ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ, ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΣΧΕΔΙΟ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ[1]

Η κατάρτιση πολιτικής ασφαλείας, σχεδίου ασφαλείας και σχεδίου ανάκαμψης από καταστροφές κρίνεται απαραίτητη για την ασφαλή επεξεργασία και προστασία των προσωπικών δεδομένων.

1. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Η Πολιτική Ασφαλείας (Security Policy) αποτελεί έγγραφο του υπευθύνου επεξεργασίας στο οποίο περιγράφονται οι στόχοι της ασφάλειας και οι αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται ώστε να επιτευχθούν αυτοί οι στόχοι. Καθορίζει τη δέσμευση της Διοίκησης και την προσέγγιση ενός οργανισμού ή μιας επιχείρησης αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων και δικτύων και την προστασία προσωπικών δεδομένων που τηρεί ο υπεύθυνος επεξεργασίας.

Στην πολιτική ασφαλείας θα πρέπει, κατ' ελάχιστο, να περιγράφονται οι βασικές αρχές προστασίας προσωπικών δεδομένων και ασφαλείας που εφαρμόζονται. Ειδικότερα, η πολιτική ασφαλείας πρέπει να θέτει τις βασικές αρχές για α) οργανωτικά μέτρα ασφαλείας αναφορικά με τους ρόλους και τις αρμοδιότητες του προσωπικού και των εξωτερικών συνεργατών-εκτελούντων την επεξεργασία, τον καθορισμό και τις αρμοδιότητες του υπευθύνου ασφαλείας, την εκπαίδευση του προσωπικού, τη διαχείριση περιστατικών ασφαλείας, καθώς και την καταστροφή των προσωπικών δεδομένων, β) τα τεχνικά μέτρα ασφάλειας αναφορικά με τη διαχείριση των χρηστών του πληροφοριακού συστήματος, την αναγνώριση και αυθεντικοποίηση των χρηστών, την ασφάλεια των επικοινωνιών, τη λειτουργία των αρχείων καταγραφής του πληροφοριακού συστήματος, την εξαγωγή αντιγράφων ασφαλείας, γ) τα μέτρα φυσικής ασφάλειας. Επίσης, στην πολιτική ασφαλείας πρέπει να προσδιορίζονται επακριβώς οι ρόλοι κάθε εμπλεκόμενου εντός της εταιρείας ή οργανισμού, οι αρμοδιότητες, οι ευθύνες και τα καθήκοντά του ως προς τις διαδικασίες που αφορούν στην ασφάλεια. Ακόμα, η πολιτική ασφαλείας πρέπει να περιγράφει και κατάλληλη διαδικασία για την αναθεώρησή της.

Στην πολιτική ασφαλείας πρέπει, κατ' ελάχιστο, να αναφέρονται τα εξής:

1. Οι βασικές αρχές ασφαλείας που οφείλει να τηρεί ο υπεύθυνος επεξεργασίας, όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων, η απόδοση ευθυνών σε περιπτώσεις λαθών και παραβάσεων, κ.λπ.

2. Τα αγαθά (αρχεία σε οποιαδήποτε μορφή ή εξοπλισμός) τα οποία πρέπει να προστατευτούν.

3. Ο σκοπός και το πεδίο εφαρμογής της πολιτικής ασφαλείας ως προς τη διαφύλαξη των αγαθών και των βασικών αρχών ασφαλείας.

4. Το οργανωτικό πλαίσιο ρόλων, αρμοδιοτήτων, καθηκόντων που αφορούν την ασφάλεια (συμπεριλαμβανομένων αυτών που άπτονται της υλοποίησης, εφαρμογής και επισκόπησης της πολιτικής ασφαλείας), την ενημέρωση του προσωπικού σχετικά με τη συμμόρφωση με αυτή και τις δέουσες ενέργειες σε περίπτωση παραβίασής της.

5. Οι επιμέρους τομείς ασφαλείας που αφορά η πολιτική και οι βασικοί κανόνες/διαδικασίες που πρέπει να ακολουθούνται σε καθέναν από τους τομείς αυτούς για την επίτευξη των στόχων που θέτει η πολιτική ασφαλείας.

[1] Πηγή: Ελληνική Αρχή Προστασίας Δεδομένων

6. Η διαδικασία εσωτερικών ελέγχων, η οποία πρέπει να λαμβάνει χώρα για την επισκόπηση της ορθής εφαρμογής της πολιτικής ασφαλείας και την αποτίμηση της αποτελεσματικότητας των μέτρων ασφαλείας.

Σε περίπτωση που η επεξεργασία προσωπικών δεδομένων γίνεται από εκτελούντες, η πολιτική ασφαλείας πρέπει να αναγράφει επακριβώς το είδος αυτής, με ταυτόχρονη αναφορά στην αντίστοιχη σύμβαση/ρήτρα που υπογράφεται μεταξύ των δύο πλευρών. Η χρονική διάρκεια της επεξεργασίας πρέπει επίσης να αναφέρεται στην πολιτική ασφαλείας.

Αν τμήμα ή ολόκληρη η επεξεργασία συντελείται αποκλειστικά σε συστήματα που βρίσκονται υπό την αποκλειστική εποπτεία του εκτελούντος την επεξεργασία, τότε αυτό πρέπει να αναγράφεται στην πολιτική ασφαλείας. Το τμήμα της πολιτικής ασφαλείας που αφορά τον εκτελούντα την επεξεργασία πρέπει επίσης να είναι κοινοποιημένο σε αυτόν. Σε αυτή την περίπτωση, το συγκεκριμένο τμήμα της πολιτικής ασφαλείας πρέπει να αναφέρει ρητά την υποχρέωση που βαρύνει τον εκτελούντα την επεξεργασία για την πλήρη υιοθέτηση και εφαρμογή της.

Οι οδηγίες και διαδικασίες που περιλαμβάνονται στην πολιτική ασφαλείας υλοποιούνται με την εφαρμογή των μέτρων προστασίας ή ασφαλείας. Η πολιτική ασφαλείας, μαζί με το σύνολο των μέτρων προστασίας, αποτελούν και το σχέδιο ασφαλείας του οργανισμού.

1.1 Χαρακτηριστικά της πολιτικής ασφαλείας

Η πολιτική ασφαλείας μπορεί να είναι είτε ενιαία, ώστε να καλύπτει όλα τα πληροφοριακά συστήματα και τις διαδικασίες που άπτονται της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, είτε να αποτελείται από τμήματα όπου το κάθε ένα να αναφέρεται σε κάποιο υπο-σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα ή επιμέρους τομέα ασφαλείας (όπως επιμέρους πολιτική για τη διαχείριση αντιγράφων ασφαλείας, για τη διαχείριση περιστατικών παραβίασης της ασφάλειας, κ.λπ). Στη δεύτερη περίπτωση, οι επιμέρους πολιτικές αποτελούν παραρτήματα της γενικότερης πολιτικής ασφαλείας και μνημονεύονται σε αυτή.

Επίσης, πρέπει να είναι απόλυτα σαφής ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της. Προς τούτο, πρέπει να είναι απαλλαγμένη από εξειδικευμένους τεχνικούς όρους και αναφορές, οι οποίοι ενδεχομένως να καθιστούν δύσκολη την εφαρμογή της και να την εξαρτούν από συγκεκριμένες τεχνολογικές επιλογές. Η πολιτική ασφαλείας δεν πρέπει να τροποποιείται συχνά. Πέραν των τακτικών αναθεωρήσεών της, δύναται να τροποποιείται στις περιπτώσεις που συμβαίνουν σημαντικές αλλαγές σε κάποιο τουλάχιστον από τα εξής: α) στην οργανωτική δομή του υπευθύνου επεξεργασίας, β) στα πληροφοριακά συστήματα, γ) στις απαιτήσεις ασφαλείας, δ) στις τεχνολογικές εξελίξεις, ε) στο είδος ή/και στην επεξεργασία των προσωπικών δεδομένων. Η πολιτική ασφαλείας μπορεί επίσης να μεταβάλλεται κατόπιν διενέργειας εσωτερικού ή εξωτερικού ελέγχου, ο οποίος καταδεικνύει μη επαρκή ή/και μη αποτελεσματικά μέτρα ως προς την ασφάλεια, ή κατόπιν περιστατικού παραβίασης της ασφάλειας. Τέλος, σημειώνεται ότι μια πολιτική ασφαλείας οφείλει να είναι γενικεύσιμη, υπό την έννοια ότι η εφαρμογή της σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα του οργανισμού να είναι δυνατή χωρίς να απαιτούνται μεγάλες τροποποιήσεις σε μικρά χρονικά διαστήματα.

