και κατά τη διάρκεια της εφαρμογής των σχεδίων επιχειρησιακής συνέχειας, τα ιδρύματα διασφαλίζουν την εφαρμογή αποτελεσματικών μέτρων επικοινωνίας σε καταστάσεις κρίσεων, ούτως ώστε όλοι οι σχετικοί εσωτερικοί και εξωτερικοί ενδιαφερόμενοι και ειδικότερα:

α) η Τράπεζα της Ελλάδος·

β) οι λοιπές αρμόδιες αρχές, εφόσον απαιτείται βάσει εθνικών ή ενωσιακών κανονιστικών ρυθμίσεων·

γ) οι σχετικοί πάροχοι υπηρεσιών (οντότητες ομίλου ή τρίτοι πάροχοι)

να ενημερώνονται εγκαίρως και με κατάλληλο τρόπο.

ΚΕΦΑΛΑΙΟ VIII. ΔΙΑΧΕΙΡΙΣΗ ΣΧΕΣΕΩΝ ΜΕ ΧΡΗΣΤΕΣ ΥΠΗΡΕΣΙΩΝ ΠΛΗΡΩΜΩΝ

96. Οι ΠΥΠ θεσπίζουν και εφαρμόζουν διεργασίες υποστήριξης και καθοδήγησης προς τους χρήστες υπηρεσιών πληρωμών με σκοπό την ενίσχυση της ευαισθητοποίησής τους σχετικά με τους κινδύνους ασφάλειας που συνδέονται με τις υπηρεσίες πληρωμών.

97. Η υποστήριξη και η καθοδήγηση που παρέχεται στους χρήστες υπηρεσιών πληρωμών επικαιροποιείται ανάλογα με όποιες νέες απειλές και ευπάθειες προκύπτουν, ενώ οι όποιες αλλαγές ανακοινώνονται στους χρήστες υπηρεσιών πληρωμών.

98. Όπου είναι δυνατό βάσει των λειτουργικών δυνατοτήτων των προϊόντων, οι ΠΥΠ επιτρέπουν στους χρήστες υπηρεσιών πληρωμών να απενεργοποιούν συγκεκριμένες λειτουργικές δυνατότητες από τις παρεχόμενες λειτουργίες πληρωμών.

99. Εάν, σύμφωνα με την παρ. 1 του άρθρου 68 του ν. 4537/2018, ένας ΠΥΠ έχει συμφωνήσει με τον πληρωτή την ύπαρξη ορίων δαπάνης όσον αφορά τις πράξεις πληρωμής που εκτελούνται μέσω συγκεκριμένων μέσων πληρωμών, ο ΠΥΠ παρέχει στον πληρωτή τη δυνατότητα να προσαρμόζει τα εν λόγω όρια μέχρι το ανώτατο συμφωνηθέν όριο.

100. Οι ΠΥΠ παρέχουν τη δυνατότητα στους χρήστες υπηρεσιών πληρωμών να λαμβάνουν ειδοποιήσεις σχετικά με επιτυχημένες και/ή αποτυχημένες απόπειρες εκκίνησης πράξεων πληρωμής, οι οποίες τους παρέχουν τη δυνατότητα εντοπισμού δόλιας ή κακόβουλης χρήσης του λογαριασμού τους.

101. Οι ΠΥΠ τηρούν ενήμερους τους χρήστες υπηρεσιών πληρωμών σχετικά με επικαιροποιήσεις των διαδικασιών ασφάλειας οι οποίες τους επηρεάζουν αναφορικά με την παροχή υπηρεσιών πληρωμών.

102. Οι ΠΥΠ παρέχουν στους χρήστες υπηρεσιών πληρωμών κάθε δυνατή βοήθεια σχετικά με όλες τις ερωτήσεις, τα αιτήματα για υποστήριξη και τις γνωστοποιήσεις για ανωμαλίες ή ζητήματα που αφορούν θέματα ασφάλειας σε σχέση με τις υπηρεσίες πληρωμών. Οι χρήστες υπηρεσιών πληρωμών ενημερώνονται κατάλληλα σε

σχέση με τον τρόπο που μπορούν να λαμβάνουν την εν λόγω υποστήριξη.

