ISMS-PO-00 Πολιτική Ασφάλειας Πληροφοριών

Πληροφορίες Εγγράφου

Διαβάθμιση:	Εσωτερική Χρήση
Τίτλος:	ISMS-PO-00 Πολιτική Ασφάλειας Πληροφοριών
Έκδοση:	1.0
Κατάσταση:	Τελική
Ημ/νία:	09/07/2025

Έλεγχος Εγγράφου

Έκδοση	Ημερομηνία	Συντάκτης(ες)	Κύριες Αλλαγές	Ελέγχθηκε από	Εγκρίθηκε από
0.1	04/05/2022	Δρ. Θεόδωρος Ντούσκας	Draft	Σπ. Ψωμαδέλης	Σπ. Ψωμαδέλης
1.00	24/05/2022	Δρ. Θεόδωρος Ντούσκας	Τελική	Σπ. Ψωμαδέλης	Σπ. Ψωμαδέλης
2.00	05/09/2022	Δρ. Θεόδωρος Ντούσκας	Ενημερωμένη έκδοση	Σπ. Ψωμαδέλης	Σπ. Ψωμαδέλης
2.10	23/08/2024	Δρ. Θεόδωρος Ντούσκας	Ενημερωμένη έκδοση	Σπ. Ψωμαδέλης	Σπ. Ψωμαδέλης
2.20	09/07/2025	Δρ. Θεόδωρος Ντούσκας	Ετήσια Αναθεώρηση	Σπ. Ψωμαδέλης	Σπ. Ψωμαδέλης

Πίνακας Περιεχομένων

1 Εισαγωγή

1.1 Σκοπός του εγγράφου

Το έγγραφο αυτό, αποτελεί την Πολιτική Ασφάλειας Πληροφοριών της ELTRAK. Παρουσιάζονται οι βασικές αρχές ασφάλειας που διέπουν την παρούσα πολιτική, καθώς και μια σύνοψη των κύριων σημείων όλων των πολιτικών και διαδικασιών ασφάλειας της ELTRAK.

Η ELTRAK πρέπει να παρέχει τα απαραίτητα μέσα για την ορθή εφαρμογή του ΣΔΑΠ εντός του πεδίου εφαρμογής του ΣΔΑΠ.

1.2 Έγγραφα αναφοράς – Παραπομπές

Πίνακας 1 - Έγγραφα αναφοράς – Παραπομπές

α/α	Τίτλος	Τύπος
1	Όλες οι Πολιτικές και οι Διαδικασίες Ασφάλειας Πληροφοριών της ELTRAK	Πολιτική/Διαδικασία
2	Όλα τα αρχεία που αναφέρονται σε αυτήν την πολιτική	Αρχεία

1.3 Ορισμοί και Ακρωνύμια

Στη συνέχεια παρατίθενται ορισμένοι βασικοί ορισμοί και ακρωνύμια που αναφέρονται στο παρόν έγγραφο.

Πίνακας 2 – Ορισμοί και Ακρωνύμια

Όρος	Περιγραφή
Αγαθά ή Περιουσιακά Στοιχεία (Assets)	Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία, άρα σπουδαιότητα, εκφραζόμενη σε χρηματικούς ή άλλους όρους.
Αδυναμία (Vulnerability)	Σημείο ενός ΠΣ που μπορεί να επιτρέψει να συμβεί μία παραβίαση.
Ακεραιότητα (Integrity)	Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

Ανάδοχος, Συμβασιούχος (Partner, Contracted Party)	Φορείς, εταιρείες, οργανισμοί ή φυσικά πρόσωπα με τους οποίους υπήρξαν, υπάρχουν, είτε πρόκειται να υπάρξουν εργασιακές συμβατικές σχέσεις.
Ανάλυση και Διαχείριση Επικινδυνότητας	Η διαδικασία αποτίμησης της σημαντικότητας των αγαθών ενός ΠΣ, των πιθανών απειλών και των αδυναμιών έναντι σε αυτές τις απειλές με στόχο την εύρεση του επίπεδου επικινδυνότητας.
Απειλή (Threat)	Μία πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων χαρακτηριστικών ασφάλειας ενός πληροφοριακού συστήματος.
Ασφάλεια Πληροφοριακού Συστήματος (IS Security)	Το οργανωμένο πλαίσιο από έννοιες, αρχές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τόσο τα στοιχεία του ΠΣ όσο και ολόκληρο το ΠΣ από τυχαία ή σκόπιμη απειλή.
Αυθεντικοποίηση (Authentication)	Η εξακρίβωση της γνησιότητας μίας πληροφορίας ή της γνησιότητας της ταυτότητας ενός χρήστη ή ενός υπολογιστικού συστήματος.
Αυθεντικότητα (Authenticity)	Αποφυγή ατελειών και ανακριβειών κατά την εξουσιοδοτημένη τροποποίηση μιας πληροφορίας.
Διαθεσιμότητα (Availability)	Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας ή των υπολογιστικών πόρων σε νόμιμα εξουσιοδοτημένους χρήστες.
Εγκυρότητα (Validity)	Απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.
Εμπιστευτικότητα (Confidentiality)	Αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες.
Επικινδυνότητα (Risk)	Συνάρτηση της αξίας ενός αγαθού, της έντασης των απειλών και της σοβαρότητας των αντίστοιχων αδυναμιών.
Επίπτωση (Impact)	Η απώλεια μιας αξίας, η αύξηση του κόστους ή κάποια άλλη απώλεια που προκύπτει ως αποτέλεσμα μιας παραβίασης.