Τα αναγραφόμενα στην πολιτική ασφαλείας πρέπει να είναι δεσμευτικά για όλο το προσωπικό που χειρίζεται καθ' οιονδήποτε τρόπο προσωπικά δεδομένα, ενώ επίσης πρέπει να είναι και σε συμφωνία με τη σχετική κείμενη νομοθεσία.

2. ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

Το Σχέδιο Ασφαλείας (Security Plan) είναι το έγγραφο στο οποίο περιγράφονται τα οργανωτικά και τεχνικά μέτρα, καθώς και τα μέτρα φυσικής ασφαλείας που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν για την κάλυψη των βασικών αρχών και κανόνων ασφαλείας που αναφέρονται στην πολιτική ασφαλείας, καθώς και οι απαραίτητες ενέργειες για την υλοποίησή τους. Αφορά τόσο αυτοματοποιημένα, όσο και μη αυτοματοποιημένα συστήματα διαχείρισης και επεξεργασίας δεδομένων και πρέπει να εφαρμόζεται με ακρίβεια για την προστασία των προσωπικών δεδομένων, ευαίσθητων και μη, που τηρούνται από τον υπεύθυνο επεξεργασίας. Το Σχέδιο αυτό υπόκειται σε τακτικές επισκοπήσεις και αναθεωρήσεις, δεδομένης της ραγδαίας ανάπτυξης τεχνολογικών λύσεων και της εφαρμογής τους στα πληροφοριακά συστήματα και τεχνολογικές υποδομές.

Το Σχέδιο Ασφαλείας αποτελείται από την περιγραφή του συστήματος επεξεργασίας προσωπικών δεδομένων του υπευθύνου επεξεργασίας, τα οργανωτικά, τεχνικά μέτρα ασφαλείας, καθώς και τα μέτρα φυσικής ασφάλειας που εφαρμόζονται, το πλάνο υλοποίησης μέτρων ασφαλείας και την περιγραφή των διαδικασιών συνεχούς επισκόπησης και αναθεώρησης του σχεδίου ασφαλείας.

2.1 Περιγραφή του συστήματος επεξεργασίας προσωπικών δεδομένων

Περιγράφεται η τεχνολογική υποδομή και τα πληροφοριακά συστήματα που υποστηρίζουν την επεξεργασία των προσωπικών δεδομένων.

2.2 Μέτρα Ασφαλείας

Περιγράφονται τα μέτρα ασφαλείας που εφαρμόζονται από τον οργανισμό ή την επιχείρηση. Τα μέτρα ασφαλείας μπορούν να εντάσσονται στις παρακάτω τρεις κύριες κατηγορίες:

Α. Οργανωτικά μέτρα ασφαλείας

1. Υπεύθυνος Ασφαλείας
2. Οργάνωση / Διαχείριση προσωπικού
3. Διαχείριση πληροφοριακών αγαθών
4. Εκτελούντες την επεξεργασία
5. Καταστροφή δεδομένων και αποθηκευτικών μέσων
6. Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων
7. Εκπαίδευση προσωπικού
8. Έλεγχος

Β. Τεχνικά μέτρα ασφαλείας

1. Έλεγχος πρόσβασης
2. Αντίγραφα ασφαλείας
3. Διαμόρφωση υπολογιστών
4. Αρχεία καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας
5. Ασφάλεια επικοινωνιών
6. Αποσπώμενα μέσα αποθήκευσης
7. Ασφάλεια λογισμικού
8. Διαχείριση αλλαγών

Γ. **Μέτρα φυσικής ασφαλείας**

1. Έλεγχος φυσικής πρόσβασης
2. Περιβαλλοντική ασφάλεια
3. Έκθεση εγγράφων
4. Προστασία φορητών μέσων αποθήκευσης

5. Μεταφορά φακέλων
6. Εναλλακτικές εγκαταστάσεις

Αναλυτικότερα τα μέτρα ασφαλείας κατά κατηγορία:

Α. Οργανωτικά μέτρα ασφαλείας

1. Υπεύθυνος ασφαλείας

Α) Ορισμός Υπεύθυνου Ασφαλείας
Πρέπει να οριστεί διακριτή θέση υπεύθυνου ασφαλείας (ή, ενδεχομένως, αντίστοιχης ομάδας ατόμων) εντός του οργανισμού ή της επιχείρησης με σαφώς ορισμένες αρμοδιότητες. Πρέπει ο υπεύθυνος ασφαλείας να έχει, τουλάχιστον, την επίβλεψη και τον έλεγχο της εφαρμογής της πολιτικής ασφαλείας και των μέτρων ασφαλείας.

2. Οργάνωση/Διαχείριση προσωπικού

Α) Ρόλοι/εξουσιοδοτήσεις
Πρέπει να δημιουργηθούν οργανωτικοί ρόλοι για συγκεκριμένες εργασίες εντός του οργανισμού/εταιρείας και να γίνει σύνδεση του προσωπικού με τους αντίστοιχους ρόλους. Πρέπει να υπάρχει σαφής διαχωρισμός και ανάθεση καθηκόντων/αρμοδιοτήτων σε κάθε υπάλληλο, με βάση το ρόλο του. Οι ρόλοι πρέπει να ανατίθενται επισήμως (εγγράφως). Οι υπάλληλοι πρέπει να έχουν δικαίωμα πρόσβασης μόνο στα απολύτως απαραίτητα δεδομένα προσωπικού χαρακτήρα, βάσει των αρμοδιοτήτων και καθηκόντων που τους έχουν ανατεθεί και υπαγορεύονται από το ρόλο τους (με άλλα λόγια, σε κάθε μέλος του οργανισμού ανατίθενται συγκεκριμένα δικαιώματα πρόσβασης σύμφωνα με τους ρόλους τους οποίους λαμβάνει).

Β) Αναθεώρηση ρόλων
Πρέπει να υπάρχει διαδικασία για την περιοδική επανεξέταση και αναθεώρηση των εξουσιοδοτήσεων και δικαιωμάτων πρόσβασης για όλα τα στάδια της εργασιακής πορείας των υπαλλήλων (πρόσληψη, μετακίνηση, αλλαγή καθηκόντων, αποχώρηση, κ.λπ).

Γ) Δέσμευση εμπιστευτικότητας
Ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Για το σκοπό αυτό, είναι απαραίτητη η λήψη ειδικών μέτρων για τη δέσμευση του προσωπικού που επεξεργάζεται προσωπικά δεδομένα ως προς την εμπιστευτικότητα, ιδίως όταν το εν λόγω προσωπικό δεν δεσμεύεται ήδη από απόρρητο. Η σύνταξη κωδίκων δεοντολογίας μπορεί επίσης να βοηθήσει προς την κατεύθυνση αυτή.

Δ) Αποχώρηση υπαλλήλου
Πρέπει να υπάρχει σαφής διαδικασία προσανατολισμένη στην ασφάλεια, η οποία να τηρείται κατά την αποχώρηση μέλους του προσωπικού. Μέτρα προστασίας σε αυτή την κατεύθυνση μπορούν να είναι τα ακόλουθα:
α) Κατάργηση όλων των λογαριασμών πρόσβασης, των εξουσιοδοτήσεων και των κωδικών-συνθηματικών πρόσβασης.
β) Κατάργηση των λογαριασμών ηλεκτρονικού ταχυδρομείου και μη ανάθεσή τους σε άλλον ή άλλους υπαλλήλους (μη επαναχρησιμοποίηση τους).
γ) Επιστροφή οποιουδήποτε εξοπλισμού έχει παρασχεθεί στον υπάλληλο και ανήκει στον υπεύθυνο επεξεργασίας, (συμπεριλαμβανομένων υπολογιστών, κλειδιών, ηλεκτρονικών καρτών εισόδου/εξόδου, κ.λπ).