ΚΕΦΑΛΑΙΟ ΙΧ. ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

103. Η παρούσα Πράξη τίθεται σε ισχύ από την ημερομηνία δημοσίευσής της στην Εφημερίδα της Κυβερνήσεως.

104. Από την έναρξη ισχύος της παρούσας καταργούνται:

(α) το Παράρτημα 2 «Αρχές ασφαλούς και αποτελεσματικής λειτουργίας των συστημάτων πληροφορικής στα πλαίσια της διαχείρισης του λειτουργικού κινδύνου από τα πιστωτικά ιδρύματα» της ΠΔ/ΤΕ 2577/9.3.2006 «Πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης της οργάνωσης και των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών και χρηματοδοτικών ιδρυμάτων και σχετικές αρμοδιότητες των διοικητικών τους οργάνων» (Α’ 59),

(β) η Πράξη Εκτελεστικής Επιτροπής («ΠΕΕ») 157/4/02.04.2019 «Υιοθέτηση των κατευθυντηρίων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών σχετικά με τα μέτρα ασφάλειας για τους λειτουργικούς κινδύνους ασφάλειας που σχετίζονται με τις υπηρεσίες πληρωμών» (Β’ 1646), και κάθε υφιστάμενη αναφορά στα ανωτέρω νοείται ως αναφορά στην παρούσα Πράξη.

105. Εξουσιοδοτείται η Διεύθυνση Επιθεώρησης Εποπτευόμενων Εταιρειών της Τράπεζας της Ελλάδος να παρέχει οδηγίες και διευκρινίσεις για την εφαρμογή της παρούσας.

106. Η παρούσα να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως και να αναρτηθεί στον ιστότοπο της Τράπεζας της Ελλάδος.

Ο Πρόεδρος

ΙΩΑΝΝΗΣ ΣΤΟΥΡΝΑΡΑΣ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

Το Εθνικό Τυπογραφείο αποτελεί δημόσια υπηρεσία υπαγόμενη στην Προεδρία της Κυβέρνησης και έχει την ευθύνη τόσο για τη σύνταξη, διαχείριση, εκτύπωση και κυκλοφορία των Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ), όσο και για την κάλυψη των εκτυπωτικών - εκδοτικών αναγκών του δημοσίου και του ευρύτερου δημόσιου τομέα (ν. 3469/2006/Α΄ 131 και π.δ. 29/2018/Α΄58).

1. ΦΥΛΛΟ ΤΗΣ ΕΦΗΜΕΡΙΔΑΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ (ΦΕΚ)

• Τα **ΦΕΚ σε ηλεκτρονική μορφή** διατίθενται δωρεάν στο **www.et.gr**, την επίσημη ιστοσελίδα του Εθνικού Τυπογραφείου. Όσα ΦΕΚ δεν έχουν ψηφιοποιηθεί και καταχωριστεί στην ανωτέρω ιστοσελίδα, ψηφιοποιούνται και αποστέλλονται επίσης δωρεάν με την υποβολή αίτησης, για την οποία αρκεί η συμπλήρωση των αναγκαίων στοιχείων σε ειδική φόρμα στον ιστότοπο www.et.gr.

• Τα **ΦΕΚ σε έντυπη μορφή** διατίθενται σε μεμονωμένα φύλλα είτε απευθείας από το Τμήμα Πωλήσεων και Συνδρομητών, είτε ταχυδρομικά με την αποστολή αιτήματος παραγγελίας μέσω των ΚΕΠ, είτε με ετήσια συνδρομή μέσω του Τμήματος Πωλήσεων και Συνδρομητών. Το κόστος ενός ασπρόμαυρου ΦΕΚ από 1 έως 16 σελίδες είναι 1,00 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,20 €. Το κόστος ενός έγχρωμου ΦΕΚ από 1 έως 16 σελίδες είναι 1,50 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,30 €. Το τεύχος Α.Σ.Ε.Π. διατίθεται δωρεάν.

