ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS
ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
SCHOOL OF INFORMATION SCIENCES & TECHNOLOGY
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
DEPARTMENT OF INFORMATICS

Εργαστήριο Ασφάλειας Πληροφοριών & Προστασίας Κρίσιμων Υποδομών

Διευθυντής: Καθηγητής Δημήτρης Α. Γκρίτζαλης

Τεχνικός Σύμβουλος Προσαρμογής του ΤΕΑΥΕΤ στο Γενικό Κανονισμό Προστασίας Δεδομένων

Φάση ΦΕ-4 | Παραδοτέο ΠΑ-8.1

Γενική Πολιτική Προστασίας Δεδομένων

T.E.A.Y.E.T.

Εργαστήριο Ασφάλειας Πληροφοριών & Προστασίας Κρίσιμων Υποδομών
Διευθυντής: Καθηγητής Δημήτρης Α. Γκρίτζαλης

Τεχνικός Σύμβουλος Προσαρμογής του ΤΕΑΥΕΤ στο Γενικό Κανονισμό Προστασίας Δεδομένων

Χρηματοδότηση:	ΤΕΑΥΕΤ	Κωδικός έργου:	ΤΕΑΥΕΤ-ΓΚΠΔ
Ημερομηνία:	15.05.2018	Αποδέκτες:	ΤΕΑΥΕΤ
Κωδικός παραδοτέου:	ΠΑ-8.1	Ενότητα εργασίας:	ΦΕ-4
Τύπος παραδοτέου:	Αναφορά Ελέγχου	Εκδοχή:	1.0

Τίτλος: **Γενική Πολιτική Προστασίας Δεδομένων**

Διευθυντής έργου: **Δημήτρης Γκρίτζαλης**, Καθηγητής Ασφάλειας στις ΤΠΕ

Συγγραφείς: **Γιώργος Στεργιόπουλος,** Διδάκτορας Ασφάλειας Κρίσιμων Υποδομών, **Θεόδωρος Ντούσκας**, Διδάκτορας Ασφάλειας Πληροφοριών, **Αργυρώ Αναγνωστοπούλου,** Ειδική Ασφάλειας στις ΤΠΕ, **Ευστράτιος Βασιλέλλης,** Ειδικός Ασφάλειας στις ΤΠΕ.

Περίληψη: Το παραδοτέο αυτό περιλαμβάνει τη Γενική Πολιτική Προστασίας Δεδομένων του Συστήματος Διαχείρισης Προστασίας Δεδομένων (ΣΔΠΔ). Ειδικότερα, περιλαμβάνει τις βασικές αρχές προστασίας δεδομένων τις οποίες πρέπει να κοινοποιήσει το ΤΕΑΥΕΤ σε όλους τους εμπλεκόμενους χρήστες (εσωτερικούς και εξωτερικούς συνεργάτες).

Διαβάθμιση: Κοινά γνωστοποιήσιμο.

Λέξεις κλειδιά: ΤΕΑΥΕΤ, Ασφάλεια Πληροφοριών, Ασφάλεια Υπολογιστών, Ασφάλεια Δικτύων, Πολιτική Προστασίας Δεδομένων, Διαδικασίες Προστασίας Δεδομένων, Μέτρα Προστασίας, Δεδομένα Προσωπικού Χαρακτήρα, Γενικός Κανονισμός Προσωπικών Δεδομένων.

Κωδικός εγγράφου: **ΤΕΑΥΕΤ-ΓΚΠΔ/ΦΕ- 4/ΠΑ-8.1/1.0/15.05.2018**

Πίνακας περιεχομένων

1 ΕΙΣΑΓΩΓΗ 4

2 ΔΗΛΩΣΗ ΓΕΝΙΚΗΣ ΠΟΛΙΤΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ 4

2.1 ΣΤΟΧΟΣ 4
2.2 ΓΕΝΙΚΗ ΠΟΛΙΤΙΚΗ 4

3 ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ 5

3.1 ΛΕΙΤΟΥΡΓΙΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ 5
3.2 ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ 5
3.3 ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ 6
3.4 ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΩΝ 6
3.5 ΠΡΟΣΤΑΣΙΑ ΕΝΑΝΤΙΑ ΣΕ ΚΑΚΟΒΟΥΛΟ ΚΑΙ ΦΟΡΗΤΟ ΚΩΔΙΚΑ 7
3.6 ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ 7
3.7 ΔΙΑΧΕΙΡΙΣΗ ΜΕΣΩΝ ΑΠΟΘΗΚΕΥΣΗΣ 7
3.8 ΠΑΡΑΚΟΛΟΥΘΗΣΗ 8
3.9 ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ 9
3.10 ΑΝΑΠΤΥΞΗ ΚΑΙ ΣΥΝΤΗΡΗΣΗ ΣΥΣΤΗΜΑΤΩΝ 9
3.11 ΕΤΗΣΙΟΣ ΈΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΩΝ 10
3.12 ΕΞΑΣΦΑΛΙΣΗ ΤΗΣ ΣΥΝΕΧΙΣΗΣ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ 10

4 ΥΠΟΔΟΜΗ ΠΣ 10

4.1 ΑΣΦΑΛΕΙΣ ΠΕΡΙΟΧΕΣ 10
4.2 ΑΣΦΑΛΕΙΑ ΕΓΓΡΑΦΩΝ ΚΑΙ ΕΞΟΠΛΙΣΜΟΥ 11
4.3 ΔΙΑΧΕΙΡΙΣΗ ΚΥΚΛΟΥ ΖΩΗΣ ΕΞΟΠΛΙΣΜΟΥ 11

5 ΠΡΟΣΒΑΣΗ ΣΤΑ ΠΣ 12

5.1 ΓΕΝΙΚΑ 12
5.2 ΈΛΕΓΧΟΣ ΠΡΟΣΠΕΛΑΣΗΣ ΣΕ ΔΙΑΚΟΜΙΣΤΕΣ ΚΑΙ ΛΟΓΙΣΜΙΚΟ 13
5.3 ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΠΡΟΣΒΑΣΗ ΠΡΟΜΗΘΕΥΤΩΝ 13

6 ΛΟΓΙΣΜΙΚΟ 14

7 ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΗ ΝΟΜΟΘΕΣΙΑ ΠΕΡΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ 14

7.1 ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ 16
7.2 ΕΝΤΟΠΙΣΜΟΣ ΚΑΙ ΑΝΤΙΔΡΑΣΗ ΣΕ ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ 17
7.3 ΑΣΦΑΛΗΣ ΑΡΧΕΙΟΘΕΤΗΣΗ ΔΕΔΟΜΕΝΩΝ 17
7.4 ΔΙΑΧΕΙΡΙΣΗ ΕΚΤΕΛΟΥΝΤΩΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ 18
7.5 ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΟΥΣ 18
7.6 ΔΙΑΣΥΝΔΕΣΗ ΑΡΧΕΙΩΝ ΜΕ ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ 19
7.7 ΦΑΚΕΛΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ 19

8 ΠΕΙΘΑΡΧΙΚΗ ΔΙΑΔΙΚΑΣΙΑ 20

1 Εισαγωγή

Το παρόν παραδοτέο αποτυπώνει την Γενική Πολιτική Προστασίας Δεδομένων του Συστήματος Διαχείρισης Προστασίας Δεδομένων (ΣΔΠΔ) του ΤΕΑΥΕΤ.

Η Γενική Πολιτική Προστασίας Δεδομένων περιλαμβάνει τις βασικές αρχές προστασίας δεδομένων τις οποίες πρέπει να επικοινωνήσει το ΤΕΑΥΕΤ σε όλους τους εμπλεκόμενους χρήστες (εσωτερικούς και εξωτερικούς συνεργάτες).

Το ΤΕΑΥΕΤ πρέπει, επίσης, να εξασφαλίζει διαρκώς τους απαραίτητους πόρους για την ορθή εφαρμογή της Γενικής Πολιτικής, από όλα τα τμήματα, συστήματα, χρήστες του ΤΕΑΥΕΤ, τις παρεχόμενες υπηρεσίες καθώς και τις συναφείς δραστηριότητες.

2 Δήλωση Γενικής Πολιτικής Προστασίας Δεδομένων

2.1 Στόχος

Στόχος της Γενικής Πολιτικής Προστασίας Δεδομένων είναι η διασφάλιση της Επιχειρησιακής Συνέχειας και η ελαχιστοποίηση του κινδύνου ζημίας, μέσω πρόληψης περιστατικών παραβίασης δεδομένων και μείωσης των δυνητικών επιπτώσεών τους στο ΤΕΑΥΕΤ.

2.2 Γενική Πολιτική

Στόχος της Γενικής Πολιτικής Προστασίας Δεδομένων είναι η προστασία των δεδομένων προσωπικού χαρακτήρα έναντι όλων των εσωτερικών, εξωτερικών, εκούσιων ή ακούσιων απειλών.

- Το ΤΕΑΥΕΤ έχει εγκρίνει την Γενική Πολιτική Προστασίας Δεδομένων και προσυπογράφει, δια του παρόντος, την πλήρη δέσμευσή για την αποτελεσματική εφαρμογή και την παροχή επαρκών πόρων για τη συνεχή βελτίωση του Συστήματος Διαχείρισης Προστασίας Δεδομένων.
- Η Γενική Πολιτική Προστασίας Δεδομένων αποσκοπεί στο να διασφαλιστούν τα εξής:
  - Συνεχής προστασία των δεδομένων από τυχόν **μη εξουσιοδοτημένη πρόσβαση**.
  - Συνεχής διασφάλιση της **Εμπιστευτικότητας** των δεδομένων του ΤΕΑΥΕΤ, των πελατών και συνεργατών.
  - Συνεχής διατήρηση της **Ακεραιότητας** των δεδομένων του ΤΕΑΥΕΤ, των πελατών και συνεργατών.
  - Συνεχής διασφάλιση της **Διαθεσιμότητα** των δεδομένων και των επιχειρησιακών διαδικασιών.
  - Διαρκής παρακολούθηση και τήρηση των **Νομοθετικών και Κανονιστικών Απαιτήσεων** του ΤΕΑΥΕΤ.
  - Το **Σχέδιο Επιχειρησιακής Συνέχειας** τηρείται και ελέγχεται για την αποτελεσματικότητά του.
  - **Συνεχής εκπαίδευση** σε θέματα Προστασίας Δεδομένων για όλους τους εργαζομένους του ΤΕΑΥΕΤ.
  - Οι (επιβεβαιωμένες ή υποτιθέμενες) **παραβιάσεις δεδομένων προσωπικού χαρακτήρα** αναφέρονται στο Υπεύθυνο Προστασίας Δεδομένων, διερευνώνται ενδελεχώς και αντιμετωπίζονται άμεσα και αποτελεσματικά.
- Έχουν αναπτυχθεί και εφαρμόζονται κατάλληλες διαδικασίες και επιμέρους πολιτικές προστασίας δεδομένων για την υποστήριξη της εν λόγω πολιτικής, περιλαμβανομένων τεχνικών και οργανωτικών μέτρων προστασίας.