3. Διαχείριση πληροφοριακών αγαθών

Α) Καταγραφή
Πρέπει να υπάρχουν σαφείς διαδικασίες διαχείρισης υλικού και λογισμικού που περιλαμβάνουν την τήρηση επικαιροποιημένου καταλόγου των πληροφοριακών και επικοινωνιακών υποδομών και συστημάτων, του λογισμικού καθώς και των κατηγοριών αρχείων και δεδομένων που χρησιμοποιούνται ή τηρούνται από τον υπεύθυνο επεξεργασίας, όπως επίσης και τον καθορισμό ενός ή περισσοτέρων ατόμων ή ρόλων που είναι κάτοχοι ή/και υπεύθυνοι των αντίστοιχων αγαθών.

Β) Διαχείριση φυσικού αρχείου
Πρέπει να υπάρχουν συγκεκριμένες διαδικασίες για την ορθή οργάνωση/αρχειοθέτηση/ταξινόμηση του φυσικού αρχείου (δηλ. του αρχείου με τους φυσικούς φακέλους).

Γ) Διαβάθμιση πληροφοριών
Τα δεδομένα πρέπει να διαβαθμίζονται βάσει του είδους και της κρισιμότητάς τους, καθώς επίσης και να υπάρχουν συγκεκριμένες διαδικασίες διαχείρισής τους με βάση τη διαβάθμιση αυτή.

Δ) Διακίνηση πληροφοριακών αγαθών
Σε περίπτωση που εξοπλισμός (π.χ. υπολογιστής ή USB) με προσωπικά δεδομένα μεταφέρεται εκτός των εγκαταστάσεων του υπευθύνου επεξεργασίας, η ενέργεια αυτή πρέπει να καταγράφεται (ημερομηνία και ώρα εξόδου, πρόσωπο που χρησιμοποιεί τον εξοπλισμό, επιστροφή του εξοπλισμού) και να τελεί υπό την έγκριση είτε του υπευθύνου επεξεργασίας είτε του υπευθύνου ασφαλείας.

4. Εκτελούντες την επεξεργασία

Α) Καταγραφή
Ο υπεύθυνος επεξεργασίας πρέπει να τηρεί κατάλογο όλων των εκτελούντων την επεξεργασία που χειρίζονται προσωπικά δεδομένα για λογαριασμό του εντός ή εκτός των εγκαταστάσεων του.

Β) Έγγραφη ανάθεση
Στην περίπτωση που ο υπεύθυνος επεξεργασίας αναθέτει την επεξεργασία δεδομένων σε εκτελούντα, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως και προβλέπει ότι ο εκτελών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπευθύνου και ότι οι λοιπές υποχρεώσεις ως προς την ασφάλεια βαρύνουν αναλόγως και αυτόν (τον εκτελούντα).
Οι έγγραφες αναθέσεις-συμβάσεις πρέπει να περιέχουν κατ' ελάχιστο περιγραφή των προσωπικών δεδομένων, το σκοπό, τον τόπο και τον τρόπο/διαδικασία της επεξεργασίας, καθώς και τα επίπεδα των υπηρεσιών που πρέπει να επιτυγχάνει ο εκτελών την επεξεργασία (σε επίπεδο ασφαλείας και ποιότητας δεδομένων).

Γ) Μέτρα ασφαλείας που αφορούν τους εκτελούντες
Ο εκτελών την επεξεργασία οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφαλή τήρηση και επεξεργασία των προσωπικών δεδομένων του υπεύθυνου επεξεργασίας. Ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίσει ότι ο εκτελών την επεξεργασία τηρεί τους όρους της πολιτικής ασφαλείας του (του υπευθύνου) στο μέτρο που αυτή τον αφορά (τον εκτελούντα) αναφορικά με κανόνες πρόσβασης στα συστήματα, διαχείριση περιστατικών ασφαλείας, μέτρα φυσικής ασφαλείας, κ.λπ.
Δικαιώματα πρόσβασης σε μέλη του προσωπικού του εκτελούντος στα συστήματα του υπευθύνου επεξεργασίας εκχωρούνται μόνο όταν αυτό είναι απαραίτητο για την υλοποίηση των συμβατικών τους υποχρεώσεων. Πρέπει να ανατίθενται οι ελάχιστες απαιτούμενες

εξουσιοδοτήσεις, οι οποίες με τη σειρά τους θα πρέπει να καταργούνται με τη λήξη της συμβατικής υποχρέωσης.

Δ) Τόπος επεξεργασίας
Για τη συντήρηση/αναβάθμιση του εξοπλισμού που φέρει προσωπικά δεδομένα θα πρέπει πάντοτε να εξετάζεται το ενδεχόμενο, εφόσον είναι εφικτό και πρόσφορο, αυτή να πραγματοποιείται στο χώρο του υπευθύνου επεξεργασίας.
Όταν η επεξεργασία γίνεται εκτός των εγκαταστάσεων του υπευθύνου επεξεργασίας, ο υπεύθυνος θα πρέπει να εξασφαλίζει ότι ο εκτελών παρέχει επίπεδο ασφαλείας τουλάχιστον ανάλογο με αυτό που ορίζεται στην πολιτική ασφαλείας του υπευθύνου.

Ε) Δέσμευση εμπιστευτικότητας προσωπικού του εκτελούντος
Οι υπάλληλοι του εκτελούντος που επεξεργάζονται, κατά το χρονικό διάστημα της σύμβασης, προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας πρέπει να δεσμεύονται εγγράφως με κατάλληλη δήλωση εμπιστευτικότητας.

5. Καταστροφή δεδομένων και αποθηκευτικών μέσων

Α) Διαδικασίες καταστροφής δεδομένων
Πριν από την καταστροφή εντύπων ή ηλεκτρονικών αρχείων που περιέχουν προσωπικά δεδομένα θα πρέπει να λαμβάνονται τα κατάλληλα μέτρα ώστε να διασφαλίζεται η πλήρης και μόνιμη διαγραφή των δεδομένων αυτών..
Ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει συγκεκριμένη γραπτή διαδικασία για την καταστροφή των δεδομένων, τόσο όταν πρόκειται για προγραμματισμένη μαζική καταστροφή δεδομένων, όσο και όταν πρόκειται για καταστροφή δεδομένων σε καθημερινή βάση (π.χ. με χρήση καταστροφέων εγγράφων) και να ενημερώνει σχετικά τους υπαλλήλους του.

6. Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων

Α) Καθορισμός διαδικασιών
Ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει διαδικασίες για την αναγνώριση, αναφορά και άμεση αντιμετώπιση των περιστατικών παραβίασης της ασφάλειας των προσωπικών δεδομένων στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας, όπως τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.
Στις διαδικασίες αυτές πρέπει να περιλαμβάνονται κατ' αρχάς οι ενέργειες που είναι αναγκαίες για τη διερεύνηση του εκάστοτε περιστατικού – τρόπος αναφοράς περιστατικού, προσωπικό που θα ενεργοποιηθεί, αρχεία-συστήματα που θα πρέπει να διερευνηθούν, τι θα περιλαμβάνει το αρχείο διαχείρισης περιστατικού, κ.λπ. Θα πρέπει να υπάρχει καταγραφή του κάθε συμβάντος σε σχετικό αρχείο, που θα περιλαμβάνει τη χρονική στιγμή που έλαβε χώρα, το πρόσωπο που το ανέφερε και σε ποιον το ανέφερε, εκτίμηση των συνεπειών και της κρισιμότητας του περιστατικού, διαδικασίες ανάκαμψης/διόρθωσης που ακολουθήθηκαν, καθώς και ενδεχόμενη διαδικασία ενημέρωσης των θιγομένων ατόμων (υποκειμένα των δεδομένα) ανάλογα με την έκταση του περιστατικού, κ.ο.κ.