Ζημία (Damage)	Η απώλεια, μερική ή ολική, της αξίας ενός αγαθού.
Κρυπτογράφηση	Τα εμπιστευτικά δεδομένα πρέπει να προστατεύονται από κρυπτοσυστήματα που υπόκεινται σε συγκεκριμένη πολιτική του οργανισμού που αφορά την χρήση της κρυπτογραφίας. Η πολιτική αυτή λαμβάνει υπόψη τα πρότυπα στον τομέα αυτό.
Μέτρο ασφάλειας (Security Countermeasure)	Ένα μέτρο σχεδιασμένο με σκοπό να εμποδίσει μία παραβίαση, να μειώσει μία αδυναμία-σημείο ευπάθειας ή να μειώσει τις δυνητικές επιπτώσεις.
Περιστατικό (Incident)	Ένα γεγονός, το οποίο έχει ως συνέπεια μία παραβίαση ή αποτελεί μία απόπειρα παραβίασης ή θέτει σε κίνδυνο την ασφάλεια ενός ΠΣ
Παραβίαση (Breach)	Ένα γεγονός το οποίο προσβάλλει μία ή περισσότερες από τις ακόλουθες ιδιότητες: αυθεντικότητα, διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, εγκυρότητα.
Πληροφοριακό Σύστημα (Information System)	Ένα οργανωμένο σύνολο αλληλοεπιδρώντων στοιχείων (άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός και διαδικασίες), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μιας επιχείρησης ή ενός οργανισμού.
Πολιτική Ασφάλειας και Προστασίας Δεδομένων (Security and Data Protection Policy)	Περιγραφή, σε γενικό επίπεδο, του συνόλου των κανόνων, των μέτρων και των διαδικασιών που ορίζουν τα φυσικά, διαδικαστικά και προσωπικά μέτρα ασφάλειας πληροφοριών και προστασίας των δεδομένων, που λαμβάνονται κατά τη διαχείριση, τη διανομή και την προστασία των αγαθών.

2 Πολιτική Ασφάλειας Πληροφοριών

2.1 Στόχος

Οι πληροφορίες αποτελούν κρίσιμο αγαθό για τις λειτουργίες της ELTRAK και την ικανότητά της να επιτυγχάνει στρατηγικούς επιχειρηματικούς στόχους. Ως εκ τούτου, η προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών είναι επιτακτική για τον οργανισμό. Στόχος αυτής της πολιτικής είναι να ορίσει τις βασικές αρχές που απαιτούνται για την προστασία των πληροφοριακών περιουσιακών στοιχείων από ένα ευρύ φάσμα απειλών και την αποτελεσματική μείωση των επιχειρησιακών κινδύνων.

Η Πολιτική Ασφάλειας Πληροφοριών παρέχει την κατεύθυνση της διαχείρισης και την υποστήριξη για την ασφάλεια των πληροφοριών σύμφωνα με τις επιχειρησιακές απαιτήσεις και τους σχετικούς νόμους και κανονισμούς.

2.2 Πεδίο Εφαρμογής

Αυτή η πολιτική ισχύει για όλα τα συστήματα, τα άτομα και τις διαδικασίες της ELTRAK, συμπεριλαμβανομένων των μελών του διοικητικού συμβουλίου, των διευθυντών, των εργαζομένων, των εργολάβων και άλλων τρίτων που έχουν πρόσβαση στα πληροφοριακά συστήματα της ELTRAK.

2.3 Γενική Πολιτική

Η ELTRAK έχει εγκρίνει την Πολιτική Ασφάλειας Πληροφοριών και προσυπογράφει, δια του παρόντος, την πλήρη δέσμευσή για την αποτελεσματική εφαρμογή και την παροχή επαρκών πόρων για τη συνεχή βελτίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ).

