ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΣΤΑΤΙΣΤΙΚΗ ΥΠΗΡΕΣΙΑ

Π Ο Λ Ι Τ Ι Κ Ε Σ

Α Σ Φ Α Λ Ε Ι Α Σ

Έκδοση 1.0

Μάρτιος 2026

ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

1. Εισαγωγή και Σκοπός

Η Στατιστική Υπηρεσία (ΣΥ), ως ο αρμόδιος φορέας για την ανάπτυξη, παραγωγή και διάδοση των επίσημων στατιστικών στην Κύπρο, αναγνωρίζει ότι η ασφάλεια των πληροφοριακών της συστημάτων αποτελεί θεμελιώδη πυλώνα για τη διατήρηση της δημόσιας εμπιστοσύνης. Στο πλαίσιο της συμμόρφωσης με τον περί Επίσημων Στατιστικών Νόμο του 2021 (Ν. 25(Ι)/2021) και τον Κώδικα Ορθής Πρακτικής για τις Ευρωπαϊκές Στατιστικές, η ΣΥ εφαρμόζει ένα ολοκληρωμένο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).

Το παρόν έγγραφο παρέχει μια αναλυτική επισκόπηση των πεδίων που διέπουν την ασφάλεια των δεδομένων, διασφαλίζοντας ότι όλες οι πληροφορίες που συλλέγονται και τυγχάνουν επεξεργασίας προστατεύονται από κάθε είδους απειλή, εσωτερική ή εξωτερική, τυχαία ή κακόβουλη.

2. Νομικό Πλαίσιο και Κανονιστική Συμμόρφωση

Η Στατιστική Υπηρεσία δεσμεύεται για την πλήρη εναρμόνισή της με το εθνικό και ευρωπαϊκό δίκαιο. Οι δραστηριότητες ασφάλειας διέπονται από:

- Τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR - ΕΕ 2016/679).
- Τις διατάξεις για το Στατιστικό Απόρρητο, όπως αυτές καθορίζονται στο εθνικό και ενωσιακό δίκαιο.
- Τις κατευθυντήριες γραμμές του Τμήματος Υπηρεσιών Πληροφορικής (ΤΥΠ) και της Αρχής Ψηφιακής Ασφάλειας.

Η Υπηρεσία διενεργεί συνεχείς εσωτερικούς και εξωτερικούς ελέγχους, καθώς και τεχνικές αξιολογήσεις ευπαθειών, προκειμένου να διαπιστώνεται το επίπεδο συμμόρφωσης και να λαμβάνονται διορθωτικά μέτρα όπου απαιτείται.

3. Θεματικοί Τομείς Προστασίας

3.1 Στρατηγική Διακυβέρνηση και Οργάνωση

Η διαχείριση της ασφάλειας των πληροφοριών είναι ενσωματωμένη στη διοικητική δομή της Υπηρεσίας. Καθορίζονται σαφείς ρόλοι και αρμοδιότητες, με την υποστήριξη του Υπεύθυνου Προστασίας Δεδομένων (DPO), του Υπεύθυνου Ασφάλειας Πληροφοριακών Συστημάτων (ISSO) και της Επιτροπής Ασφάλειας Πληροφοριακών Συστημάτων. Η ασφάλεια δεν περιορίζεται μόνο στη λειτουργία των συστημάτων, αλλά αποτελεί αναπόσπαστο μέρος της διαχείρισης κάθε νέου έργου από το στάδιο του σχεδιασμού του, διασφαλίζοντας ότι οι απαιτούμενοι έλεγχοι ασφάλειας προβλέπονται εξαρχής.