7. Εκπαίδευση προσωπικού

Α) Βασική εκπαίδευση
Η εκπαίδευση του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων, καθώς και σε ειδικές σχετικές με ασφάλεια λειτουργίες του πληροφοριακού συστήματος (π.χ. χρήση μη προβλέψιμων κωδικών πρόσβασης και συνθηματικών, τρόπο εντοπισμού και αναφοράς των περιστατικών παραβίασης της ασφαλείας, σωστή χρήση των e-mail και των αποσπώμενων μέσων αποθήκευσης) είναι ιδιαιτέρως σημαντική για την ορθή εφαρμογή των οργανωτικών και τεχνικών μέτρων ασφαλείας. Η εκπαίδευση κατά την πρόσληψη πρέπει να περιλαμβάνει

κατ' ελάχιστο την κοινοποίηση στους εργαζόμενους της πολιτικής ασφαλείας, για την οποία πρέπει κατά το δυνατόν να διαπιστωθεί ότι είναι πλήρως κατανοητή από όλους, καθώς επίσης και των διαδικασιών διαχείρισης περιστατικών παραβίασης δεδομένων και ανάκαμψης από καταστροφές, εφόσον άπτονται των αρμοδιοτήτων τους. Σκόπιμο θα ήταν να υπάρχει εταιρικός δικτυακός τόπος (web portal) στον οποίον θα είναι αναρτημένη η περιγραφή των βασικών διαδικασιών ασφαλείας που πρέπει να γνωρίζουν τα μέλη του προσωπικού. Θα πρέπει επίσης η εκπαίδευση να συνεχίζεται και μετά την πρόσληψη, είτε σε σημαντικές αλλαγές των διαδικασιών ασφαλείας είτε κατά την εμφάνιση σημαντικών θεμάτων ασφαλείας. Επίσης, ως προς το σκοπό της εκπαίδευσης κρίνεται σκόπιμη η κατάρτιση ειδικότερων ενημερωτικών εντύπων.

Γ) Εξειδικευμένη εκπαίδευση
Πρέπει να παρέχεται στο προσωπικό που έχει αναλάβει τη διαχείριση της ασφάλειας διαρκής εξειδικευμένη εκπαίδευση σχετικά με τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών.

8. Έλεγχος

Α) Διαδικασία ελέγχων
Πρέπει να υπάρχουν διαδικασίες για την εκπόνηση προγραμματισμένων έλεγχων (είτε εσωτερικών είτε εξωτερικών, σε ετήσια βάση), όπου να αποτυπώνεται και να ελέγχεται η τήρηση των μέτρων ασφαλείας και η αποτελεσματικότητά τους. Αποτέλεσμα των ελέγχων μπορεί να είναι η τροποποίηση κάποιων μέτρων ασφαλείας ή η προσθήκη νέων. Τα πορίσματα των ελέγχων συνοδευόμενα από τις αναγκαίες τροποποιήσεις των μέτρων ασφαλείας πρέπει να υποβάλλονται στον υπεύθυνο ασφαλείας, ενώ επίσης να ενημερώνεται και ο υπεύθυνος επεξεργασίας. Ο υπεύθυνος ασφαλείας θα πρέπει να αξιοποιεί το εν λόγω πόρισμα προβαίνοντας στις αναγκαίες τροποποιήσεις των μέτρων ασφαλείας καθώς και της πολιτικής ασφαλείας.

Β. Τεχνικά μέτρα ασφαλείας

1. Έλεγχος πρόσβασης

Α) Διαχείριση λογαριασμών χρηστών
Ο υπεύθυνος επεξεργασίας πρέπει να υιοθετήσει συγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών των χρηστών, οι οποίες πρέπει να περιλαμβάνουν κατ' ελάχιστο διαδικασίες για την προσθήκη, μεταβολή ιδιοτήτων και διαγραφή λογαριασμού. Πρέπει να αποδίδεται διαφορετικός λογαριασμός πρόσβασης σε κάθε χρήστη.

Β) Μηχανισμοί ελέγχου πρόσβασης
Πρέπει να αναπτυχθούν μηχανισμοί που να μην επιτρέπουν προσβάσεις σε πόρους/εφαρμογές/αρχεία από μη εξουσιοδοτημένους χρήστες: ουσιαστικά, πρέπει να υπάρχουν κατάλληλα μέτρα που να εξασφαλίζουν την εγγυημένα ορθή ταυτοποίηση και αυθεντικοποίηση των χρηστών, ενώ ταυτοχρόνως πρέπει να γίνεται σε τεχνικό επίπεδο συγκεκριμένη εκχώρηση δικαιωμάτων/εξουσιοδοτήσεων σε κάθε χρήστη.

Γ) Διαχείριση συνθηματικών
Ο υπεύθυνος επεξεργασίας οφείλει να υιοθετήσει συγκεκριμένη πολιτική διαχείρισης των συνθηματικών των χρηστών, η οποία να περιλαμβάνει τουλάχιστον κανόνες αποδοχής για το ελάχιστο μήκος (προτεινόμενο ελάχιστο μήκος αποτελούν οι 8 χαρακτήρες) και επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του.
Τα συνθηματικά δεν πρέπει να είναι κάπου καταγεγραμμένα στην πραγματική τους μορφή (ούτε σε φυσικό ούτε σε ηλεκτρονικό αρχείο). Εάν τα συνθηματικά διατηρούνται ηλεκτρονικά στο πλαίσιο της διαδικασίας ταυτοποίησης-αυθεντικοποίησης των χρηστών,

τότε πρέπει να είναι σε μη αναγνώσιμη μορφή από την οποία δεν πρέπει να είναι εφικτή η ανάκτηση της αρχικής τους μορφής. Επίσης, οι χρήστες πρέπει να υποχρεώνονται να αλλάζουν οι ίδιοι το (προκαθορισμένο) συνθηματικό που τους ανατίθεται εξαρχής, καθώς επίσης και να υποχρεώνονται να αλλάζουν το συνθηματικό τους ανά τακτά χρονικά διαστήματα (οπωσδήποτε εντός διαστήματος μικρότερου του ενός έτους).

Δ) Μη επιτυχημένες προσπάθειες πρόσβασης
Πρέπει να υπάρχουν κατάλληλοι μηχανισμοί ώστε να απαγορεύεται η πρόσβαση σε έναν εξουσιοδοτημένο χρήστη, μετά από ένα πλήθος επαναλαμβανομένων αποτυχημένων αιτήσεων πρόσβασης (για παράδειγμα, υποβολή λανθασμένων συνθηματικών). Για έναν τέτοιο χρήστη, πρέπει να επανεξετάζεται η εξουσιοδότησή του για να έχει δικαίωμα πρόσβασης.

Ε) Αδρανοποιημένος υπολογιστής
Μέτρα πρέπει να ληφθούν προς αποφυγή περιπτώσεων όπου θα δύναται κάποιος να έχει εύκολα πρόσβαση οποιουδήποτε τύπου σε προσωπικά δεδομένα, λόγω ενός ανοιχτού υπολογιστή, ο οποίος μένει χωρίς επίβλεψη (έστω και για λίγα λεπτά). Προς αυτή την κατεύθυνση μπορούν ενδεικτικά να αναπτυχθούν διαδικασίες αυτόματης αποσύνδεσης (μετά από ένα εύλογο χρονικό διάστημα αδράνειας) ή/και ενεργοποίηση της προφύλαξης οθόνης (screen saver) του υπολογιστή – για την απενεργοποίηση της οποίας θα απαιτείται χρήση συνθηματικού.

