Έκδοση 1.0, σε ισχύ από 25/05/2025

Ασφάλεια Πληροφοριακών Συστημάτων και Πολιτική Προστασίας Προσωπικών Δεδομένων

Πίνακας περιεχομένων

Γλωσσάριο

Όρος	
Υπεύθυνος επεξεργασίας δεδομένων	«υπεύθυνος επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της εν λόγω επεξεργασίας καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.
Εκτελών την επεξεργασία δεδομένων	«εκτελών την επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας.

1 Σκοπός Του Παρόντος Εγγράφου

Αυτό το έγγραφο συνοψίζει τα κύρια σημεία του συστήματος της Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Προσωπικών Δεδομένων για την Ε.Σ.Α.Ε.

2 Βασικές Αρχές Συστήματος και Πολιτικής Ασφάλειας

Το Σύστημα και η Πολιτική Ασφάλειας πληροφοριακών συστημάτων, καθώς και όλα τα θέματα, σημεία ελέγχου, διαδικασίες και αναφορές που περιλαμβάνει, διέπονται από ένα σύνολο βασικών αρχών που πρέπει να τηρούνται από όλους τους ρόλους που εμπλέκονται στη χρήση, διαχείριση και ανάπτυξη των πληροφοριακών συστημάτων της Ε.Σ.Α.Ε. Τέτοια σημεία ελέγχου βοηθούν στη διασφάλιση της λειτουργίας του οργανισμού, δηλαδή της Ε.Σ.Α.Ε. για:

- Διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών,
- Να παρέχουν ίση μεταχείριση (προνόμια και δικαιώματα) σε όλους τους χρήστες της Ε.Σ.Α.Ε.,
- Εφαρμογή όλων των απαραίτητων μέτρων για τη διασφάλιση της εμπιστευτικότητας και του απορρήτου των ενδεχομένως ευαίσθητων πληροφοριών και δεδομένων που συλλέγονται από τα συστήματα της Ε.Σ.Α.Ε. και επίσης από τρίτα μέρη που επεξεργάζονται τέτοια δεδομένα.

3 Σύνοψη συστήματος και πολιτικής

Αυτό το κείμενο συνοψίζει το επίσημο σύστημα Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Προσωπικών Δεδομένων (ΑΠΣΠΠΔ) της Ε.Σ.Α.Ε. Σκοπός του συστήματος πολιτικής είναι να θέσει τις απαραίτητες πολιτικές, απαιτήσεις και μέτρα ασφαλείας προκειμένου να διασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων και των επιχειρησιακών πόρων της Ε.Σ.Α.Ε. Οι κανόνες και οι κανονισμοί ασφαλείας που περιγράφονται στο παρόν κείμενο εφαρμόζονται σταδιακά μέσω ειδικών μέτρων ασφαλείας.

Αυτή η σύντομη έκδοση προορίζεται για ενημερωτικούς σκοπούς, προς όλους τους ενδιαφερόμενους.

Η πολιτική ΑΠΣΠΠΔ διαδραματίζει σημαντικό παράγοντα στην ικανότητα της Ε.Σ.Α.Ε. να λειτουργεί απρόσκοπτα και η εφαρμογή του βοηθά στην υποστήριξη των επιχειρησιακών δραστηριοτήτων. Επιπλέον, η ανάπτυξη και εφαρμογή της πολιτικής συμβάλλει στη συμμόρφωση με τις ειδικές απαιτήσεις ανεξαρτησίας, διαφάνειας και εμπιστευτικότητας της Ε.Σ.Α.Ε. που απορρέουν από το κανονιστικό και νομικό πλαίσιο που διέπει τη λειτουργία της Ε.Σ.Α.Ε.

Η ανάπτυξη και διατήρηση αυτής της πολιτικής ασφάλειας αποσκοπεί:

- Να λειτουργεί ως σημείο αναφοράς για όλα τα θέματα που σχετίζονται άμεσα ή έμμεσα με την ασφάλεια των δεδομένων,
- Να παρέχει καθοδήγηση στην επιλογή και εφαρμογή μέτρων ασφαλείας και αντιμέτρων,
- Η ενίσχυση των «διαύλων επικοινωνίας» μεταξύ των εμπλεκόμενων φορέων και των ενδιαφερόμενων μερών,
- Για την ασφάλεια και τη διαχείριση πόρων,
- Η εμπέδωση της σημασίας της ασφάλειας των Πληροφοριακών Συστημάτων,
- Να βοηθήσει στην ανάπτυξη μιας «κουλτούρας και φιλοσοφίας ασφάλειας και ιδιωτικότητας» για τον ανθρώπινο παράγοντα,
- Για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας ευαίσθητων πληροφοριών και δεδομένων σε συστήματα της Ε.Σ.Α.Ε., χρήστες που διαχειρίζονται τέτοιες πληροφορίες.