3.2 Διαχείριση Ανθρώπινου Δυναμικού και Καλλιέργεια Κουλτούρας

Όλοι οι λειτουργοί της ΣΥ ενημερώνονται για τις υποχρεώσεις τους όσον αφορά την εμπιστευτικότητα κατά την πρόσληψή τους και συμμετέχουν σε τακτικά προγράμματα εκπαίδευσης και ευαισθητοποίησης. Στόχος είναι η κατανόηση των κινδύνων και η υιοθέτηση ορθών πρακτικών κατά τον χειρισμό των πληροφοριών. Επιπλέον, προβλέπονται αυστηρές διαδικασίες κατά την αποχώρηση ή μετακίνηση προσωπικού, διασφαλίζοντας την άμεση διακοπή της πρόσβασης σε πληροφοριακά στοιχεία και την επιστροφή των περιουσιακών στοιχείων της Υπηρεσίας.

3.3 Ταξινόμηση και Διαχείριση Πληροφοριακών Στοιχείων

Κάθε πληροφοριακό στοιχείο (δεδομένα, λογισμικό, υλικό) καταγράφεται σε λεπτομερές μητρώο και ταυτοποιείται με μοναδικούς κωδικούς. Οι πληροφορίες ταξινομούνται ανάλογα με τον βαθμό κρισιμότητας και εμπιστευτικότητάς τους. Η διαβάθμιση αυτή καθορίζει τα αντίστοιχα επίπεδα προστασίας που πρέπει να εφαρμόζονται κατά την αποθήκευση, τη χρήση και τη διανομή τους.

3.4 Έλεγχος Πρόσβασης

Η πρόσβαση στις πληροφορίες διέπεται από την αρχή της αναγκαίας γνώσης. Η είσοδος στα πληροφοριακά συστήματα επιτρέπεται μόνο μέσω εγκεκριμένων διαδικασιών ταυτοποίησης και αυστηρών πολιτικών κωδικών πρόσβασης. Τα δικαιώματα πρόσβασης αναθεωρούνται σε τακτά χρονικά διαστήματα για να διασφαλίζεται ότι παραμένουν ευθυγραμμισμένα με τα τρέχοντα καθήκοντα των χρηστών.

3.5 Φυσική Ασφάλεια και Προστασία Υποδομών

Η Στατιστική Υπηρεσία εφαρμόζει μέτρα φυσικής προστασίας σε διάφορα επίπεδα για τη διασφάλιση των εγκαταστάσεων και του εξοπλισμού της:

- **Ζώνες Ασφαλείας:** Οι χώροι εργασίας διαχωρίζονται σε διαβαθμισμένες ζώνες με ελεγχόμενη πρόσβαση. Κρίσιμες υποδομές, όπως το δωμάτιο διακομιστών και το δωμάτιο αρχειοθέτησης διαβαθμισμένων εγγράφων, παραμένουν κλειδωμένα και η είσοδος σε αυτά επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.
- **Έλεγχος Επισκεπτών:** Κάθε εξωτερικός επισκέπτης καταγράφεται κατά την είσοδο και την έξοδό του και συνοδεύεται καθ' όλη τη διάρκεια της παραμονής του στους χώρους της Υπηρεσίας από αρμόδιο λειτουργό.
- **Προστασία από Περιβαλλοντικούς Κινδύνους:** Οι χώροι φύλαξης δεδομένων και εξοπλισμού διαθέτουν συστήματα πυρανίχνευσης, αυτόματης πυρόσβεσης, έλεγχο θερμοκρασίας.
- **Ασφάλεια Εξοπλισμού:** Ο εξοπλισμός τοποθετείται με τρόπο που ελαχιστοποιεί τους κινδύνους από φυσικές απειλές ή μη εξουσιοδοτημένη πρόσβαση, ενώ η συντήρηση του κρίσιμου εξοπλισμού γίνεται μόνο από εγκεκριμένους τεχνικούς υπό την επίβλεψη της Υπηρεσίας.
- **Ασφαλής Απόρριψη:** Εφαρμόζονται αυστηρές διαδικασίες για την καταστροφή αποθηκευτικών μέσων και εγγράφων που δεν απαιτούνται πλέον, ώστε να είναι αδύνατη η ανάκτηση των πληροφοριών.