2. Αντίγραφα ασφαλείας

Α) Τήρηση αντιγράφων ασφαλείας
Ο υπεύθυνος επεξεργασίας πρέπει να αναπτύξει συγκεκριμένη πολιτική για τη λήψη και διαχείριση των αντιγράφων ασφαλείας. Η πολιτική πρέπει να περιλαμβάνει τουλάχιστον τους κανόνες/διαδικασίες που αφορούν τα εξής: την επιλογή των κρίσιμων πόρων (εφαρμογές, λειτουργικά συστήματα, αρχεία, δεδομένα αρχείων χρηστών, κ.λπ.) που χρήζουν δημιουργίας αντιγράφων ασφαλείας, τη συχνότητα της δημιουργίας/λήψης των αντιγράφων ασφαλείας (ανά τακτά διαστήματα, σε ημερήσια ή εβδομαδιαία βάση, ανάλογα με το μέγεθος και το είδος των δεδομένων, καθώς και με το πότε αυτά μεταβάλλονται), την κατάλληλη επισήμανση[2] αυτών, την ασφαλή αποθήκευσή τους και την ορθή ανάκτηση των δεδομένων από τα αντίγραφα ασφαλείας (συμπεριλαμβανομένου του περιοδικού ελέγχου ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται). Τα παραπάνω πρέπει να εξασφαλίζουν ότι σε περίπτωση εκτάκτων περιστατικών ασφαλείας και απώλειας ή καταστροφής δεδομένων για άλλη αιτία (π.χ. αστοχία υλικού), η διαθεσιμότητα και ακεραιότητα αυτών παραμένει.

Β) Τόπος τήρησης
Κάποιο αντίγραφο ασφαλείας πρέπει να διατηρείται σε διαφορετικό χώρο/φυσική τοποθεσία από τα πρωτογενή δεδομένα, ο οποίος να διαθέτει μέτρα ασφαλείας ανάλογα με τα μέτρα που υιοθετούνται για τα πρωτογενή δεδομένα. Επίσης, να λαμβάνονται μέτρα για την ασφαλή μεταφορά του.

3. Διαμόρφωση υπολογιστών

Α) Προστασία από κακόβουλο λογισμικό
Πρέπει να υπάρχει προστασία από κακόβουλο λογισμικό όλων των υπολογιστών (τόσο των προσωπικών υπολογιστών των υπαλλήλων όσο και των διακομιστών (servers)) που τηρούν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα. Αυτό μπορεί να επιτευχθεί (πέραν της

[2] Μπορούν να επισημαίνονται η ημερομηνία λήψης των δεδομένων, το εύρος των λαμβανόμενων δεδομένων, το είδος του αντιγράφου (incremental, full), η περιοδικότητα λήψης του κάθε αντιγράφου (ημερήσιο, εβδομαδιαίο, μηνιαίο, ετήσιο) καθώς και ο αριθμός των συνολικών αντιγράφων, κ.λπ.

σωστής χρήσης αυτών από τους υπαλλήλους) με αντιβιοτικά προγράμματα (antivirus), καθώς και με χρήση προγραμμάτων τειχών ασφαλείας (firewall). Τόσο το antivirus όσο και το firewall πρέπει να διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις. Επιπλέον, στο λειτουργικό σύστημα των υπολογιστών (εφόσον είναι συνδεδεμένοι στο Διαδίκτυο) πρέπει να εγκαθίστανται ανά τακτά διαστήματα ενημερώσεις ασφαλείας.

Β) Ρυθμίσεις υπολογιστών
Δεν πρέπει να επιτρέπονται ενέργειες απλών χρηστών στους υπολογιστές οι οποίες επηρεάζουν τη συνολική τους διαμόρφωση (π.χ. απενεργοποίηση αντιβιοτικών προγραμμάτων, εγκατάσταση νέων προγραμμάτων ή αλλαγή ρυθμίσεων υπαρχόντων, κ.λπ.). Πρέπει να γίνεται περιοδικός έλεγχος του εγκατεστημένου λογισμικού για τον τυχόν εντοπισμό προγραμμάτων που έχουν εγκατασταθεί εκτός των εγκεκριμένων διαδικασιών.

Γ) Υπολογιστές-διακομιστές
Σε περίπτωση που κάποιος υπολογιστής χρησιμοποιείται σαν κεντρικός διακομιστής (server) για άλλους υπολογιστές, τότε δεν θα πρέπει να μπορεί να χρησιμοποιείται ως σταθμός εργασίας από κάποιον χρήστη.

Δ) Σύνδεση αποσπώμενων μέσων
Οι ηλεκτρονικοί υπολογιστές που χρησιμοποιούνται από τους τελικούς χρήστες δεν πρέπει να διαθέτουν δυνατότητα εξαγωγής δεδομένων με τη χρήση αποσπώμενων μέσων (π.χ. USB, CD/DVD) – εκτός αν υπάρχει έγκριση από τον Υπεύθυνο Ασφαλείας (ή άλλης μορφής έγκριση, μέσω διαδικασίας που προβλέπεται στην πολιτική ασφαλείας).

Ε) Υπολογιστές με πρόσβαση στο Διαδίκτυο
Δεν πρέπει να αποθηκεύονται δεδομένα προσωπικού χαρακτήρα σε υπολογιστές που έχουν σύνδεση με το διαδίκτυο **(**εκτός αν κάτι τέτοιο είναι απολύτως απαραίτητο στο πλαίσιο του ρόλου/αρμοδιοτήτων που έχουν ανατεθεί στο χρήστη του υπολογιστή).

4. Αρχεία καταγραφής (log files)

Α) Τήρηση και έλεγχος αρχείων καταγραφής
Στα κρίσιμα συστήματα, θα πρέπει να υπάρχουν διαδικασίες για την τήρηση και τον έλεγχο των αρχείων καταγραφής όλων των ενεργειών (log files) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων ασφαλείας. Πρέπει να διασφαλίζεται η προστασία και η ακεραιότητα των αρχείων αυτών.
Στα αρχεία αυτά δύναται να έχουν πρόσβαση ο υπεύθυνος ασφαλείας, οι διαχειριστές συστημάτων και όποια άλλα μέλη του προσωπικού είναι επιφορτισμένα με αρμοδιότητες διαχείρισης περιστατικών ασφαλείας κατόπιν έγγραφης εξουσιοδότησης.
Η πρόσβαση στα αρχεία καταγραφής πρέπει επίσης να καταγράφεται και να υπόκειται στους ίδιους περιορισμούς με τα υπόλοιπα αρχεία καταγραφής.

Β) Ειδικές ενέργειες που πρέπει να καταγράφονται
Πρέπει να ληφθεί μέριμνα ώστε στα αρχεία καταγραφής ενεργειών να τηρούνται οπωσδήποτε, κατ' ελάχιστο, τα εξής: το αναγνωριστικό του χρήστη που αιτήθηκε την προσπέλαση δεδομένων προσωπικού χαρακτήρα, η ημερομηνία και ώρα του σχετικού αιτήματος, το σύστημα μέσω του οποίου αιτήθηκε την πρόσβαση (υπολογιστής, πρόγραμμα λογισμικού, κ.λπ.), καθώς και αν τελικά προσπέλασε τα αρχεία που αιτήθηκε. Επίσης, πρέπει να καταγράφονται και τα αιτήματα εκτύπωσης αρχείων με προσωπικά δεδομένα, καθώς και οι αλλαγές σε κρίσιμα αρχεία του συστήματος ή στα δικαιώματα των χρηστών. Επίσης, πρέπει να τηρούνται στοιχεία που αφορούν τις προσπάθειες μη εξουσιοδοτημένης πρόσβασης και τις αλλαγές στην παραμετροποίηση εφαρμογών και συστημάτων, τον προκαθορισμό κρίσιμων γεγονότων (events), η καταγραφή των οποίων θα επιβλέπεται άμεσα από τον υπεύθυνο ασφαλείας και τους διαχειριστές των συστημάτων και γενικότερα κάθε ενέργεια η

οποία μπορεί να υποδηλώνει διενέργεια επίθεσης, όπως προσπάθειες καταγραφής των προσφερόμενων υπηρεσιών του συστήματος (port scanning).