• **Τρόποι αποστολής κειμένων προς δημοσίευση:**

Α. Τα κείμενα προς δημοσίευση στο ΦΕΚ, από τις υπηρεσίες και τους φορείς του δημοσίου, αποστέλλονται ηλεκτρονικά στη διεύθυνση **webmaster.et@et.gr** με χρήση προηγμένης ψηφιακής υπογραφής και χρονοσήμανσης.

Β. Κατ’ εξαίρεση, όσοι πολίτες δεν διαθέτουν προηγμένη ψηφιακή υπογραφή μπορούν είτε να αποστέλλουν ταχυδρομικά, είτε να καταθέτουν με εκπρόσωπό τους κείμενα προς δημοσίευση εκτυπωμένα σε χαρτί στο Τμήμα Παραλαβής και Καταχώρισης Δημοσιευμάτων.

• Πληροφορίες, σχετικά με την αποστολή/κατάθεση εγγράφων προς δημοσίευση, την ημερήσια κυκλοφορία των Φ.Ε.Κ., με την πώληση των τευχών και με τους ισχύοντες τιμοκαταλόγους για όλες τις υπηρεσίες μας, περιλαμβάνονται στον ιστότοπο (www.et.gr). Επίσης μέσω του ιστότοπου δίδονται πληροφορίες σχετικά με την πορεία δημοσίευσης των εγγράφων, με βάση τον Κωδικό Αριθμό Δημοσιεύματος (ΚΑΔ). Πρόκειται για τον αριθμό που εκδίδει το Εθνικό Τυπογραφείο για όλα τα κείμενα που πληρούν τις προϋποθέσεις δημοσίευσης.

2. ΕΚΤΥΠΩΤΙΚΕΣ - ΕΚΔΟΤΙΚΕΣ ΑΝΑΓΚΕΣ ΤΟΥ ΔΗΜΟΣΙΟΥ

Το Εθνικό Τυπογραφείο ανταποκρινόμενο σε αιτήματα υπηρεσιών και φορέων του δημοσίου αναλαμβάνει να σχεδιάσει και να εκτυπώσει έντυπα, φυλλάδια, βιβλία, αφίσες, μπλοκ, μηχανογραφικά έντυπα, φακέλους για κάθε χρήση, κ.ά.

Επίσης σχεδιάζει ψηφιακές εκδόσεις, λογότυπα και παράγει οπτικοακουστικό υλικό.

Ταχυδρομική Διεύθυνση: Καποδιστρίου 34, τ.κ. 10432, Αθήνα	Ιστότοπος: **www.et.gr**
ΤΗΛΕΦΩΝΙΚΟ ΚΕΝΤΡΟ: 210 5279000 - fax: 210 5279054	Πληροφορίες σχετικά με την λειτουργία του ιστότοπου: **helpdesk.et@et.gr**
ΕΞΥΠΗΡΕΤΗΣΗ ΚΟΙΝΟΥ **Πωλήσεις - Συνδρομές:** (Ισόγειο, τηλ. 210 5279178 - 180) **Πληροφορίες:** (Ισόγειο, Γρ. 3 και τηλεφ. κέντρο 210 5279000) **Παραλαβή Δημ. Ύλης:** (Ισόγειο, τηλ. 210 5279167, 210 5279139)	Αποστολή ψηφιακά υπογεγραμμένων εγγράφων προς δημοσίευση στο ΦΕΚ: **webmaster.et@et.gr**
Ωράριο για το κοινό: Δευτέρα ως Παρασκευή: 8:00 - 13:30	Πληροφορίες για γενικό πρωτόκολλο και αλληλογραφία: **grammateia@et.gr**

Πείτε μας τη γνώμη σας,

για να βελτιώσουμε τις υπηρεσίες μας, συμπληρώνοντας την ειδική φόρμα στον ιστότοπό μας.

02028930507210016