- Η Πολιτική Ασφάλειας Πληροφοριών αποσκοπεί στο να διασφαλιστούν τα εξής:
  - Συνεχής προστασία των πληροφοριών από τυχόν μη εξουσιοδοτημένη πρόσβαση.
  - Συνεχής διασφάλιση της Εμπιστευτικότητας των πληροφοριών της ELTRAK, των πελατών και των συνεργατών της.
  - Συνεχής διατήρηση της Ακεραιότητας των πληροφοριών της ELTRAK, των πελατών και των συνεργατών της.
  - Συνεχής διασφάλιση της Διαθεσιμότητας των πληροφοριών και των επιχειρησιακών διαδικασιών.
  - Διαρκής παρακολούθηση και τήρηση των Νομοθετικών και Κανονιστικών Απαιτήσεων της ELTRAK.
  - Το Σχέδιο Επιχειρησιακής Συνέχειας τηρείται και ελέγχεται για την αποτελεσματικότητά του.
  - Συνεχής εκπαίδευση σε θέματα Ασφάλειας Πληροφοριών για όλους τους εργαζομένους της ELTRAK.

- Η αναγνώριση και η διερεύνηση πιθανών παραβιάσεων ασφάλειας πληροφοριών και δεδομένων προσωπικού χαρακτήρα αναφέρονται στον Υπεύθυνο Ασφάλειας Πληροφοριών, διερευνώνται ενδελεχώς και αντιμετωπίζονται άμεσα και αποτελεσματικά.

- Όλες οι κατάλληλες διαδικασίες και οι επιμέρους πολιτικές ασφάλειας πληροφοριών έχουν αναπτυχθεί και εφαρμόζονται για την υποστήριξη της εν λόγω πολιτικής, περιλαμβανομένων τεχνικών και οργανωτικών μέτρων προστασίας.
- Η ELTRAK διασφαλίζει τη συνεχή συμμόρφωση με τις απαιτήσεις του προτύπου ISO 27001:2022, μέσα από διαρκή παρακολούθηση της εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.
- Ο Υπεύθυνος Ασφάλειας Πληροφοριών είναι υπεύθυνος για την τήρηση της Πολιτικής Ασφάλειας Πληροφοριών, καθώς και για την παροχή υποστήριξης και συμβουλών κατά την εφαρμογή της.
- Όλοι οι κάτοχοι θέσεων ευθύνης της ELTRAK είναι άμεσα υπεύθυνοι για την εφαρμογή της Πολιτικής, καθώς και για τη διασφάλιση της συμμόρφωσης του προσωπικού που εποπτεύουν.
- Η συμμόρφωση με την Πολιτική Ασφάλειας Πληροφοριών είναι υποχρεωτική για όλους όσους εργάζονται ή συνεργάζονται με την ELTRAK.
- Τυχόν παραβιάσεις της Πολιτικής Ασφάλειας Πληροφοριών, 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

Για τη συντήρηση των πληροφοριακών συστημάτων και υποδομών της ELTRAK χρησιμοποιούνται λειτουργικές διαδικασίες, ώστε να διασφαλίζεται η μέγιστη δυνατή αξιοποίηση των αγαθών της.

Πιθανές αλλαγές στα Πληροφοριακά Συστήματα της ELTRAK ελέγχονται από την ISMS-PR-15 Διαδικασία Διαχείρισης Αλλαγών.

Τα περιβάλλοντα ανάπτυξης και δοκιμών λογισμικού και εφαρμογών είναι ξεχωριστά από τα ενεργά περιβάλλοντα παραγωγής, για τη μείωση του κινδύνου τυχαίων αλλαγών, καθώς και μη εξουσιοδοτημένης πρόσβασης σε δεδομένα.

Όλες οι σημαντικές αλλαγές στη βασική υποδομή (π.χ. δίκτυο, διακομιστές) θα πρέπει να λαμβάνονται υπόψη για τον αντίκτυπο που μπορεί να έχουν στην ασφάλεια των πληροφοριών της ELTRAK.

Τα περιβάλλοντα ανάπτυξης και δοκιμών λογισμικού διαχωρίζονται χρησιμοποιώντας κατάλληλα μέτρα ελέγχου, όπως:

- Εκτέλεση λογισμικού σε διαφορετικούς υπολογιστές, διαφορετικούς τομείς και τομείς δικτύου.
- Χρήση διαφορετικών ονομάτων χρήστη και κωδικών πρόσβασης.
- Ανάθεση εργασιών σε όσους έχουν πρόσβαση σε πληροφοριακά συστήματα, τόσο για τον έλεγχο όσο και για την κατηγοριοποίηση των λειτουργιών στις οποίες μπορούν να έχουν πρόσβαση.