Γ) Διαγραφή αρχείων καταγραφής
Δεν θα πρέπει να υφίσταται δυνατότητα διαγραφής των αρχείων καταγραφής του συστήματος από ένα μόνο άτομο. Τέτοια διαγραφή θα πρέπει να γίνεται με την παρουσία 2 τουλάχιστον ατόμων, τα οποία θα έχουν διαφορετικούς ρόλους (π.χ. υπεύθυνος ασφαλείας + διοικητικός διευθυντής).

5. Ασφάλεια επικοινωνιών

Α) Έλεγχος δικτυακών συσκευών
Πρέπει να εξασφαλίζεται επαρκής έλεγχος των συνδεόμενων στο δίκτυο συσκευών (ως προς την πρόσβαση σε αυτές αλλά και τη χρήση τους).

Β) Απομακρυσμένη πρόσβαση
Ο υπεύθυνος επεξεργασίας πρέπει να υιοθετήσει συγκεκριμένη διαδικασία για τη διαχείριση της απομακρυσμένης πρόσβασης σε συστήματα (π.χ. από εταιρείες συντήρησης) μέσω ασφαλών καναλιών με δυνατή ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση. Προς τούτο, επισημαίνεται ιδιαίτερα ότι οι τεχνολογίες απομακρυσμένης πρόσβασης (π.χ. Remote Desktop, VNC, ασύρματη σύνδεση, κ.λπ.) πρέπει να επιτρέπονται μόνο σε εξουσιοδοτημένα πρόσωπα για τα οποία είναι απόλυτα απαραίτητες στο πλαίσιο των αρμοδιοτήτων τους. Συνεπώς, η απομακρυσμένη πρόσβαση πρέπει να γίνεται υπό την εποπτεία και έλεγχο του υπευθύνου επεξεργασίας (π.χ. των διαχειριστών ή/και του υπευθύνου ασφαλείας) και να καταγράφεται.

Γ) Κανάλι επικοινωνίας
Πρέπει να εξασφαλίζεται ότι η επικοινωνία μεταξύ υπολογιστών/κόμβων γίνεται μέσω επαρκώς ασφαλούς καναλιού επικοινωνίας (π.χ. με χρήση κρυπτογράφησης ή ιδιωτικών γραμμών ελεγχόμενης φυσικής πρόσβασης).

Δ) Πρωτόκολλα δικτύου
Πρέπει να αποφεύγεται η χρήση ευπαθών ως προς την ασφάλεια πρωτοκόλλων όπως FTP, telnet (όπου δεν γίνεται κρυπτογράφηση) και, όταν υπηρεσίες τέτοιων πρωτοκόλλων είναι αναγκαίες, να γίνεται χρήση των αντίστοιχων ασφαλών (όπως, για παράδειγμα, SFTP, SSH).

Ε) Περιμετρική ασφάλεια
Πρέπει να υπάρχει διαδικασία για τον επαρκή έλεγχο των δικτυακών συνδέσεων του εσωτερικού δικτύου του υπευθύνου επεξεργασίας από και προς το διαδίκτυο ή άλλα εξωτερικά, μη έμπιστα, δίκτυα όπως μέσω του σημείου ελέγχου της περιμέτρου (firewall). Οι συνδέσεις που ενεργοποιούνται μέσω του firewall και οι υπηρεσίες που εξυπηρετούν πρέπει να εγκρίνονται από τον υπεύθυνο ασφαλείας. Πρέπει, επίσης, να τηρείται επικαιροποιημένος κατάλογος με τις εγκεκριμένες συνδέσεις από και προς το δίκτυο του υπευθύνου επεξεργασίας και τις υπηρεσίες που εξυπηρετούν.

6. Αποσπώμενα μέσα αποθήκευσης

Α) Χρήση κρυπτογράφησης
Πρέπει να υπάρχουν διαδικασίες για την αποτελεσματική κρυπτογράφηση (επιλογή σύγχρονων και ισχυρών αλγορίθμων κρυπτογράφησης, κατάλληλο μέγεθος κλειδιών και τεχνικές διαχείρισης αυτών, κ.λπ.) αρχείων με προσωπικά δεδομένα, ιδίως ευαίσθητα, που τηρούνται σε φορητά αποθηκευτικά μέσα (π.χ. USB δίσκους κ.ο.κ.), αφού για αυτές τις περιπτώσεις ο κίνδυνος διαρροής δεδομένων αυξάνεται.

7. Ασφάλεια λογισμικού

Α) Σχεδιασμός εφαρμογών
Ο σχεδιασμός των εφαρμογών που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων πρέπει να πραγματοποιείται λαμβάνοντας υπόψη τις βασικές αρχές της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας (privacy by design). Ως εκ τούτου, οι εφαρμογές πρέπει, να ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων (data minimization), καθώς και της ποιότητας των δεδομένων και να περιλαμβάνουν τη δυνατότητα της διαγραφής δεδομένων μετά το χρονικό διάστημα που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Επίσης, πρέπει να επιτρέπουν την υλοποίηση όλων των απαιτούμενων τεχνικών μηχανισμών ασφαλείας για την προστασία των δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

Β) Ασφαλής ανάπτυξη εφαρμογών
Σε περίπτωση ανάπτυξης εφαρμογών, είτε εσωτερικά στον οργανισμό είτε από εξωτερικό συνεργάτη, θα πρέπει να προβλέπεται διαδικασία ασφαλούς υλοποίησης λογισμικού, ώστε να εντοπισθούν τυχόν ευπάθειες αυτού ως προς την ασφάλεια προτού αυτό μεταβεί σε λειτουργική φάση. Στις περιπτώσεις όπου η ανάπτυξη των εφαρμογών γίνεται από εξωτερικό συνεργάτη, θα πρέπει να υπάρχουν προδιαγραφές ασφαλείας της εφαρμογής στο έγγραφο περιγραφής απαιτήσεων λογισμικού, το οποίο εμπεριέχεται στη σύμβαση με τον εκάστοτε ανάδοχο.

Γ) Προστασία αρχείων λειτουργικών συστημάτων
Τα λειτουργικά αρχεία των συστημάτων (system files), τα δεδομένα ελέγχου συστημάτων (system test data), καθώς και ο πηγαίος κώδικας (source code) των προγραμμάτων λογισμικού πρέπει να ελέγχονται και να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση.

8. Διαχείριση αλλαγών

Α) Πολιτική διαχείρισης αλλαγών
Ο υπεύθυνος επεξεργασίας πρέπει να ορίσει σαφή πολιτική διαχείρισης όλων των αλλαγών που πραγματοποιούνται στα πληροφοριακά συστήματα, η οποία να περιέχει κατ' ελάχιστον: καταγραφή των αιτημάτων αλλαγής, καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών, καθορισμό των κριτηρίων αποδοχής της αλλαγής και χρονοδιάγραμμα υλοποίησης.

Β) Περιβάλλον δοκιμών
Θα πρέπει να γίνεται δοκιμή των ενημερώσεων λογισμικού, τόσο σε επίπεδο επιμέρους εφαρμογών όσο και σε επίπεδο λειτουργικού συστήματος, σε δοκιμαστικό περιβάλλον. Προαιρετικά, ο υπεύθυνος επεξεργασίας μπορεί να εφαρμόσει κεντρική διαχείριση όλων των ενημερώσεων λογισμικού.
Η ανάπτυξη λογισμικού πρέπει να γίνεται σε δοκιμαστικό περιβάλλον, το οποίο να είναι απομονωμένο από το παραγωγικό σύστημα και επικαιροποιημένο. Κατά την ανάπτυξη ή αναβάθμιση λογισμικού και τη δοκιμή του θα πρέπει να χρησιμοποιούνται δοκιμαστικά και όχι πραγματικά δεδομένα ή δεδομένα του παραγωγικού συστήματος, εκτός εάν κάτι τέτοιο είναι απολύτως απαραίτητο και δεν υπάρχει εναλλακτική λύση. Αν είναι αναγκαίο μπορούν να χρησιμοποιηθούν πραγματικά δεδομένα σε ανωνυμοποιημένη μορφή ή διαφορετικά πρέπει να περιορίζονται στα απολύτως απαραίτητα για τους σκοπούς του ελέγχου.