Το σύστημα ΑΠΣΔΔΠ προσδιορίζει τους ρόλους, τις ευθύνες και τις ικανότητες των μελών της Ε.Σ.Α.Ε. που σχετίζονται άμεσα με την εφαρμογή του.

4 Ενότητες για τη διακυβέρνηση και την πολιτική

Η Ε.Σ.Α.Ε. σε τακτά χρονικά διαστήματα ή σε περιπτώσεις σημαντικών αλλαγών επανεξετάζει και αναθεωρεί το σύστημα και την πολιτική ασφαλείας, ώστε να διασφαλίζει τα ακόλουθα:

- Ευθυγραμμίζεται με τις ανάγκες του οργανισμού και τη στρατηγική του.
- Διασφάλιση της επάρκειας των προβλεπόμενων προστατευτικών μέτρων σε σχέση με τους κινδύνους που αντιμετωπίζουν τα συστήματα πληροφορικής.
- Επίτευξη συμμόρφωσης με τις κανονιστικές απαιτήσεις, ιδίως όσον αφορά την προστασία των εμπορικά ή προσωπικών ευαίσθητων πληροφοριών και την ίση μεταχείριση των χρηστών του της Ε.Σ.Α.Ε.

Κατά την ανασκόπηση λαμβάνονται υπόψη όλα τα στοιχεία που συμβάλλουν στη διαμόρφωση μιας ολοκληρωμένης εικόνας του επιχειρησιακού περιβάλλοντος και των πληροφοριακών συστημάτων της Ε.Σ.Α.Ε. κατά την τρέχουσα περίοδο. Ειδικά στοιχεία που πρέπει να ληφθούν υπόψη είναι τα ακόλουθα:

- Η τρέχουσα κατάσταση και το επίπεδο των προληπτικών και διορθωτικών μέτρων ασφαλείας.
- Τα αποτελέσματα προηγούμενων ελέγχων ασφάλειας πληροφοριών και απορρήτου που πραγματοποιήθηκαν από τη διοίκηση ή από ανεξάρτητους φορείς.
- Οι συστάσεις σχετικά με την ορθή εφαρμογή του προγράμματος συμμόρφωσης του συστήματος ΑΠΣΔΔΠ της Ε.Σ.Α.Ε., ώστε να παραμένουν ευθυγραμμισμένες με τις κανονιστικές απαιτήσεις.
- Καταγραφή των αλλαγών που έγιναν από την προηγούμενη αναθεώρηση της πολιτικής (αλλαγές στις επιχειρηματικές διαδικασίες, στο νομοθετικό και εποπτικό πλαίσιο, στον τεχνικό εξοπλισμό και το προσωπικό).
- Η (αναθεωρημένη) ανάλυση πιθανών υφιστάμενων ή νέων κινδύνων.
- Η αξιολόγηση σύγχρονων μεθόδων επίθεσης σε πληροφοριακά συστήματα για την ολοκληρωμένη προσέγγιση των απειλών και τρωτών σημείων ασφαλείας.
- Αναφορές σχετικά με περιστατικά παραβίασης της ασφάλειας ή της ιδιωτικότητας των Πληροφοριακών Συστημάτων.

Η Ε.Σ.Α.Ε. διατηρεί και αναπτύσσει πολιτικές για:

- την διαβάθμιση και διαχείριση των δεδομένων και των πληροφοριών που επεξεργάζεται,
- την αποδεκτή χρήση των πληροφοριακών συστημάτων της από όλα τα ενδιαφερόμενα μέρη,
- τις αρχές και την διαχείριση των κωδικών πρόσβασης,
- την διαχείριση περιστατικών ασφαλείας,
- τις περιοδικές επιθεωρήσεις για την επικύρωση και την ενίσχυση της ασφάλειας,
- την δημιουργία αντιγράφων ασφαλείας πληροφοριακών συστημάτων και διαχείριση επιχειρησιακής συνέχειας,
- τις αξιολογήσεις παρόχων υπηρεσιών cloud,
- την περιοδική επανεξέταση του συστήματος διαχείρισης ασφάλειας μαζί με επικαιροποιημένες εκτιμήσεις κινδύνου.