- Το ΤΕΑΥΕΤ διασφαλίζει τη συνεχή συμμόρφωση με την νομοθεσία και τις απαιτήσεις του ΓΚΠΔ, μέσα από διαρκή παρακολούθηση της εφαρμογής του Συστήματος Διαχείρισης Προστασίας Δεδομένων.
- Ο Υπεύθυνος Προστασίας Δεδομένων είναι υπεύθυνος για την τήρηση της Γενικής Πολιτικής Προστασίας Δεδομένων, καθώς και για την παροχή υποστήριξης και συμβουλών κατά την εφαρμογή της.
- Όλοι οι κάτοχοι θέσεων ευθύνης του ΤΕΑΥΕΤ είναι άμεσα υπεύθυνοι για την εφαρμογή της Γενικής Πολιτικής, καθώς και για τη διασφάλιση της συμμόρφωσης του προσωπικού που εποπτεύουν.
- Η συμμόρφωση με τη Γενική Πολιτική Προστασίας Δεδομένων είναι υποχρεωτική για όλους όσους εργάζονται ή συνεργάζονται με το ΤΕΑΥΕΤ.
- Τυχόν παραβιάσεις της Γενικής Πολιτικής Προστασίας Δεδομένων, υπόκεινται σε πειθαρχικές κυρώσεις. Κάθε κύρωση εξαρτάται από τη φύση και την επίπτωση της παράβασης.

3 Διαχείριση Επικοινωνιών και Διαδικασιών

3.1 Λειτουργικές Διαδικασίες και Υποχρεώσεις

Οι λειτουργικές διαδικασίες χρησιμοποιούνται καθημερινά για την συντήρηση των Πληροφοριακών Συστημάτων (ΠΣ) και των υποδομών του ΤΕΑΥΕΤ, προκειμένου να εξασφαλιστεί η μέγιστη δυνατή αξιοποίηση των περιουσιακών του στοιχείων.

Πιθανές αλλαγές στα Πληροφοριακά Συστήματα του ΤΕΑΥΕΤ ελέγχονται με κατάλληλη διαδικασία ελέγχου των αλλαγών (Διαδικασία Διαχείρισης Αλλαγών - Change Management Procedure).

Τα περιβάλλοντα ανάπτυξης και δοκιμής λογισμικού και εφαρμογών είναι ξεχωριστά από τα ενεργά παραγωγικά περιβάλλοντα, έτσι ώστε να μειωθεί ο κίνδυνος τυχαίων αλλαγών, καθώς και η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα.

Όλες οι σημαντικές αλλαγές στη βασική υποδομή (π.χ. δίκτυο, εξυπηρετητές) πρέπει να μελετώνται για τις επιπτώσεις που ενδέχεται να επιφέρουν στην ασφάλεια των πληροφοριών και την προστασία των δεδομένων του ΤΕΑΥΕΤ.

Τα περιβάλλοντα ανάπτυξης και δοκιμής λογισμικού διαχωρίζονται με χρήση κατάλληλων ελέγχων, περιλαμβανομένων των ακόλουθων:

- Εκτέλεση λογισμικού σε διαφορετικούς υπολογιστές, διαφορετικό δικτυακό τομέα πρόσβασης (domain) και δίκτυο.
- Χρήση διαφορετικών ονομάτων χρήστη και κωδικών πρόσβασης.
- Ανάθεση καθηκόντων σε όσους έχουν πρόσβαση σε -Πληροφοριακά Συστήματα, τόσο για τον έλεγχο, όσο και για την κατηγοριοποίηση των λειτουργιών στις οποίες θα έχουν πρόσβαση.

3.2 Χρήση Ηλεκτρονικού Ταχυδρομείου

Το ηλεκτρονικό ταχυδρομείο είναι εργαλείο ζωτικής σημασίας για την επικοινωνία, τόσο εσωτερικά, όσο και με τους πελάτες και προμηθευτές. Ωστόσο, λόγω της ευελιξίας και της γενικής του διαθεσιμότητας, η χρήση του ηλεκτρονικού ταχυδρομείου εγκυμονεί μια σειρά σημαντικών κινδύνων και όλοι οι χρήστες πρέπει να παραμείνουν σε εγρήγορση και να υιοθετήσουν ορθές πρακτικές κατά την αποστολή και λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Η **Πολιτική Ηλεκτρονικού Ταχυδρομείου** θέτει τους βασικούς κανόνες ορθής χρήσης του ηλεκτρονικού ταχυδρομείου , καθώς επίσης και τις επιτρεπτές ενέργειες των εξουσιοδοτημένων χρηστών. Ισχύει για κάθε χρήση της υπηρεσίας, ανεξάρτητα από το μέσο ή την τοποθεσία πρόσβασης π.χ. μέσω κινητών συσκευών ή εκτός γραφείου.

3.3 Χρήση Διαδικτύου

Ο στόχος της **Πολιτικής Αποδεκτής Χρήσης Διαδικτύου** είναι να κατευθύνει όλους τους χρήστες των υπηρεσιών Διαδικτύου σχετικά με:

- Την αναμενόμενη πρακτική κατά την εργασία.
- Την ανάδειξη ζητημάτων που επηρεάζουν τη χρήση του διαδικτύου.
- Την περιγραφή των προτύπων που οι χρήστες πρέπει να υιοθετούν.
- Την καταγραφή των ενεργειών που πρέπει να ληφθούν για την παρακολούθηση της αποτελεσματικότητας της πολιτικής αυτής.
- Την προειδοποίηση των χρηστών για τις συνέπειες της μη ορθής χρήσης του Διαδικτύου.
- Την αποφυγή μεταφοράς δεδομένων προσωπικού χαρακτήρα, όπως αναγνωριστικά χρηστών και κωδικούς πρόσβασης, μέσω URL.

Οι υποδομές Διαδικτύου είναι διαθέσιμες για τους σκοπούς των επιχειρησιακών διαδικασιών του ΤΕΑΥΕΤ.

Αναγνωρίζεται ότι είναι αδύνατο να καθοριστούν σαφείς κανόνες που καλύπτουν όλες τις διαθέσιμες διαδικτυακές δραστηριότητες. Συνεπώς, η τήρησή τους πρέπει να ενταχθεί στο γενικότερο πνεύμα της πολιτικής, ώστε να διασφαλιστεί ότι γίνεται επαρκώς παραγωγική χρήση της εγκατάστασης.

Η πολιτική αυτή καλύπτει όλες τις υπηρεσίες διαδικτύου που παρέχονται από το ΤΕΑΥΕΤ, με σκοπό την εκτέλεση και την υποστήριξη των δραστηριοτήτων του ΤΕΑΥΕΤ.

Η πολιτική προορίζεται για τα μέλη του διοικητικού συμβουλίου, τις επιτροπές, τις υπηρεσίες, τους συνεργάτες, τους υπαλλήλους, καθώς και τα συμβεβλημένα με το ΤΕΑΥΕΤ μέρη τα οποία έχουν οριστεί ως εξουσιοδοτημένοι χρήστες του Διαδικτύου.

Η Πολιτική Αποδεκτής Χρήσης Διαδικτύου πρέπει να εφαρμόζεται κάθε φορά που χρησιμοποιείται η παρεχόμενη εγκατάσταση Διαδικτύου. Αυτό περιλαμβάνει την πρόσβαση μέσω οποιασδήποτε συσκευής, όπως επιτραπέζιοι υπολογιστές ή έξυπνα κινητά τηλέφωνα (smartphones).

3.4 Σχεδιασμός Συστημάτων

Τα συστήματα ή/και οι εγκαταστάσεις της υποδομής πληροφοριακών συστημάτων καλύπτονται από σχέδιο πρόβλεψης αναγκών (δείτε περισσότερα στη **Διαδικασία Διαχείρισης Αλλαγών**) και από διαδικασίες αντικατάστασης εξοπλισμού οι οποίες εξασφαλίζουν ότι αυξημένες απαιτήσεις ισχύος και αποθήκευσης δεδομένων μπορούν να αντιμετωπιστούν και να εκπληρωθούν εγκαίρως.

Τα τμήματα πρέπει να ενημερώνουν τον Υπεύθυνο Ασφάλειας, για θέματα ΠΣ, για τυχόν νέες απαιτήσεις ή αναβαθμίσεις, service packs ή διορθώσεις (patches) που απαιτούνται για τα υπάρχοντα συστήματα.

Τα νέα προϊόντα πρέπει να προμηθεύονται μέσω των προβλεπόμενων νόμιμων διαδικασιών.

Τα νέα πληροφοριακά συστήματα, οι αναβαθμίσεις προϊόντων και οι διορθώσεις λογισμικού πρέπει να υποβάλλονται σε κατάλληλο έλεγχο πριν την αποδοχή και διάθεσή τους στο παραγωγικό πληροφοριακό σύστημα, σύμφωνα με την **Διαδικασία Ασφαλούς Ανάπτυξης Συστημάτων**.

Τα κριτήρια επιλογής πρέπει να είναι σαφώς προσδιορισμένα, προσυμφωνημένα και τεκμηριωμένα, καθώς και να έχουν εγκριθεί από το ΤΕΑΥΕΤ.

Οι εφαρμογές τρίτων, πρέπει να ελέγχονται για πιθανά πακέτα διορθώσεων λογισμικού (service pack), καθώς και για μεμονωμένες διορθώσεις λογισμικού (patches).

Οι εκτενείς και σημαντικές αναβαθμίσεις των Πληροφοριακών Συστημάτων, πρέπει να ελέγχονται διεξοδικά σε ασφαλές περιβάλλον δοκιμών, που αποτελεί αντίγραφο του παραγωγικού συστήματος.

3.5 Προστασία ενάντια σε Κακόβουλο και Φορητό Κώδικα

Έχουν ληφθεί ενδεδειγμένα μέτρα για την προστασία όλων των πληροφοριακών συστημάτων, υποδομών και πληροφοριών ενάντια σε κακόβουλο κώδικα.