Γ. Μέτρα φυσικής ασφαλείας

1. Έλεγχος φυσικής πρόσβασης

Α) Φυσική πρόσβαση σε εγκαταστάσεις και computer room
Πρέπει να υπάρχουν τα κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης στους κρίσιμους χώρους όπου βρίσκεται ο φυσικός εξοπλισμός (συμπεριλαμβανομένης τηλεπικοινωνιακής και δικτυακής καλωδίωσης) που υποστηρίζει τα πληροφοριακά συστήματα και την επεξεργασία προσωπικών δεδομένων, έτσι ώστε να επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό (για παράδειγμα, κάποιοι χώροι -όπως αυτοί που βρίσκεται δικτυακός εξοπλισμός- πρέπει να είναι μόνιμα κλειδωμένοι). Σε ορισμένες δε περιπτώσεις (αναλόγως της φύσης των δεδομένων και των υπαρχόντων κινδύνων) ενδέχεται να είναι πρόσφορο να καταγράφεται κάθε πρόσβαση σε συγκεκριμένο φυσικό χώρο.

Β) Τήρηση καταλόγου
Ο υπεύθυνος επεξεργασίας πρέπει να διατηρεί επικαιροποιημένο κατάλογο με τα δικαιώματα φυσικής πρόσβασης του προσωπικού καθώς και με το προσωπικό που διαθέτει κωδικούς, κάρτες εισόδου και κλειδιά για πρόσβαση σε κρίσιμους, ως προς την ασφάλεια, χώρους. Οι κατάλογοι αυτοί θα πρέπει να υπόκεινται σε τακτική αναθεώρηση.

2. Περιβαλλοντική ασφάλεια

Α) Προστασία από φυσικές καταστροφές
Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για την προστασία των κτιρίων, των κρίσιμων χώρων, του computer room, των γραφείων του προσωπικού, του εξοπλισμού πληροφορικής και του χώρου τήρησης φυσικού αρχείου από ζημιές που μπορούν να προκληθούν από φυσικές καταστροφές ή κακόβουλες ενέργειες, όπως πλημμύρα, υπερθέρμανση, πυρκαγιά, σεισμός, έκρηξη, διαρροή νερού, διακοπή ρεύματος, διάρρηξη/κλοπή, βανδαλισμός, κ.λπ. Ενδεικτικά μέτρα προς αυτή την κατεύθυνση είναι τα εξής: συναγερμός, πόρτες και παράθυρα ασφαλείας, πυροπροστασία, απομάκρυνση εξοπλισμού από υδροσωληνώσεις και πηγές σκόνης, ανιχνευτές υγρασίας και πλημμύρας, αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών, κ.λπ.

3. Έκθεση εγγράφων

Α) Τοποθέτηση φακέλων
Οι φάκελοι που περιέχουν προσωπικά δεδομένα (φυσικό αρχείο) πρέπει να είναι τοποθετημένοι σε φωριαμούς και να μην εκτίθενται σε κοινή θέα.

Β) Μεταφορά φακέλων
Θα πρέπει να καταγράφεται η μεταφορά των φυσικών φακέλων σε διαφορετικά γραφεία ή οργανωτικές μονάδες.

Γ) Clean desk policy
Δεν θα πρέπει να αφήνονται εκτεθειμένα, χωρίς επίβλεψη, έγγραφα και φορητά μέσα αποθήκευσης πάνω σε γραφεία.

Δ) Συσκευές αναπαραγωγής εγγράφων
Λοιπές συσκευές που δύναται να χρησιμοποιηθούν για υποκλοπή ή για την έκθεση προσωπικών δεδομένων σε κοινή θέα, όπως φωτοαντιγραφικά, συσκευές fax, εκτυπωτές, κ.λπ. θα πρέπει να προστατεύονται κατάλληλα.

4. Προστασία φορητών μέσων αποθήκευσης

Α) Ασφάλεια φορητών μέσων
Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για τη φυσική ασφάλεια και προστασία των φορητών αποθηκευτικών μέσων - όπως να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση και να είναι πάντα υπό επίβλεψη κατά τη διάρκεια της χρήσης τους.

5. Εναλλακτικές εγκαταστάσεις

Α) Προστασία εναλλακτικών εγκαταστάσεων
Τα ανωτέρω μέτρα ελέγχου φυσικής πρόσβασης και περιβαλλοντικής ασφαλείας θα πρέπει να εφαρμόζονται και στις εναλλακτικές εγκαταστάσεις και εξοπλισμό που χρησιμοποιεί ο υπεύθυνος επεξεργασίας στο πλαίσιο του σχεδίου ανάκαμψης από καταστροφές.

2.3 Πλάνο υλοποίησης των μέτρων ασφαλείας

Περιγράφονται τα κενά ασφαλείας που έχουν εντοπιστεί για καθεμία από τις κατηγορίες μέτρων ασφαλείας που αναφέρονται ανωτέρω, καθώς και τα μέτρα ασφαλείας τα οποία προτίθεται να εφαρμόσει ο οργανισμός ή η επιχείρηση για την κάλυψή τους. Επίσης αναφέρεται το χρονοδιάγραμμα υλοποίησης των νέων αυτών μέτρων ασφαλείας που πρόκειται να εφαρμοστούν. Μετά την υλοποίηση και εφαρμογή τους, το σχέδιο ασφαλείας επικαιροποιείται.

2.4 Επισκόπηση – αναθεώρηση

Πρέπει να υπάρχουν διαδικασίες για την τακτική ενημέρωση του σχεδίου ασφαλείας. Η επανεξέταση όλων των μέτρων ασφαλείας, καθώς και των λειτουργιών, αποτελεί σημαντικό βήμα προς τη θωράκιση των συστημάτων επιχειρήσεων και οργανισμών και την ενίσχυση των αμυντικών μηχανισμών τους.

3. ΣΧΕΔΙΟ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ

Το Σχέδιο Ανάκαμψης από Καταστροφές (Disaster Recovery and Contingency Plan) είναι το έγγραφο που αναφέρεται στα μέτρα προστασίας, ανάκαμψης και αποκατάστασης πληροφοριακών συστημάτων και τεχνολογικών υποδομών σε περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές, εξωτερικές επιθέσεις/εισβολές, κ.λπ.

Το σχέδιο αυτό είναι απαραίτητο για την αποτύπωση των διαδικασιών και των τεχνικών μέτρων που πρέπει να εφαρμόσει ο υπεύθυνος επεξεργασίας για την προστασία των προσωπικών δεδομένων σε περίπτωση κάποιου έκτακτου περιστατικού, όπως φυσικές καταστροφές (π.χ. σεισμός, πυρκαγιά, πλημμύρα) ή μεγάλης εμβέλειας περιστατικά ασφαλείας (π.χ. καταστροφή από ιομορφικό λογισμικό). Ως εκ τούτου, συμπληρώνει το σχέδιο ασφαλείας (ή αποτελεί μέρος του). Οι διαδικασίες αυτές θα πρέπει να προβλέπουν σενάρια διακοπής της επιχειρησιακής λειτουργίας του οργανισμού και τον τρόπο ανάκαμψης/συνέχισης αυτής. Ο υπεύθυνος επεξεργασίας θα πρέπει να διαθέτει εναλλακτικές εγκαταστάσεις και εξοπλισμό, στα πλαίσια του σχεδίου ανάκαμψης από καταστροφές, προκειμένου να διατηρήσει την επιχειρησιακή του λειτουργία σε περίπτωση καταστροφής.

Επίσης, το σχέδιο αυτό πρέπει να ελέγχεται περιοδικά προκειμένου να διαπιστώνεται η αποτελεσματικότητα των μεθόδων ανάκαμψης. Οι έλεγχοι πρέπει να καλύπτουν όλο το εύρος, τις διαδικασίες και τα δεδομένα των συστημάτων.