3.2 Χρήση ηλεκτρονικού ταχυδρομείου

Το ηλεκτρονικό ταχυδρομείο (email) είναι ένα ζωτικό εργαλείο επικοινωνίας τόσο εσωτερικά όσο και με πελάτες και προμηθευτές.

Η *ISMS-PO-07 Πολιτική Ηλεκτρονικού Ταχυδρομείου* ορίζει τους βασικούς κανόνες για την ορθή χρήση του ηλεκτρονικού ταχυδρομείου, καθώς και τις επιτρεπόμενες ενέργειες των εξουσιοδοτημένων χρηστών. Η πολιτική ισχύει για κάθε χρήση της υπηρεσίας, ανεξάρτητα από τη συσκευή ή την τοποθεσία (π.χ., μέσω smartphone ή εξωτερικού γραφείου).

3.3 Χρήση Διαδικτύου

Ο στόχος της *ISMS-PO-10 Πολιτικής Αποδεκτής Χρήσης Διαδικτύου* είναι να κατευθύνει όλους τους χρήστες σχετικά με:

- Αναμενόμενες πρακτικές στην εργασία.
- Επισήμανση ζητημάτων που επηρεάζουν τη χρήση του διαδικτύου.
- Περιγραφή των προτύπων που πρέπει να υιοθετήσουν οι χρήστες.
- Καταγραφή των απαραίτητων ενεργειών για την παρακολούθηση της εφαρμογής της πολιτικής.
- Ειδοποίηση των χρηστών για τις συνέπειες της κακής χρήσης του διαδικτύου.

Οι υποδομές Διαδικτύου είναι διαθέσιμες για τους σκοπούς των λειτουργικών διαδικασιών της ΕΛΤΡΑΚ. Δεδομένου ότι δεν είναι δυνατόν να καθοριστούν σαφείς κανόνες που να καλύπτουν όλες τις διαθέσιμες διαδικτυακές δραστηριότητες, η συμμόρφωσή τους με αυτούς θα πρέπει να ενσωματωθεί στο γενικό πνεύμα της πολιτικής, προκειμένου να διασφαλιστεί ότι η χρήση της υπηρεσίας είναι επαρκώς παραγωγική.

Η *ISMS-PO-10 Πολιτική Αποδεκτής Χρήσης Διαδικτύου* πρέπει να εφαρμόζεται κάθε φορά που χρησιμοποιείται η υπηρεσία Διαδικτύου. Αυτό περιλαμβάνει την πρόσβαση μέσω οποιασδήποτε συσκευής, όπως υπολογιστές ή smartphone.

3.4 Σχεδιασμός συστημάτων

Τα πληροφοριακά συστήματα και οι εγκαταστάσεις καλύπτονται από ένα σχέδιο πρόβλεψης αναγκών (βλ. *ISMS-PR-15 Διαδικασία Διαχείρισης Αλλαγών*) και από διαδικασίες αντικατάστασης εξοπλισμού που διασφαλίζουν ότι οι αυξημένες απαιτήσεις ισχύος και αποθήκευσης δεδομένων μπορούν να αντιμετωπιστούν και να καλυφθούν σε αποδεκτό χρόνο.

Οι χρήστες της ELTRAK πρέπει να ενημερώνουν τον Υπεύθυνο Ασφάλειας Πληροφοριών για ζητήματα ασφάλειας πληροφοριών, νέα αιτήματα ή αναβαθμίσεις, service packs ή ενημερώσεις κώδικα 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 από την αποδοχή και τη διαθεσιμότητά τους στο περιβάλλον παραγωγής (βλ. *ISMS-PR-12 Διαδικασία Ασφαλούς Ανάπτυξης*).

Τα κριτήρια επιλογής πρέπει να προσδιορίζονται, να έχουν συμφωνηθεί εκ των προτέρων και να έχουν τεκμηριωθεί, καθώς και να έχουν εγκριθεί από την ELTRAK.

Οι εφαρμογές τρίτων πρέπει να δοκιμάζονται για πιθανά service packs, καθώς και για μεμονωμένες ενημερώσεις κώδικα.

Οι σημαντικές αναβαθμίσεις των πληροφοριακών συστημάτων πρέπει να δοκιμάζονται διεξοδικά σε ένα ασφαλές περιβάλλον δοκιμών, ως αντίγραφο του συστήματος παραγωγής.

3.5 Προστασία από κακόβουλο κώδικα

Πρέπει να λαμβάνονται όλα τα κατάλληλα μέτρα για την προστασία των πληροφοριακών συστημάτων, των υποδομών και των πληροφοριών από κακόβουλο κώδικα.