Υπάρχει αποτελεσματικό και ενημερωμένο λογισμικό προστασίας από κακόβουλο λογισμικό (anti-virus) σε όλους τους εξυπηρετητές και υπολογιστές. Προκειμένου να αποφευχθεί η εκτέλεση κακόβουλου ή/και φορητού κώδικα, έχουν τεθεί σε εφαρμογή, κατάλληλοι έλεγχοι πρόσβασης (π.χ. δικαιώματα διαχείρισης/χρήστη) για την αποτροπή της μη-εξουσιοδοτημένης εγκατάστασης λογισμικού από τους χρήστες.

Ορισμένα είδη κακόβουλου κώδικα χρησιμοποιούν τεχνολογίες (εντοπίζονται συχνά σε ιστοσελίδες και e-mail) που περιλαμβάνουν, αλλά δεν περιορίζονται, στις: ActiveX, Java, JavaScript, VBScript, Μακροεντολές, HTTPS, HTML.

Το προσωπικό του ΤΕΑΥΕΤ οφείλει να μην εισάγει κακόβουλο κώδικα στα πληροφοριακά συστήματα του Οργανισμού.

Αν υπάλληλος του ΤΕΑΥΕΤ εντοπίσει κάποιον ιό σε ΠΣ, πρέπει να ενημερώσει άμεσα τον Υπεύθυνο Ασφάλειας.

Όλοι οι εξυπηρετητές πρέπει να έχουν εγκατεστημένες τις αναβαθμίσεις και διορθώσεις λογισμικού (patches) που είναι κρίσιμες για την ασφάλεια των συστημάτων, αμέσως μόλις αυτές καταστούν διαθέσιμες και ελεγχθούν.

Οι διορθώσεις λογισμικού (patches) πρέπει να εγκαθίστανται στο λογισμικό ολόκληρου του δικτύου του ΤΕΑΥΕΤ.

Αιτήματα για την εγκατάσταση νέου λογισμικού γίνονται δεκτά μόνον εφόσον προϋπάρχει σαφής τεχνική επαλήθευσή τους.

3.6 Αντίγραφα Ασφαλείας

Λαμβάνονται τακτικά αντίγραφα ασφαλείας των βασικών επιχειρησιακών πληροφοριών προκειμένου να διασφαλιστεί ότι το ΤΕΑΥΕΤ μπορεί να ανακάμψει από μια καταστροφή, αποτυχία των ψηφιακών μέσων ή από ανθρώπινο λάθος.

Χρησιμοποιείται κατάλληλος κύκλος δημιουργίας αντιγράφων ασφαλείας, ο οποίος είναι επαρκώς τεκμηριωμένος (**Πολιτική Αντιγράφων Ασφάλειας και Ανάκτησης Δεδομένων** και **Διαδικασία Λήψης Αντιγράφων Ασφάλειας**).

Οποιοσδήποτε αποθηκεύει πληροφορίες πρέπει να διασφαλίσει ότι οι πληροφορίες αυτές αποθηκεύονται και σε αντίγραφα ασφαλείας.

Ένα πλήρες αντίγραφο ασφαλείας αποθηκεύεται σε τοποθεσία εκτός της κύριας τοποθεσίας των πληροφοριακών συστημάτων. Η τοποθεσία αυτή είναι επιλεγμένη ώστε να μην επηρεαστεί από κάποια καταστροφή που πιθανώς λάβει χώρα στο κεντρικό κτήριο.

Στην περίπτωση που η ανάγκη για διαθεσιμότητα των δεδομένων είναι υψηλή, συνίσταται η δημιουργία αντιγράφων των δεδομένων σε δεύτερη τοποθεσία.

3.7 Διαχείριση Μέσων Αποθήκευσης

Μέσα αποθήκευσης δεδομένων αποτελούν, μεταξύ άλλων, τα ακόλουθα:

- Σκληροί Δίσκοι Υπολογιστών (εσωτερικών και εξωτερικών)
- CD
- DVD
- Οπτικοί Δίσκοι
- USB sticks

- Αναγνώστες καρτών
- MP3 Players
- Ψηφιακές φωτογραφικές μηχανές
- Κασέτες αντιγράφων ασφαλείας
- Ηχητικές κασέτες (περιλαμβανομένων των μηχανημάτων υπαγόρευσης και τηλεφωνητών)

Αφαιρούμενα μέσα (π.χ. ταινίες, δίσκοι, κασέτες και εκτυπωμένα έγγραφα) πρέπει να προστατεύονται για την αποτροπή ζημιών, κλοπής ή μη εξουσιοδοτημένης πρόσβασης.

Τα μέσα αποθήκευσης που μεταφέρονται πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, κατάχρηση ή προσβολή της ακεραιότητας των δεδομένων που αποθηκεύουν.

Τα έγγραφα τεκμηρίωσης του πληροφοριακού συστήματος πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Αυτά περιλαμβάνουν έγγραφα που έχουν δημιουργηθεί από το ΤΕΑΥΕΤ ή από οποιαδήποτε άλλο χρήστη των ΠΣ (δεν περιλαμβάνουν οδηγίες (manuals) που συνοδεύουν το λογισμικό).

Υπάρχουν τεκμηριωμένες διαδικασίες που αφορούν τα αντίγραφα ασφαλείας που χρειάζεται να απομακρύνονται από τα κτίρια του ΤΕΑΥΕΤ.

Τα μέσα αποθήκευσης αντιγράφων ασφαλείας τηρούνται σε ασφαλές περιβάλλον.

Έχουν ληφθεί πρόνοιες, για να διασφαλιστεί η διαθεσιμότητα των δεδομένων, που είναι αναγκαίο να υπάρχουν διαθέσιμα πέραν της διάρκειας ζωής των μέσων, όπου αποθηκεύονται τα αντίγραφα ασφαλείας (**Διαδικασία Λήψης Αντιγράφων Ασφάλειας**).

Η Πολιτική Λήψης Αντιγράφων Ασφαλείας καθορίζει αναλυτικά το χώρο τήρησης, τον χρόνο τήρησης και το είδος αντιγράφων ασφαλείας των δεδομένων του ΤΕΑΥΕΤ για εντός και εκτός κεντρικής υποδομής (περισσότερα στην **Διαδικασία Λήψης Αντιγράφων Ασφάλειας**).

Όλα τα έγγραφα καθώς και εκείνα που περιλαμβάνουν καταλόγους υλικού και λογισμικού πρέπει να φέρουν ειδικά αναγνωριστικά προκειμένου να διαχωρίζονται οι διαφορετικές εκδόσεις εγγράφων (**Διαδικασία Ελέγχου Εγγράφων**).

3.8 Παρακολούθηση

Τα αρχεία καταγραφής και ελέγχου (audit logs) πρέπει να περιλαμβάνουν τουλάχιστον τις ακόλουθες πληροφορίες:

- Αναγνωριστικό (id) του συστήματος
- Αναγνωριστικό χρήστη
- Επιτυχής/ανεπιτυχής σύνδεση (login)
- Επιτυχής/ανεπιτυχής αποσύνδεση (logoff)
- Μη εξουσιοδοτημένη πρόσβαση της εφαρμογής
- Αλλαγές στις ρυθμίσεις του συστήματος
- Χρήση προνομιακών λογαριασμών (πχ. διαχείριση λογαριασμού, αλλαγές πολιτικής, διαμόρφωση συσκευής)

Τα αρχεία καταγραφής και ελέγχου τα οποία καταγράφουν τις εξαιρέσεις και τα λοιπά γεγονότα που σχετίζονται με την ασφάλεια, διατηρούνται για διάστημα τουλάχιστον έξι μηνών ή περισσότερο αν απαιτείται από τη νομοθεσία (περισσότερα στην **Πολιτική Καταγραφής και Παρακολούθησης Ενεργειών Χρήσης**).

Η πρόσβαση στα αρχεία καταγραφής, προστατεύεται από μη εξουσιοδοτημένη πρόσβαση.

Απαγορεύεται στους διαχειριστές του συστήματος να μπορούν να διαγράφουν ή να απενεργοποιούν τα αρχεία καταγραφής των δικών τους δραστηριοτήτων.

Όπου κρίνεται σκόπιμο, τα διαβαθμισμένα δεδομένα αποθηκεύονται χωριστά από τα μη διαβαθμισμένα.

Οι διαχειριστές των συστημάτων πρέπει να τηρούν αρχείο καταγραφής (και) των δικών τους δραστηριοτήτων.

Τα αρχεία καταγραφής και ελέγχου πρέπει να περιλαμβάνουν (περισσότερα στην **Πολιτική Καταγραφής και Παρακολούθησης Ενεργειών Χρήσης**):

- Τις χρονικές στιγμές δημιουργίας αντιγράφων ασφαλείας, μαζί με λεπτομέρειες για την αλλαγή των μέσων λήψης αντιγράφων ασφαλείας.
- Τα γεγονότα εκκίνησης και τερματισμού συστημάτων και οποίου χρήστη έχει εμπλακεί σε αυτές.
- Τα σφάλματα του συστήματος (είδος, ημερομηνία, ώρα) μαζί με τις διορθωτικές ενέργειες.

Τα αρχεία καταγραφής πρέπει να ελέγχονται τακτικά για να διασφαλιστεί ότι ακολουθούνται οι σωστές διαδικασίες.

Τα ρολόγια των υπολογιστών συγχρονίζονται, προκειμένου να εξασφαλιστεί η ακρίβεια των αρχείων ελέγχου των συστημάτων.

3.9 Διαχείριση Δικτύων

Η διαχείριση του δικτύου είναι ζωτικής σημασίας για την παροχή των προβλεπόμενων υπηρεσιών από το ΤΕΑΥΕΤ.

Οι συνδέσεις προς την υποδομή δικτύου του ΤΕΑΥΕΤ πρέπει να γίνονται με ελεγχόμενο τρόπο.

Τα ασύρματα δίκτυα εφαρμόζουν ελέγχους προστασίας των δεδομένων που διέρχονται μέσω αυτών, καθώς και αποτροπής μη εξουσιοδοτημένης πρόσβασης.

Υπάρχουν σαφείς αρμοδιότητες και διαδικασίες για απομακρυσμένη πρόσβαση σε ΠΣ του ΤΕΑΥΕΤ.

Η αρχιτεκτονική του δικτύου είναι καταγεγραμμένη και αποθηκεύεται μαζί με τις ρυθμίσεις του υλικού και του λογισμικού που συνθέτουν το δίκτυο.

Τα μέρη του δικτύου καταγράφονται σε ένα μητρώο περιουσιακών στοιχείων (Asset Inventory).