3.6 Λειτουργική Ασφάλεια και Αντιμετώπιση Κακόβουλου Λογισμικού

Η Υπηρεσία εφαρμόζει τεχνικά μέτρα για την προστασία από ιούς και άλλες μορφές κακόβουλου λογισμικού. Η διαχείριση των αλλαγών στις υποδομές ακολουθεί τυποποιημένα στάδια έγκρισης και δοκιμών, ώστε να αποφεύγονται αστοχίες που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια. Παράλληλα, τηρούνται λεπτομερή αρχεία καταγραφής των διαφόρων δραστηριοτήτων για τον εντοπισμό και τη διερεύνηση ύποπτων ενεργειών.

3.7 Κρυπτογραφία και Ασφάλεια Επικοινωνιών

Η Στατιστική Υπηρεσία εφαρμόζει προηγμένα τεχνικά μέτρα κρυπτογράφησης για την προστασία των δεδομένων τόσο κατά την αποθήκευση όσο και κατά τη διαβίβασή τους. Χρησιμοποιούνται διεθνώς αναγνωρισμένα πρότυπα ισχυρής κρυπτογράφησης για την ασφάλεια αρχείων, εγγράφων και φορητών μέσων αποθήκευσης. Η διακίνηση πληροφοριών διενεργείται μέσω προστατευμένων καναλιών επικοινωνίας και ασφαλών πρωτοκόλλων μεταφοράς, ενώ η πρόσβαση στο δίκτυο περιορίζεται αποκλειστικά σε εξουσιοδοτημένο εξοπλισμό μέσω του Κυβερνητικού Δικτύου.

3.8 Επιχειρησιακή Συνέχεια και Ανάκτηση από Καταστροφή

Η ΣΥ διαθέτει σχέδια επιχειρησιακής συνέχειας για την αντιμετώπιση σοβαρών περιστατικών (π.χ. φυσικές καταστροφές ή εκτεταμένες βλάβες). Εφαρμόζεται αυστηρή πολιτική δημιουργίας αντιγράφων ασφαλείας (backups), τα οποία φυλάσσονται σε ασφαλείς, απομακρυσμένες τοποθεσίες. Τα σχέδια ανάκτησης δοκιμάζονται ετησίως για να διασφαλίζεται η ετοιμότητα της Υπηρεσίας να αποκαταστήσει τις κρίσιμες λειτουργίες της σε ελάχιστο χρόνο.

3.9 Διαχείριση Περιστατικών και Διερεύνηση

Η ΣΥ διαθέτει επίσημο μηχανισμό αναφοράς και διαχείρισης περιστατικών ασφάλειας. Κάθε ενδεχόμενη παραβίαση καταγράφεται, αξιολογείται ως προς τη σοβαρότητά της και αντιμετωπίζεται άμεσα. Η Υπηρεσία διασφαλίζει ότι τα αποδεικτικά στοιχεία συλλέγονται και προστατεύονται με τρόπο που επιτρέπει τη μετέπειτα ανάλυσή τους.

3.10 Διαχείριση Κύκλου Ζωής και Καταστροφή Δεδομένων

Τα δεδομένα διατηρούνται μόνο για το χρονικό διάστημα που απαιτείται για την εκπλήρωση των στατιστικών σκοπών ή των νομικών υποχρεώσεων της Υπηρεσίας. Μετά το πέρας της περιόδου διατήρησης, εφαρμόζονται διαδικασίες ασφαλούς και οριστικής καταστροφής ή ανωνυμοποίησης, ώστε να είναι αδύνατη η ανάκτηση ή η ταυτοποίηση των υποκειμένων των δεδομένων.

3.11 Σχέσεις με Προμηθευτές και Τρίτα Μέρη

Όπου απαιτείται η συνεργασία με εξωτερικούς παρόχους υπηρεσιών πληροφορικής, η ΣΥ επιβάλλει αυστηρούς όρους ασφάλειας μέσω συμβατικών δεσμεύσεων. Οι προμηθευτές οφείλουν να συμμορφώνονται με τις πολιτικές ασφάλειας της Υπηρεσίας, ενώ η πρόσβασή τους στα συστήματα παρακολουθείται και περιορίζεται στα απολύτως απαραίτητα πλαίσια του έργου τους.