Στο σχέδιο ανάκαμψης από καταστροφές, πρέπει να προβλέπονται μέτρα που στοχεύουν στα ακόλουθα:

- Ελαχιστοποίηση διακοπών της κανονικής λειτουργίας
- Περιορισμός της έκτασης των ζημιών και καταστροφών και αποφυγή πιθανής κλιμάκωσης αυτών
- Δυνατότητα ομαλής υποβάθμισης
- Εγκατάσταση εναλλακτικών μέσων λειτουργίας εκ των προτέρων
- Εκπαίδευση, εξάσκηση και εξοικείωση του ανθρώπινου δυναμικού με διαδικασίες έκτακτης ανάγκης
- Δυνατότητα ταχείας και ομαλής αποκατάστασης της λειτουργίας
- Ελαχιστοποίηση των οικονομικών επιπτώσεων

Το σχέδιο αυτό πρέπει να προσδιορίζει τους πιθανούς κινδύνους και γενικότερα τα κριτήρια που καθορίζουν την κατάσταση ως έκτατη και επιβάλλουν την ενεργοποίησή του. Πρέπει να υπάρχουν σαφείς και γραπτές διαδικασίες που να θέτουν τον οργανισμό σε κατάσταση έκτακτης ανάγκης και να επιτρέπουν ανάκληση του σχεδίου.

Το σχέδιο ανάκαμψης από καταστροφές πρέπει να προσδιορίζει τις σημαντικές λειτουργίες (critical functions and systems) και τα αντίστοιχα συστήματα του οργανισμού, τη στρατηγική προστασίας τους (protection strategy) και την προτεραιότητα με την οποία θα τεθούν σε εφαρμογή οι δραστηριότητες του οργανισμού στο εναλλακτικό σύστημα. Επίσης, το σχέδιο πρέπει να περιέχει μια κατάσταση με τα μέλη του προσωπικού που θα κληθούν στην περίπτωση καταστροφής, καθώς και τα τηλέφωνα των προμηθευτών υλικού και λογισμικού, των σημαντικών συνεργατών ή πελατών, των ατόμων που βρίσκονται σε διαφορετικές εγκαταστάσεις που θα χρησιμοποιηθούν από την επιχείρηση για τη συνέχιση της λειτουργίας της. Επίσης, το σχέδιο θα πρέπει να περιέχει διαδικασίες για τον υπολογισμό της ζημιάς από την καταστροφή που συντελέστηκε. Ακόμα θα πρέπει να περιέχει έναν ρεαλιστικό χρονοπρογραμματισμό με σαφή ανάθεση καθηκόντων για την αποκατάσταση της λειτουργίας του οργανισμού.

Το σχέδιο αυτό πραγματεύεται, εκτός των άλλων, την ανάκαμψη της λειτουργίας της υπολογιστικής και επικοινωνιακής υποδομής μετά από φυσικές καταστροφές (φωτιές, πλημμύρες, σεισμούς, κ.λπ.). Για την ταχύτερη δυνατή αντιμετώπιση των έκτακτων περιστάσεων, προτείνεται η τοποθέτηση συναγερμών, οι οποίοι χρησιμοποιούνται τόσο για την ανίχνευση (επικείμενης) ζημιάς λόγω των φαινομένων αυτών, αλλά και για την ανίχνευση εισβολών στα συστήματα.

Αναφορικά με την αντιμετώπιση των έκτακτων καταστάσεων, μπορούν να χρησιμοποιηθούν ειδικές συσκευές φιλτραρίσματος, όπως είναι τα φίλτρα αέρος, που περιορίζουν τις ζημιές από τον καπνό και από άλλα βλαβερά αέρια και τα φίλτρα θορύβου, που ελαττώνουν το άκουσμα εξωτερικών θορύβων. Επίσης, για τους περιβαλλοντικούς ελέγχους υπάρχουν συσκευές ή μέθοδοι που ελέγχουν τη θερμοκρασία, την πίεση, την υγρασία και άλλους περιβαλλοντικούς παράγοντες. Παραδείγματα είναι τα κλιματιστικά, οι ελεγκτές υγρασίας και οι ιονιστές της ατμόσφαιρας.

Για την αντιμετώπιση περιστατικών πυρκαγιάς, μπορεί να τοποθετηθεί ειδικός εξοπλισμός σε ενδεικνυόμενα μέρη. Παραδείγματα αποτελούν οι πυροσβεστήρες, οι ειδικοί αφροί, ειδικά χρηματοκιβώτια για την αποθήκευση σπουδαίων εγγράφων, αντιγράφων ασφαλείας και άλλων σημαντικών αντικειμένων, και οι εγκαταστάσεις αποθήκευσης νερού, οι οποίες έχουν και δυνατότητες άντλησης. Αυτό το τελευταίο είναι πολύ σημαντικό και για την αντιμετώπιση διαρροών νερού.

Όσον αφορά τις εισβολές, για την ανίχνευση και αντιμετώπισή τους μπορούν να χρησιμοποιηθούν ειδικά συστήματα λογισμικού, τα επονομαζόμενα συστήματα ανίχνευσης εισβολών, τα οποία κάνουν χρήση διαφόρων αισθητήρων και δίνουν τακτικές αναφορές στα κέντρα ελέγχου.

Ακόμα, στο σχέδιο αυτό προβλέπεται τρόπος αντιμετώπισης των διακοπών στην παροχή ηλεκτρικού ρεύματος. Για το λόγο αυτό συνιστάται η χρήση ειδικών γεννητριών, οι οποίες παρέχουν συνεχώς ενέργεια σε ζωτικά τμήματα του εξοπλισμού. Στο σχέδιο ανάκαμψης από καταστροφές περιλαμβάνονται και τα μέτρα για τον έλεγχο της φυσικής πρόσβασης κατά τη διάρκεια της αντιμετώπισης έκτακτων περιστάσεων.

Πρέπει να επισημανθεί, ωστόσο, ότι οι κίνδυνοι αυτού του είδους ελαχιστοποιούνται, αν έχει προηγουμένως καταστρωθεί ένα προσεγμένο σχέδιο ασφαλείας. Το σχέδιο ανάκαμψης από καταστροφές, άλλωστε, έρχεται να συμπληρώσει το σχέδιο ασφάλειας.

Το σχέδιο αυτό αντιμετωπίζει τις περιπτώσεις απώλειας δεδομένων, λογισμικού και υλικού με τη δημιουργία αντιγράφων ασφαλείας, τα οποία φυλάσσονται σε άλλους προστατευόμενους χώρους (κτίρια). Αναφορικά με την αντιμετώπιση της έλλειψης διαθεσιμότητας της υποδομής, διακρίνονται κυρίως δύο τρόποι: *cold sites* (ή shells) και *hot sites*. Τα πρώτα είναι, στην ουσία, εγκαταστάσεις όπου υπάρχει παροχή ηλεκτρικής ενέργειας και κλιματισμός. Στις εγκαταστάσεις αυτές θα μπορεί να εγκαθίσταται ένα υπολογιστικό σύστημα, όμοιο ακριβώς με αυτό που λειτουργεί στα κυρίως κτίρια, το οποίο θα μπορεί να τίθεται άμεσα σε λειτουργία, κάθε φορά που κάτι τέτοιο θα κρίνεται απαραίτητο. Τα *hot sites*, από την άλλη, είναι και αυτά εγκαταστάσεις, στις οποίες όμως υπάρχει ήδη εγκατεστημένο ένα υπολογιστικό σύστημα, το οποίο είναι και ανά πάσα στιγμή έτοιμο για λειτουργία και χρήση. Το σύστημα αυτό διαθέτει περιφερειακά, τηλεπικοινωνιακές γραμμές, γεννήτριες και ακόμα και προσωπικό για να το χειριστεί άμεσα, σε περίπτωση έκτακτης ανάγκης. Για την ενεργοποίηση ενός *hot site*, αρκεί να φορτωθούν τα δεδομένα και τα αντίγραφα ασφαλείας του γενικού λογισμικού και των εφαρμογών, αντίγραφα των οποίων φυλάσσονται αποθηκευμένα, κατά κανόνα, σε διαφορετικά κτίρια από αυτά που βρίσκονται τα συστήματα κανονικής λειτουργίας του οργανισμού.