Ανά τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το χρόνο), πραγματοποιείται έλεγχος όλου του λογισμικού πάνω στο δίκτυο του ΤΕΑΥΕΤ και απενεργοποιούνται τυχόν προγράμματα και υπηρεσίες που δεν απαιτούνται.

Το ασύρματο δίκτυο του ΤΕΑΥΕΤ εφαρμόζει τεχνικές κρυπτογράφησης στα δεδομένα που διακινούνται μέσω αυτού για την αποτροπή υποκλοπής πληροφοριών. Συγκεκριμένα, χρησιμοποιείται το πρωτόκολλο ασυρμάτων δικτύων WPA-2.

3.10 Ανάπτυξη και Συντήρηση Συστημάτων

Τα δεδομένα προσωπικού χαρακτήρα που τυχόν χρησιμοποιούνται κατά την ανάπτυξη και δοκιμή λογισμικού πρέπει να προστατεύονται. Η πρόσβαση σε αυτά πρέπει να ελέγχεται σύμφωνα με το νόμο περί προστασίας δεδομένων. Όπου είναι δυνατόν, τα δεδομένα πρέπει να χρησιμοποιούνται αποπροσωποποιημένα.

Εάν κατά την ανάπτυξη ή/και δοκιμή λογισμικού του ΤΕΑΥΕΤ γίνεται επεξεργασία δεδομένων, τότε πρέπει να εφαρμόζονται συγκεκριμένα μέτρα περιλαμβανομένων, μεταξύ άλλων, των ακολούθων:

- Διαδικασία αδειοδότησης.
- Απομάκρυνση όλων των επιχειρησιακών δεδομένων από το σύστημα δοκιμής μετά τη χρήση.
- Πλήρης καταγραφή όλων των συναφών δραστηριοτήτων.
- Τυχόν προσωπικές ή εμπιστευτικές πληροφορίες πρέπει να προστατεύονται σαν να ήταν δεδομένα σε χρήση σε ενεργό, παραγωγικό πληροφοριακό σύστημα.

- Προστασία των δεδομένων και της ιδιωτικότητας, συμπεριλαμβανομένων των απαιτήσεων ασφαλείας, εκ κατασκευής και από προεπιλογή. Οι απαιτήσεις αυτές μπορούν να επηρεάσουν επιλογές που σχετίζονται με την αρχιτεκτονική (αποκεντρωμένη έναντι κεντρικής), τα χαρακτηριστικά (ταχεία ανωνυμοποίηση, ελαχιστοποίηση χρησιμοποιούμενων δεδομένων), τις τεχνολογίες (κρυπτογράφηση) κλπ. των σχεδιαζόμενων εφαρμογών ή υπηρεσιών.

3.11 Ετήσιος Έλεγχος συστημάτων

Μια φορά το χρόνο πραγματοποιείται ενδελεχής έλεγχος όλων των πληροφοριακών συστημάτων και των σχετικών εγκαταστάσεων.

Ο έλεγχος των συστημάτων πρέπει να περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα:

- Συστηματικές δοκιμές διείσδυσης (penetration test).
- Σάρωση του δικτύου, εντοπισμός και καταγραφή όλων των διευθυνσιοδοτούμενων συσκευών.
- Ανάλυση Δικτύου, περιλαμβανομένων των ευάλωτων μεταγωγέων και πυλών (switches, gateways).
- Ανάλυση των ευπαθειών, των διορθώσεων λογισμικού (patches), των ευάλωτων κωδικών πρόσβασης και των δικτυακών υπηρεσιών.
- Ανάλυση εκμετάλλευσης ευπαθειών.

3.12 Εξασφάλιση της συνέχισης των δραστηριοτήτων

Το ΤΕΑΥΕΤ οφείλει να λαμβάνει τακτικά αντίγραφα ασφαλείας προκειμένου να μειώσει τις επιδράσεις μιας ανεπιθύμητης απώλειας δεδομένων. Τα αντίγραφα ασφαλείας πρέπει να λαμβάνονται και να ελέγχονται σε τακτική βάση (δείτε περισσότερα στη **Πολιτική Αντιγράφων Ασφάλειας και Ανάκτησης Δεδομένων** και **Διαδικασία Λήψης Αντιγράφων Ασφάλειας**). Επίσης, ο οργανισμός πρέπει να διαθέτει Σχέδιο Επιχειρησιακής Συνέχειας που να προβλέπει ενδεχόμενα περιστατικά, όπως αστοχία υλικού.

Ως προς τη διαχείριση επιχειρησιακής συνέχειας, το ΤΕΑΥΕΤ οφείλει:

(α) Να δημιουργήσει Σχέδιο Επιχειρησιακής Συνέχειας δραστηριοτήτων, το οποίο θα περιλαμβάνει κατάλογο με τους εμπλεκόμενους χρήστες.
(β) Να διασφαλίσει ότι σε περίπτωση περιστατικού ασφάλειας ή παραβίασης των δεδομένων οι χρήστες, οι πάροχοι υπηρεσιών, οι εξωτερικοί συνεργάτες και τα υποκείμενα των δεδομένων, γνωρίζουν σε ποιον πρέπει να απευθυνθούν.
(γ) Να πραγματοποιεί τακτικούς ελέγχους για την αποκατάσταση των αντιγράφων ασφαλείας και της εφαρμογής του Σχεδίου Επιχειρησιακής Συνέχειας.
(δ) Να χρησιμοποιεί αδιάλειπτη παροχή ρεύματος για την προστασία του εξοπλισμού που χρησιμοποιείται σε κρίσιμου τύπου επεξεργασίες.
(ε) Να διαθέτει πλεονάζουσες αποθηκευτικές μονάδες, χρησιμοποιώντας για παράδειγμα την τεχνολογία RAID.

4 Υποδομή ΠΣ

4.1 Ασφαλείς περιοχές

Η Αποτίμηση Επικινδυνότητας προσδιορίζει το κατάλληλο επίπεδο προστασίας που πρέπει να εφαρμοστεί για να εξασφαλίσει επαρκώς τα δεδομένα που αποθηκεύονται στους χώρους του ΤΕΑΥΕΤ.

Η **Πολιτική Φυσικής & Περιβαλλοντικής Ασφάλειας** καθορίζει τα μέτρα προστασίας που πρέπει να ληφθούν για τη δημιουργία ενός ασφαλούς χώρου και εξηγεί πώς πρέπει να μεριμνά κάποιος, έτσι ώστε ο χώρος αυτός να παραμένει ασφαλής.

Οι επισκέπτες που εισέρχονται στους χώρους του ΤΕΑΥΕΤ πρέπει να καταγράφονται, μαζί με την ώρα άφιξης και αναχώρησής τους και πρέπει να φέρουν διακριτικό σήμα αναγνώρισης.

Σε περίπτωση συμβάντος ασφαλείας (σύμφωνα με τη **Διαδικασία Διαχείρισης Περιστατικών**) ή αν ένα μέλος του προσωπικού αποχωρήσει από το ΤΕΑΥΕΤ, χωρίς να ακολουθήσει τις πρέπουσες διαδικασίες τερματισμού εργασίας, όλοι οι κωδικοί πρόσβασης των συστημάτων, καθώς και οι κωδικοί του συναγερμού, πρέπει να αλλάζουν άμεσα.

4.2 Ασφάλεια εγγράφων και εξοπλισμού

Τυχόν εμπιστευτικά έγγραφα αποθηκεύονται σε κλειδωμένους φωριαμούς. Πρόσβαση σε αυτούς έχουν μόνο εξουσιοδοτημένοι υπάλληλοι του ΤΕΑΥΕΤ.

Έγγραφα που τηρούνται σε γραφεία τα οποία είναι προσβάσιμα από όλο το προσωπικό ή/και από εξωτερικούς επισκέπτες, πρέπει να προστατεύονται από φυσικά μέτρα ελέγχου πρόσβασης που περιλαμβάνουν, μεταξύ άλλων, τα ακόλουθα:

- Αρχειοθήκες που είναι κλειδωμένες και τα κλειδιά αποθηκεύονται μακριά από το συρτάρι.
- Ασφαλείς περιοχές που προστατεύονται (πχ. κλειδωμένο δωμάτιο αρχείου).

Ο εξοπλισμός υπολογιστών πρέπει να βρίσκεται σε κατάλληλες φυσικές θέσεις, ώστε να:

- Περιορίζονται οι περιβαλλοντικοί κίνδυνοι (πχ. θερμότητα, φωτιά, καπνός, νερό, κραδασμοί κλπ.).
- Περιορίζεται ο κίνδυνος κλοπής.
- Εξαλειφθεί ο κίνδυνος μη εξουσιοδοτημένα άτομα να βλέπουν πληροφορίες στις οθόνες κατά την χρήση των υπολογιστών.

Τα δεδομένα του ΤΕΑΥΕΤ τα οποία αποθηκεύονται σε ηλεκτρονική μορφή, αποθηκεύονται στους κεντρικούς διακομιστές αρχείων (file servers) του ΤΕΑΥΕΤ και όχι στους τοπικούς υπολογιστές των υπαλλήλων.

Τα κρίσιμα συστήματα του ΤΕΑΥΕΤ προστατεύονται με συσκευές αδιάλειπτης παροχής ηλεκτρικού ρεύματος (UPS), ώστε να μειωθεί ο κίνδυνος καταστροφής από διακοπές ρεύματος.

Υπάρχουν διαδικασίες που διασφαλίζουν ότι οι κατάλογοι του εξοπλισμού ενημερώνονται αμέσως μόλις περιουσιακά στοιχεία προστίθενται ή απομακρύνονται από το ΤΕΑΥΕΤ (περισσότερα στη **Διαδικασία Πρόσβασης Χρηστών**).

Τα καλώδια δικτύου που υποστηρίζουν το ΠΣ του ΤΕΑΥΕΤ πρέπει να προστατεύονται από υποκλοπή δεδομένων ή βλάβη (πχ. να μην είναι εκτεθειμένα).

Τα καλώδια τροφοδοσίας πρέπει να διαχωρίζονται από τα καλώδια του δικτύου για την αποφυγή παρεμβολών. Όπου είναι δυνατόν, οι διαδρομές τους πρέπει να αποφεύγουν κοινόχρηστους χώρους.

4.3 Διαχείριση κύκλου ζωής εξοπλισμού

Το ΤΕΑΥΕΤ και οι προμηθευτές του πρέπει να διασφαλίζουν ότι ο εξοπλισμός των πληροφοριακών συστημάτων συντηρείται σύμφωνα με τις οδηγίες του κατασκευαστή και σύμφωνα με τεκμηριωμένες εσωτερικές διαδικασίες, έτσι ώστε να εξασφαλίζεται ότι παραμένει σε άρτια κατάσταση.

Το προσωπικό που ασχολείται με τη συντήρηση εξοπλισμού πρέπει να:

- Τηρεί όλα τα αντίγραφα των οδηγιών του κατασκευαστή.
- Προσδιορίζει συνιστώμενα διαστήματα συντήρησης, μαζί με τις σχετικές προδιαγραφές.
- Ενημερώνει τους αρμόδιους σε περίπτωση βλάβης.
- Επιβεβαιώνει ότι μόνο εξουσιοδοτημένοι τεχνικοί εκτελούν εργασίες στον εξοπλισμό.
- Καταγράφει λεπτομερώς τις εργασίες επιδιόρθωσης.
- Προσδιορίζει τυχόν απαιτήσεις ασφάλισης του εξοπλισμού.
- Καταγράφει τις αστοχίες που προκύπτουν και τις ενέργειες που λήφθηκαν.

Τηρείται ιστορικό συντήρησης του εξοπλισμού, έτσι ώστε όταν ο εξοπλισμός αρχίσει να φθείρεται, να μπορούν να ληφθούν αποφάσεις σχετικά με τον κατάλληλο χρόνο που πρέπει να αντικατασταθεί.

Η συντήρηση του εξοπλισμού πρέπει να εκτελείται σύμφωνα με τις οδηγίες του κατασκευαστή (**Πολιτική Προμήθειας - Εγκατάστασης Νέου Συστήματος / Νέας Εφαρμογής**). Τέτοιες ενέργειες τεκμηριώνονται και διατίθενται στο προσωπικό υποστήριξης.

Η χρήση του εξοπλισμού εκτός του χώρου του ΤΕΑΥΕΤ πρέπει να εγκριθεί από τον προϊστάμενο κάθε χρήστη. Ο εξοπλισμός που πρόκειται να επαναχρησιμοποιηθεί ή να απομακρυνθεί πρέπει να έχει όλα τα δεδομένα και το λογισμικό του επαρκώς διαγραμμένα/κατεστραμμένα.

Αν ο εξοπλισμός πρόκειται να μεταφερθεί σε άλλον οργανισμό (πχ. επιστροφή στο πλαίσιο μιας συμφωνίας leasing), τότε η απομάκρυνση των δεδομένων πρέπει να γίνει με χρήση ειδικών εργαλείων λογισμικού για διαγραφή δεδομένων.

Προκειμένου να επιβεβαιωθεί η ορθότητα των διαδικασιών παράδοσης/παραλαβής εξοπλισμού και να αποτραπεί τυχόν απώλεια ή κλοπή αποθηκευμένου εξοπλισμού, εφαρμόζονται τα ακόλουθα (περισσότερα στην **Πολιτική Προμήθειας - Εγκατάστασης Νέου Συστήματος / Νέας Εφαρμογής)**:

- Οι παραδόσεις εξοπλισμού πρέπει να υπογράφονται από εξουσιοδοτημένο άτομο που ακολουθεί σχετική διαδικασία. Η διαδικασία αυτή επιβεβαιώνει ότι τα αντικείμενα αντιστοιχούν πλήρως στη λίστα του δελτίου παράδοσης.
- Οι περιοχές φόρτωσης και οι εγκαταστάσεις αποθήκευσης πρέπει να ασφαλίζονται επαρκώς απέναντι σε μη εξουσιοδοτημένη πρόσβαση, ενώ κάθε πρόσβαση πρέπει να ελέγχεται.
- Η απομάκρυνση αποθηκευμένου εξοπλισμού πρέπει να γίνεται μέσω κατάλληλης διαδικασίας.

5 Πρόσβαση στα ΠΣ

5.1 Γενικά

Οι κωδικοί πρόσβασης των χρηστών στα ΠΣ του ΤΕΑΥΕΤ αλλάζουν τακτικά, σύμφωνα με την αντίστοιχη πολιτική (**Πολιτική Ελέγχου Πρόσβασης**), ή κάθε φορά που ένα λογισμικό υπολογιστή ζητά ρητά από έναν χρήστη να πραγματοποιήσει αλλαγή συνθηματικού.

Η πρόσβαση στα πληροφοριακά συστήματα του ΤΕΑΥΕΤ προστατεύεται μέσω των ακόλουθων μέτρων ασφαλείας (ο κατάλογος δεν είναι πλήρης):

- Κάθε χρήστης έχει το προσωπικό του χρηστώνυμο (username) και κωδικό πρόσβασης. Απαγορεύεται η χρήση κοινών λογαριασμών από πολλαπλούς χρήστες.
- Η διαδικασία ανάκτησης των κωδικών πρόσβασης προστατεύεται.
- Η πρόσβαση των χρηστών στα ΠΣ του ΤΕΑΥΕΤ παρακολουθείται και καταγράφεται.
- Κάθε χρήστης έχει συγκεκριμένους ρόλους στο ΠΣ του ΤΕΑΥΕΤ που του παρέχουν δικαιώματα πρόσβασης ανάλογα των αρμοδιοτήτων του. Δεν επιτρέπεται η ανταλλαγή κωδικών πρόσβασης μεταξύ των χρηστών.
- Εφαρμόζονται συγκεκριμένες διαδικασίες για την χρήση των κωδικών πρόσβασης των διαχειριστών. Οι διαδικασίες αυτές πρέπει να είναι ασφαλείς και ελέγξιμες.

Οι διαδικασίες ελέγχου πρόσβασης καταγράφονται, εφαρμόζονται και ενημερώνονται σε όλο το πληροφοριακό σύστημα, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση.

Οι διαδικασίες και τα μέτρα καλύπτουν όλα τα στάδια της πρόσβασης κάθε χρήστη, από την αρχική εγγραφή νέων χρηστών μέχρι την τελική διαγραφή τους.

Τα δικαιώματα πρόσβασης στα πληροφοριακά συστήματα που παρέχονται σε κάθε χρήστη:

- Είναι ανάλογα με τα καθήκοντα που αναμένεται να εκτελέσει.
- Χρησιμοποιούν ένα μοναδικό χρηστώνυμο (username) που δεν αποκαλύπτεται σε άλλο χρήστη.
- Έχουν ένα μοναδικό κωδικό πρόσβασης που ζητείται σε κάθε νέα σύνδεση.

Τα δικαιώματα πρόσβασης των χρηστών επανεξετάζονται σε τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το χρόνο) για να εξασφαλιστεί ότι παρέχονται κατάλληλα δικαιώματα βάσει των καθηκόντων του κάθε χρήστη.

Οι λογαριασμοί διαχείρισης του συστήματος παρέχονται μόνο σε χρήστες οι οποίοι έχουν άδεια να εκτελούν καθήκοντα διαχείρισης του συστήματος.

Τα αιτήματα πρόσβασης στα πληροφοριακά συστήματα του ΤΕΑΥΕΤ πρέπει να υποβάλλονται πρώτα στον Υπεύθυνο Ασφάλειας, σύμφωνα με την **Διαδικασία Πρόσβασης Χρηστών (Access Control Procedure)**.

Οι αιτήσεις πρόσβασης πρέπει να υποβάλλονται, μόνο, εφόσον έχει δοθεί έγκριση από τον προϊστάμενο του χρήστη.

Όταν ένας εργαζόμενος αποχωρεί από το ΤΕΑΥΕΤ, η πρόσβασή του στα πληροφοριακά συστήματα πρέπει να αναστέλλεται με το πέρας των εργασιών της τελευταίας εργάσιμης ημέρας του. Είναι ευθύνη του Υπεύθυνου Ανθρώπινου Δυναμικού να ζητήσει την αναστολή των δικαιωμάτων πρόσβασης μέσω του Υπεύθυνου Ασφάλειας.

5.2 Έλεγχος προσπέλασης σε διακομιστές και λογισμικό

Η πρόσβαση σε διακομιστές ελέγχεται από μια ασφαλή διαδικασία σύνδεσης.

Η πρόσβαση στα πληροφοριακά συστήματα γίνεται μέσω ενός μοναδικού ονόματος χρήστη (username) που μπορεί να συσχετισθεί με μεμονωμένο άτομο.

Η διαδικασία σύνδεσης προστατεύεται ως εξής:

- Δεν εμφανίζει καμία προηγούμενη πληροφορία σύνδεσης (πχ. όνομα χρήστη).
- Περιορίζεται ο αριθμός ανεπιτυχών προσπαθειών και κλειδώνει ο λογαριασμός σε περίπτωση υπέρβασης του αριθμού αυτού.
- Οι χαρακτήρες του κωδικού πρόσβασης αποκρύπτονται με χρήση συμβόλων.
- Εμφανίζεται προειδοποίηση ότι μόνο εξουσιοδοτημένοι χρήστες επιτρέπεται να συνδέονται στα συστήματα.

Οι διαχειριστές του συστήματος έχουν ατομικούς λογαριασμούς διαχειριστή που καταγράφονται και ελέγχονται.

Η πρόσβαση πρέπει:

- Να είναι συμβατή με τη **Διαδικασία Πρόσβασης Χρηστών (Access Control Procedure)** και την **Πολιτική Ελέγχου Πρόσβασης (Access Control Policy)**.
- Να διαχωρίζεται σε σαφώς καθορισμένους ρόλους.
- Να είναι ανάλογη (σε επίπεδο δικαιωμάτων) του ρόλου του κάθε χρήστη.
- Να ελέγχεται και τα μέτρα ελέγχου πρόσβασης να μην μπορούν να παρακαμφθούν ή να απενεργοποιηθούν από χρήστες.
- Να καταγράφεται σε μορφή που διευκολύνει τον έλεγχο, ιδιαιτέρως όταν αφορά δεδομένα προσωπικού χαρακτήρα.

5.3 Απομακρυσμένη πρόσβαση προμηθευτών

Η απομακρυσμένη πρόσβαση των προμηθευτών, στα πληροφοριακά συστήματα του ΤΕΑΥΕΤ, ελέγχεται, σύμφωνα με τη **Διαδικασία Πρόσβασης Χρηστών (Access Control Procedure)** και την **Πολιτική Ελέγχου Πρόσβασης (Access Control Policy)**.

Τυχόν αλλαγές στις συνδέσεις των προμηθευτών πρέπει να κοινοποιούνται αμέσως στον Υπεύθυνο Ασφάλειας, έτσι ώστε η πρόσβαση να μπορεί να ελεγχθεί ή να διακοπεί.

Όλα τα δικαιώματα και οι μέθοδοι πρόσβασης, ελέγχονται από τον Υπεύθυνο Ασφάλειας.

Οι συνεργάτες ή οι εξωτερικοί προμηθευτές, πρέπει να επικοινωνούν με τον Υπεύθυνο Ασφάλειας πριν από τη σύνδεσή τους στο δίκτυο του ΤΕΑΥΕΤ. Πρέπει να τηρείται αρχείο καταγραφής της δραστηριότητάς τους.

Τυχόν λογισμικό απομακρυσμένης πρόσβασης πρέπει να απενεργοποιείται όταν δεν χρησιμοποιείται.

6 Λογισμικό

Το ΤΕΑΥΕΤ χρησιμοποιεί λογισμικό προκειμένου να υποστηρίξει τις εργασίες που πραγματοποιούνται από τους υπαλλήλους. Το λογισμικό απαιτείται να διαθέτει άδεια. Το ΤΕΑΥΕΤ δεν δέχεται τη χρήση λογισμικού δίχως άδεια.

Υπάρχουν συγκεκριμένοι τρόποι απόκτησης νέου λογισμικού, ώστε να εξασφαλίζεται πάντοτε πως το ΤΕΑΥΕΤ διαθέτει πλήρη καταγραφή του λογισμικού που έχει αγοραστεί και πως μπορεί να υποστηρίζει και να αναβαθμίζει το εν λόγω λογισμικό αναλόγως. Αυτό ισχύει και για το λογισμικό που μπορεί να καταφορτώσει (download) ή/και αγοράσει από το διαδίκτυο.

Τα shareware, freeware και λοιπά λογισμικά δημόσιας ιδιοκτησίας υπόκεινται στις ίδιες πολιτικές και διαδικασίες, όπως τα υπόλοιπα λογισμικά.

Το ΤΕΑΥΕΤ προμηθεύεται λογισμικό σύμφωνα με τις νόμιμες διαδικασίες.

Το ΤΕΑΥΕΤ τηρεί μητρώο του λογισμικού που διαθέτει. Το μητρώο αυτό πρέπει να αναφέρει:

- Τίτλο και εκδότη/ιδιοκτήτη του λογισμικού.
- Ημερομηνία και πηγή απόκτησης λογισμικού.
- Θέση εγκατάστασης και σειριακό αριθμό του υλικού όπου είναι εγκατεστημένο κάθε λογισμικό.
- Τη θέση των αντιγράφων ασφαλείας.
- Το σειριακό αριθμό του προϊόντος λογισμικού.
- Μεταπωλησιακή υποστήριξη του λογισμικού.

Το λογισμικό πρέπει να εγκαθίσταται μόνον από εξουσιοδοτημένο υπάλληλο του ΤΕΑΥΕΤ, αφού πρώτα εκπληρωθούν οι απαιτήσεις εγγραφής του (registration).

Οι αλλαγές του λογισμικού πρέπει να εγκρίνονται πριν τεθούν σε εφαρμογή (σύμφωνα με τη **Διαδικασία Ασφαλούς Ανάπτυξης Συστημάτων**).

Το λογισμικό δεν πρέπει ποτέ να καταχωρείται/συνδέεται με το όνομα ή την ταυτότητα ενός χρήστη του ΤΕΑΥΕΤ.

Το λογισμικό δεν πρέπει να αλλάζει ή να τροποποιείται από κάποιον χρήστη, εκτός εάν υπάρχει σαφής επιχειρησιακή ανάγκη.

Οποιοσδήποτε χρήστης του ΤΕΑΥΕΤ αποκτά ή χρησιμοποιεί μη εξουσιοδοτημένα αντίγραφα λογισμικού, πρέπει να υφίσταται επιπτώσεις, ανάλογες με τις περιστάσεις. Το ΤΕΑΥΕΤ δεν δέχεται την παράνομη αντιγραφή λογισμικού.

7 Συμμόρφωση με τη νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα

Το ΤΕΑΥΕΤ πρέπει να τηρεί τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), καθώς και τη νομοθεσία περί προστασίας προσωπικών δεδομένων (Ν. 2472/97). Συγκεκριμένα:

- Τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται τα ΠΣ του ΤΕΑΥΕΤ πρέπει να τυγχάνουν επεξεργασίας σύμφωνα με τις απαιτήσεις του ΓΚΠΔ «για την προστασία του ατόμου από

την επεξεργασία δεδομένων προσωπικού χαρακτήρα», όπως ισχύει και ερμηνεύεται από το Ευρωπαϊκό Κοινοβούλιο, καθώς και τις Οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

- Οι κυριότερες Οδηγίες που πρέπει να ληφθούν υπόψη κατά την ανάπτυξη και διαχείριση των ΠΣ του ΤΕΑΥΕΤ και την επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι:
  - Οδηγία 115/2001 για την προστασία δεδομένων των εργαζομένων.
  - Οδηγία 1/2005 με ενδεικτικά μέτρα για την ασφάλεια κατά την καταστροφή των δεδομένων προσωπικού χαρακτήρα.
  - Οδηγία 1/2011 για τα κλειστά κυκλώματα τηλεόρασης (βιντεοεπιτήρηση).
- Ιδιαίτερη σημασία έχει ο ορισμός Υπεύθυνου Προστασίας Δεδομένων, που οφείλει να ελέγχει και να μεριμνά για την τήρηση των διατάξεων του ΓΚΠΔ και ειδικότερα:
  - Για τη συλλογή των δεδομένων προσωπικού χαρακτήρα κατά τρόπο θεμιτό και νόμιμο.
  - Για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για το/τους σκοπό/ούς που ανταποκρίνονται στο σκοπό και στις δραστηριότητες των ΠΣ του ΤΕΑΥΕΤ που έχουν γνωστοποιηθεί.
  - Για την ακρίβεια, ενημέρωση και επικαιροποίηση των δεδομένων.
  - Για την τήρηση των δεδομένων μόνο για τη χρονική διάρκεια που απαιτείται για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους.
  - Για την επιλογή για τη διεξαγωγή της επεξεργασίας προσώπων με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.
  - Για τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.
  - Για τη σύννομη ανάθεση (έγγραφος τύπος) της επεξεργασίας δεδομένων σε εκτελούντες την επεξεργασία και την εποπτεία των εκτελούντων ως προς την τήρηση του νόμου και των συμβατικών υποχρεώσεών τους.
  - Για το σεβασμό των δικαιωμάτων ενημέρωσης, πρόσβασης και αντίρρησης των υποκειμένων.
  - Για τη συνεπή και συνεχή τήρηση των διοικητικών, διαδικαστικών υποχρεώσεων που επιβάλλει ο νόμος (γνωστοποίηση, λήψη άδειας).
  - Για την επαρκή ενημέρωση και τις εν γένει τις αποφάσεις, οδηγίες και συστάσεις της ΑΠΔΠΧ, αλλά και των δικαστηρίων.
- Ο Υπεύθυνος Προστασίας Δεδομένων είναι αρμόδιος για τον κατά νόμο διαχωρισμό των δεδομένων που υφίστανται επεξεργασία σε «δεδομένα προσωπικού χαρακτήρα» και «προσωπικά δεδομένα ειδικών κατηγοριών» και την τήρηση των αντίστοιχων απαιτήσεων επεξεργασίας (ιδίως άρ. 5-11 του ΓΚΠΔ). Εν προκειμένω επισημαίνεται ότι:
  - Κάθε πληροφορία που αναφέρεται σε ένα φυσικό πρόσωπο η ταυτότητα του οποίου είναι γνωστή ή μπορεί να προσδιοριστεί (υποκείμενο των δεδομένων) θεωρείται δεδομένο προσωπικού χαρακτήρα. Δεν νοούνται ως δεδομένα προσωπικού χαρακτήρα αυτά από τα οποία δεν μπορεί πλέον να γίνει αναγωγή στην ταυτότητα του υποκειμένου των δεδομένων (πχ. ανώνυμα στατιστικά στοιχεία).
  - Προσωπικό δεδομένο ειδικής κατηγορίας θεωρείται κάθε δεδομένο που αφορά σε φυλετική προέλευση, στην εθνική καταγωγή, στα πολιτικά φρονήματα, στις θρησκευτικές πεποιθήσεις, στις φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε ένωση ή σωματείο, στα γενετικά δεδομένα, στα βιομετρικά δεδομένα, στα δεδομένα υγείας, στα στοιχεία σχετικά με τη σεξουαλική ζωή ενός φυσικού προσώπου, στο σεξουαλικό προσανατολισμό, στο ιατρικό ιστορικό, στους ιατρικούς ισχυρισμούς, στις διαγνώσεις, στις θεραπείες και στα αντίγραφα ποινικού μητρώου.
- Ιδιαίτερη μέριμνα πρέπει να λαμβάνεται για τη συμμόρφωση προς την υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων (άρ. 12-14). Σε κάθε έντυπο, όπου συμπληρώνονται προσωπικά στοιχεία, πρέπει να υπάρχει σύντομο και εύληπτο κείμενο που θα ενημερώνει το υποκείμενο για

την επεξεργασία δεδομένων και για τα δικαιώματά του σύμφωνα με το ΓΚΠΔ. Το σχετικό κείμενο πρέπει:
  - Να αναφέρει ότι τα δεδομένα τυγχάνουν επεξεργασίας σύμφωνα με το ΓΚΠΔ.
  - Να αναφέρει ότι το υποκείμενο της επεξεργασίας έχει το δικαίωμα πρόσβασης στα δεδομένα που το αφορούν.
  - Να αναφέρει τον σκοπό της συλλογής των δεδομένων.
  - Να αναφέρει το τηλέφωνο ή/και η ηλεκτρονική διεύθυνση του Υπεύθυνου Προστασίας Δεδομένων, στον οποίο το υποκείμενο μπορεί να διατυπώνει αιτήματα ή ερωτήματα.
  - Η τήρηση δεδομένων προσωπικού χαρακτήρα υπόκειται στη διαδικαστική προϋπόθεση της γνωστοποίησης στην ΑΠΔΠΧ. Γνωστοποίηση στην Αρχή Προστασίας Προσωπικών Δεδομένων απαιτείται και σε κάθε αλλαγή του σκοπού της επεξεργασίας και σε κάθε σημαντική αλλαγή του συστήματος επεξεργασίας των δεδομένων (άρ. 6) Εφόσον τηρούνται προσωπικά δεδομένα ειδικών κατηγοριών, όπως προσδιορίζονται στο Γενικό Κανονισμό και αναφέρονται παραπάνω, απαιτείται καταρχήν να ληφθεί άδεια από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (άρ. 9-10). Επισημαίνεται ότι δεν υφίσταται υποχρέωση γνωστοποίησης σε ορισμένες περιπτώσεις που ορίζονται στο άρ. 9(2). Ως προς την επεξεργασία από και στο πλαίσιο των ΠΣ του ΤΕΑΥΕΤ, ιδιαίτερης σημασίας είναι οι περιπτώσεις που η επεξεργασία συνδέεται άμεσα με σχέση εργασίας ή έργου, όπως τα δεδομένα προσωπικού και μισθοδοσίας ή αφορά πελάτες ή προμηθευτές, εφόσον είναι φυσικά πρόσωπα. Η μη τήρηση των υποχρεώσεων γνωστοποίησης επισύρει διοικητικές και ποινικές συνέπειες (άρ. 84)
- Πρέπει να υπάρχει διαδικασία άσκησης του δικαιώματος πρόσβασης.
  - Να παρέχεται σχετικό έντυπο αίτησης σε όσους εκδηλώσουν ενδιαφέρον.
  - Να ελέγχεται ότι το άτομο στο οποίο δίδονται τα δεδομένα είναι το ίδιο με το άτομο το οποίο αφορούν τα δεδομένα ή έχει νόμιμα εξουσιοδοτηθεί για αυτόν το σκοπό.
- Όλα τα δεδομένα να τηρούνται για το χρονικό διάστημα που προβλέπεται σύμφωνα με το Νόμο και να διαγράφονται (ή να καταστρέφονται) μετά το πέρας αυτού του χρονικού διαστήματος.
  - Η Διοίκηση του ΤΕΑΥΕΤ πρέπει να καθορίσει τους χρόνους τήρησης δεδομένων για κάθε ομάδα δεδομένων.

Τα δεδομένα μπορούν να διατηρηθούν πέρα του ανωτέρω χρονικού διαστήματος, μόνο εφόσον καταστούν ανώνυμα.

7.1 Εκπαίδευση και ευαισθητοποίηση χρηστών

Το ΤΕΑΥΕΤ οφείλει να ενημερώνει διαρκώς τους χρήστες σχετικά με τις προκλήσεις στην ασφάλεια των πληροφοριών και την προστασία των δεδομένων του Οργανισμού. Η ευαισθητοποίηση των υπαλλήλων που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μπορεί να επιτευχθεί μέσω:

- ενημερώσεων του προσωπικού σχετικά με την Προστασία Δεδομένων Προσωπικού Χαρακτήρα και των κυρώσεων που επιβάλλονται από την παραβίαση του ΓΚΠΔ,
- ενημερώσεων για το ΓΚΠΔ και τον τρόπο επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα,
- εκπαιδεύσεων αναφορικά με τους κινδύνους που αφορούν τα δεδομένα αυτά,
- ενημερώσεων σχετικά με τα μέτρα που εφαρμόζει ο Οργανισμός προκειμένου να αντιμετωπιστούν οι κίνδυνοι και οι πιθανές συνέπειές τους,
- οργάνωσης συνεδριών ευαισθητοποίησης,
- τακτικές ενημερώσεις αναφορικά με τις διαδικασίες προστασίας των δεδομένων και τους ρόλους των χρηστών σε αυτές,
- αποστολή υπενθυμίσεων μέσω ηλεκτρονικού ταχυδρομείου.

Οι λειτουργικές διαδικασίες πρέπει να τεκμηριώνονται και διατηρούνται ενημερωμένες προκειμένου να κοινοποιούνται στους χρήστες που αφορούν. Συγκεκριμένα, οποιαδήποτε ενέργεια σχετίζεται με δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για λειτουργίες της διοίκησης, είτε απλώς για χρήση

κάποιας εφαρμογής, πρέπει να τεκμηριώνεται σε έγγραφα στα οποία μπορούν να αναφέρονται οι χρήστες. Η χρησιμοποιούμενη γλώσσα πρέπει να είναι σαφής και προσαρμοσμένη σε κάθε κατηγορία χρηστών.

Καταστατικό που θα αφορά το Τμήμα Μηχανογράφησης πρέπει να συνταχθεί από το ΤΕΑΥΕΤ και να επιβληθεί η εφαρμογή του. Το εν λόγω καταστατικό οφείλει να περιλαμβάνει, κατ' ελάχιστον, τα ακόλουθα:

(α) Υπενθύμιση των κανόνων προστασίας των δεδομένων, καθώς και των κυρώσεων που επιβάλλονται στις περίπτωσης μη συμμόρφωσης με αυτούς.

(β) Το πεδίο εφαρμογής, το οποίο πρέπει να περιλαμβάνει ιδίως:

- Μεθόδους παρέμβασης των ομάδων που είναι υπεύθυνες για τη διαχείριση των πόρων του ΤΕΑΥΕΤ.
- Μέσα αυθεντικοποίησης που χρησιμοποιούνται στο ΤΕΑΥΕΤ.
- Κανόνες ασφαλείας στους οποίους οφείλουν να συμμορφώνονται οι χρήστες.

(γ) Τις διαδικασίες χρήσης του εξοπλισμού πληροφορικής και των τηλεπικοινωνιακών πόρων που διατίθενται στο χρήστη, όπως σταθμοί εργασίας, φορητό εξοπλισμό (ιδιαιτέρως στο πλαίσιο τηλεργασίας), ατομικοί χώροι αποθήκευσης, τοπικά δίκτυα, προσωπικές συσκευές και οι συνθήκες επιτρεπτής χρήσης αυτών, το Διαδίκτυο, ηλεκτρονικά μηνύματα και τηλεφωνία.

(δ) Τις συνθήκες διαχείρισης του Πληροφοριακού Συστήματος και, εάν απαιτείται, η ύπαρξη συστημάτων αυτόματης διήθησης και καταγραφής, ή συστημάτων διαχείρισης των σταθμών εργασίας.

(ε) Τις ευθύνες και τις κυρώσεις σε περιπτώσεις μη-συμμόρφωσης με το Καταστατικό.

Το ΤΕΑΥΕΤ πρέπει να σχεδιάσει και να εφαρμόσει πολιτική κατηγοριοποίησης, πολλαπλών επιπέδων, των πληροφοριών, προκειμένου να καταστεί δυνατός ο εντοπισμός εγγράφων και μηνυμάτων ηλεκτρονικού ταχυδρομείου τα οποία εμπεριέχουν εμπιστευτικά δεδομένα.

Οι υπάλληλοι του ΤΕΑΥΕΤ οφείλουν να τοποθετούν εμφανείς και ρητές επισημάνσεις σε κάθε σελίδα έντυπου ή ηλεκτρονικού εγγράφου που περιέχει προσωπικά δεδομένα ειδικών κατηγοριών.

Στις συμβάσεις εργασίας πρέπει να συμπεριλαμβάνεται ειδική ρήτρα εμπιστευτικότητας σχετικά με τα δεδομένα προσωπικού χαρακτήρα.

Σε περίπτωση αλλαγών ή τροποποιήσεων στη νομοθεσία, ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να ενημερώνει το προσωπικό.

7.2 Εντοπισμός και αντίδραση σε παραβιάσεις δεδομένων

Το ΤΕΑΥΕΤ οφείλει να καταγράφει όλα τις (επιβεβαιωμένες ή υποτιθέμενες) παραβιάσεις δεδομένων προσωπικού χαρακτήρα και τις αδυναμίες ασφάλειας μέσω της **Διαδικασίας Αντιμετώπισης Περιστατικών**. Συγκεκριμένα, όλοι οι χρήστες και οι ιδιοκτήτες των Πληροφοριακών Αγαθών του ΤΕΑΥΕΤ υποχρεούνται να ακολουθήσουν τη συγκεκριμένη διαδικασία για αναφορά συμβάντων ή αδυναμιών ασφάλειας πληροφοριών. Τα συμβάντα και οι αδυναμίες ασφάλειας πληροφοριών αναφέρονται στον Υπεύθυνο Προστασίας Δεδομένων, σύμφωνα με τη διαδικασία αυτή.

7.3 Ασφαλής αρχειοθέτηση δεδομένων

Πρέπει να διασφαλίζεται ότι σε περίπτωση που το ΤΕΑΥΕΤ διατηρεί αρχεία δεδομένων που δεν χρησιμοποιούνται σε καθημερινή βάση, αλλά δεν έχει επέλθει η λήξη της περιόδου τήρησης τους, τότε οφείλουν τα αρχεία να είναι ασφαλή, και ειδικά στην περίπτωση που τα δεδομένα αυτά είναι δεδομένα προσωπικού χαρακτήρα ή ειδικών κατηγοριών.

- Το ΤΕΑΥΕΤ οφείλει να δημιουργήσει διαδικασία διαχείρισης αρχείων, στην οποία θα καθορίζονται τα δεδομένα τα οποία πρέπει να αρχειοθετούνται, ο τρόπος και η τοποθεσία αποθήκευσής τους, καθώς και ο τρόπος διαχείρισης των περιγραφικών δεδομένων.

- Το ΤΕΑΥΕΤ πρέπει να εφαρμόζει συγκεκριμένες μεθόδους πρόσβασης σε αρχειοθετημένα δεδομένα, καθώς η χρήση τέτοιων δεδομένων υποχρεούται να ακολουθεί ειδικό χειρισμό.
- Για την καταστροφή ενός αρχείου δεδομένων, το ΤΕΑΥΕΤ πρέπει να εφαρμόσει διαδικασία που να εγγυάται την πλήρη καταστροφή του.

Το ΤΕΑΥΕΤ οφείλει να αποφεύγει την χρήση μέσων τα οποία δεν έχουν επαρκή εγγύηση ως προς την διάρκεια λειτουργίας τους. Για παράδειγμα, η διάρκεια λειτουργίας των επανεγγράψιμων CDs και DVDs σπανίως υπερβαίνουν τα τέσσερα ή πέντε χρόνια.

Τέλος, σε περίπτωση που ο Οργανισμός τηρεί δεδομένα σε ενεργές βάσεις δεδομένων, οφείλει να τις δηλώσει ως αρχειοθετημένες. Τα αρχειοθετημένα δεδομένα πρέπει να είναι προσβάσιμα μόνο από το Τμήμα του ΤΕΑΥΕΤ που είναι υπεύθυνο για την διαχείρισή τους.

7.4 Διαχείριση εκτελούντων την επεξεργασία

Το ΤΕΑΥΕΤ πρέπει να επιβλέπει τους εξωτερικούς συνεργάτες σχετικά με την ασφάλεια των δεδομένων. Οι εκτελούντες την επεξεργασία οφείλουν να παρέχουν επαρκείς εγγυήσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων. Οι εγγυήσεις πρέπει, κατ' ελάχιστο, να περιλαμβάνουν:

(α) Την κρυπτογράφηση που χρησιμοποιείται ανάλογα με ανάλογα με το βαθμό ευαισθησίας των δεδομένων, ή τουλάχιστον, την ύπαρξη διαδικασιών που εγγυώνται ότι η εταιρεία παροχής υπηρεσιών δεν έχει πρόσβαση στα δεδομένα.
(β) Την κρυπτογράφηση που χρησιμοποιείται κατά τη διαβίβαση των δεδομένων (π.χ. σύνδεση μέσω HTTPS, VPN κλπ.)
(γ) Τα μέτρα που λαμβάνονται για την προστασία του δικτύου.
(δ) Την τήρηση αρχείων καταγραφής και ελέγχου (audit logs).
(ε) Την τήρηση διαδικασίας διαχείρισης των δικαιωμάτων πρόσβασης.
(στ) Τα μέσα αυθεντικοποίησης που χρησιμοποιούνται.

Οι πάροχοι υπηρεσιών οφείλουν να κοινοποιούν την πολιτική ασφαλείας που διέπει τα πληροφοριακά τους συστήματα, πριν την υπογραφή κάποιας σύμβασης. Σε αυτή πρέπει να καθορίζεται η διάρκεια, ο σκοπός επεξεργασίας, καθώς και οι υποχρεώσεις του κάθε μέρους. Το ΤΕΑΥΕΤ οφείλει να βεβαιωθεί ότι περιλαμβάνονται συγκεκριμένες διατάξεις που στοχεύουν:

(α) Στην υποχρέωση του εκτελούντα όσον αφορά την εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα που του ανατίθεται η επεξεργασία.
(β) Στις ελάχιστες προδιαγραφές όσον αφορά την αυθεντικοποίηση των χρηστών.
(γ) Στους όρους επιστροφής των δεδομένων ή/και την καταστροφή τους μετά το πέρας της σύμβασης.
(δ) Στον τρόπο διαχείρισης (επιβεβαιωμένων ή υποτιθέμενων) συμβάντων παραβίασης των δεδομένων, καθώς και την αναφορά τους στον ΤΕΑΥΕΤ το συντομότερο δυνατόν, ειδικά όταν αφορούν δεδομένα προσωπικού χαρακτήρα.

Το ΤΕΑΥΕΤ πρέπει να αποφεύγει τη χρήση υπηρεσιών νεφοϋπολογιστικής, ελλείψει οποιασδήποτε εγγύησης σχετικά με την πραγματική γεωγραφική τοποθεσία των δεδομένων ή χωρίς να εξασφαλίζεται η νομιμότητα της διαβίβασης δεδομένων εκτός της Ευρωπαϊκής Ένωσης ή/και της αναγκαιότητας να παρασχεθεί άδεια από την ΑΠΔΠΧ για να πραγματοποιηθεί η μεταφορά των δεδομένων.

7.5 Διαβίβαση δεδομένων σε τρίτους

Πρέπει να εξασφαλίζεται, ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα και ειδικών κατηγοριών γίνεται σύμφωνα με τους όρους που προβλέπει η ισχύουσα νομοθεσία.

- Πρέπει να έχουν προσδιοριστεί οι τρίτοι που είναι συνήθεις αποδέκτες των δεδομένων και να έχουν κοινοποιηθεί και στα υποκείμενα των δεδομένων κατά τη φάση της ενημέρωσης. Είναι σκόπιμο να συσταθεί κατάλογος συνήθων αποδεκτών στους οποίους επιτρέπεται η μεταβίβαση δεδομένων προσωπικού χαρακτήρα και να προσδιοριστεί ο σκοπός της μεταβίβασης.

- Η κατάρτιση του καταλόγου και η κρίση για τη νομιμότητα της διαβίβασης σε τρίτους πρέπει να ανατίθεται στον Υπεύθυνο Προστασίας Δεδομένων.
- Η χορήγηση δεδομένων προσωπικού χαρακτήρα στους παραπάνω αποδέκτες επιτρέπεται μόνο εφόσον: (α) γίνεται από άτομα που είναι εξουσιοδοτημένα για αυτόν το σκοπό, (β) περιλαμβάνει μόνο τις κατηγορίες δεδομένων για τις οποίες έχει εγκριθεί ο συγκεκριμένος αποδέκτης, (γ) γίνεται για το σκοπό για τον οποίο έχει εγκριθεί, (δ) πληρούνται όλες οι προϋποθέσεις που ορίζει το παρόν Σχέδιο Προστασίας Δεδομένων και (ε) το αίτημα έχει διατυπωθεί εγγράφως και δικαιολογημένα.

- Οι κατηγορίες αποδεκτών στους οποίους διαβιβάζονται δεδομένα προσωπικού χαρακτήρα πρέπει να αναγράφονται στην αίτηση αδείας προς την Αρχή Προστασίας Προσωπικών Δεδομένων.
- Οι οργανισμοί ή τα πρόσωπα που λαμβάνουν τα δεδομένα πρέπει να ενημερώνονται εάν αυτά αποτελούν προσωπικού χαρακτήρα ή ειδικών κατηγοριών δεδομένα και για το επίπεδο προστασίας που πρέπει να παρέχουν σε αυτά.
- Όταν τα προσωπικά δεδομένα ειδικών κατηγοριών μεταφέρονται με μαγνητικό ή οπτικό μέσο αποθήκευσης να αναγράφεται στο μέσο/συσκευασία ο βαθμός εμπιστευτικότητας. Αυτό πρέπει να πραγματοποιείται μόνο με χρήση κρυπτογράφησης και έπειτα από σχετική έγκριση του Υπεύθυνου Προστασίας Δεδομένων του ΤΕΑΥΕΤ.
- Όταν δεδομένα προσωπικού χαρακτήρα μεταφέρονται με μαγνητικά ή οπτικά μέσα η μεταφορά πρέπει να γίνεται από υπαλλήλους του ΤΕΑΥΕΤ ή από αξιόπιστη εταιρία ταχυμεταφοράς, στη σύμβαση της οποίας πρέπει να προβλέπονται οι υποχρεώσεις λήψης μέτρων ασφάλειας και τυχόν ευθύνη.
- Όταν διαβιβάζονται δεδομένα προσωπικού χαρακτήρα μέσω τηλεπικοινωνιακής σύνδεσης να χρησιμοποιείται επαρκής κρυπτογράφηση.
- Όταν η διαβίβαση γίνεται κατόπιν αιτήσεως του υποκειμένου της επεξεργασίας ή νόμιμου αντιπροσώπου του, η αίτηση πρέπει να είναι έγγραφη, ενυπόγραφη και να τηρείται στο αρχείο του ΤΕΑΥΕΤ.
- Εάν ο αποδέκτης έχει έδρα χώρα της Ευρωπαϊκής Ένωσης, να ελέγχεται αν πληρούνται οι προϋποθέσεις του ΓΚΠΔ.
- Εάν προσωπικά δεδομένα διαβιβάζονται σε χώρες εκτός Ευρωπαϊκής Ένωσης, τότε πρέπει να υποβληθεί αίτηση αδείας στην Αρχή Προστασίας Προσωπικών Δεδομένων, προκειμένου να τηρείται η συμμόρφωση με το ΓΚΠΔ.

7.6 Διασύνδεση αρχείων με δεδομένα προσωπικού χαρακτήρα

Ως προς τη διασύνδεση αρχείων με δεδομένα προσωπικού χαρακτήρα το ΤΕΑΥΕΤ υπέχει υποχρέωση γνωστοποίησης για κάθε διασύνδεση και προηγούμενης γνωστοποίησης-αίτησης για άδεια της ΑΠΔΠΧ (άδειας διασύνδεσης), εάν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ή πρόκειται να αποκαλυφθούν με τη διασύνδεση προσωπικά δεδομένα ειδικών κατηγοριών ή εάν για τη διασύνδεση πρόκειται να γίνει χρήση ίδιου (ενιαίου) κωδικού αριθμού (Ν. 2472/97, άρ. 8).

7.7 Φάκελος προστασίας δεδομένων προσωπικού χαρακτήρα

Η τήρηση των κανόνων κι εν γένει η συμμόρφωση προς τις κανονιστικές απαιτήσεις υποστηρίζεται σημαντικά από την τήρηση φακέλου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

- Να δημιουργηθεί αρχείο, όπου τηρούνται όλα τα έγγραφα και οι αποφάσεις που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα, η σχετική τεκμηρίωση (πχ. κώδικας δεοντολογίας) και το σύνολο της αλληλογραφίας με την ΑΠΔΠΧ. Ο φάκελος αυτός πρέπει να τηρείται και ενημερώνεται με ευθύνη του εσωτερικού υπεύθυνου επεξεργασίας ενώ στοιχεία αυτού πρέπει να τηρούνται παράλληλα στις κατά περίπτωση αρμόδιες υπηρεσίες και τμήματα του ΤΕΑΥΕΤ (Νομική υπηρεσία, Διεύθυνση Ρροσωπικού, Υπεύθυνο Προστασίας Δεδομένων κλπ.).

8 Πειθαρχική Διαδικασία

Ο σκοπός αυτής της διαδικασίας είναι να διασφαλιστεί ότι οι πολιτικές και οι διαδικασίες προστασίας δεδομένων τηρούνται από όλους τους χρήστες και συνεργάτες του ΤΕΑΥΕΤ.

Η πειθαρχική διαδικασία ενεργοποιείται σε περίπτωση που επέλθει παραβίαση των δεδομένων. Η διαδικασία αυτή προϋποθέτει κατάλληλη έρευνα, ώστε να διαπιστωθούν τα πραγματικά περιστατικά και να διασφαλιστεί ότι η λήψη πειθαρχικών μέτρων είναι αιτιολογημένη.

Η πειθαρχική διαδικασία πρέπει να διασφαλίσει δίκαιη και αναλογική μεταχείριση των εργαζομένων και να λάβει υπόψη τουλάχιστον τους ακόλουθους παράγοντες:

- Τη φύση της παράβασης.
- Την επίπτωση της παραβίασης στο ΤΕΑΥΕΤ.
- Την σχετική εκπαίδευση του εργαζόμενου.
- Εάν ο υπάλληλος έχει διαπράξει παραβίαση δεδομένων στο παρελθόν.