Πρέπει να υπάρχει αποτελεσματικό και ενημερωμένο λογισμικό προστασίας από κακόβουλο λογισμικό σε όλους τους διακομιστές και τους υπολογιστές. Για την πρόληψη κακόβουλου λογισμικού ή/και φορητού κακόβουλου λογισμικού, πρέπει να εφαρμόζονται κατάλληλα μέτρα ελέγχου πρόσβασης (π.χ. δικαιώματα πρόσβασης διαχειριστή/χρήστη) για την αποτροπή μη εξουσιοδοτημένης εγκατάστασης λογισμικού από τους χρήστες.

Ορισμένοι τύποι κακόβουλου κώδικα χρησιμοποιούν τεχνολογίες που περιλαμβάνουν (ενδεικτικά) ActiveX, Java, JavaScript, VBScript, μακροεντολές, HTTPS, HTML.

Το προσωπικό της ELTRAK δεν πρέπει να εισάγει κακόβουλο κώδικα στα πληροφοριακά συστήματα της εταιρείας.

Εάν ένας υπάλληλος της ELTRAK εντοπίσει ιό σε ένα πληροφοριακό σύστημα, θα πρέπει να ειδοποιήσει αμέσως τον Υπεύθυνο Ασφάλειας Πληροφοριών.

Όλοι οι διακομιστές πρέπει να διαθέτουν αναβαθμίσεις/patches που είναι κρίσιμα για την ασφάλεια του συστήματος, αμέσως μόλις γίνουν διαθέσιμα.

Τα patches πρέπει να είναι εγκατεστημένα στο λογισμικό ολόκληρου του δικτύου της ELTRAK.

Τα αιτήματα για εγκατάσταση νέου λογισμικού γίνονται δεκτά μόνο εάν υπάρχει επαρκής τεχνική επαλήθευση για αυτά.

3.6 Αντίγραφα Ασφαλείας

Λαμβάνονται τακτικά αντίγραφα ασφαλείας βασικών επιχειρησιακών πληροφοριών, ώστε να διασφαλίζεται ότι η ELTRAK μπορεί να ανακάμψει από μια καταστροφή, βλάβη ψηφιακών μέσων ή τις συνέπειες ενός ανθρώπινου λάθους.

Υπάρχει ένας κατάλληλος κύκλος δημιουργίας αντιγράφων ασφαλείας, ο οποίος είναι καλά τεκμηριωμένος (*ISMS-PO-03 Πολιτική Δημιουργίας Αντιγράφων Ασφαλείας* και *ISMS-PR-13Διαδικασία Δημιουργίας Αντιγράφων Ασφαλείας*).

Όποιος αποθηκεύει πληροφορίες πρέπει να διασφαλίζει ότι δημιουργούνται αντίγραφα ασφαλείας.

Ένα πλήρες αντίγραφο ασφαλείας αποθηκεύεται σε μια τοποθεσία εκτός της κύριας τοποθεσίας αποθήκευσης των πληροφοριακών συστημάτων. Αυτή η τοποθεσία επιλέγεται έτσι ώστε να μην επηρεαστεί από ένα καταστροφικό συμβάν (π.χ. πυρκαγιά) που είναι πιθανό να λάβει χώρα στο κεντρικό κτίριο.

3.7 Διαχείριση μέσων αποθήκευσης

Οι κατηγορίες μέσων αποθήκευσης που καλύπτονται από αυτήν τη διαδικασία περιλαμβάνουν τα ακόλουθα:

- Φορητοί υπολογιστές.
- CD/DVD.
- USB memory stick.
- Εξωτερικές φορητές μονάδες δίσκου.
- Κινητά τηλέφωνα.

Τα αφαιρούμενα μέσα (όπως USB, δίσκοι και εκτυπωμένα έγγραφα) πρέπει να προστατεύονται για την αποτροπή ζημιάς, κλοπής ή μη εξουσιοδοτημένης πρόσβασης.

Τα μέσα αποθήκευσης που μεταφέρονται πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, κατάχρηση ή εισβολή στα δεδομένα που αποθηκεύουν.

Όλα Τα έγγραφα και αρχεία των πληροφοριακών συστημάτων πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Σε αυτά περιλαμβάνονται έγγραφα που δημιουργούνται από την ELTRAK ή άλλο χρήστη των πληροφοριακών συστημάτων (εκτός από τα εγχειρίδια που συνοδεύουν το λογισμικό).

Υπάρχουν τεκμηριωμένες διαδικασίες σχετικά με τα αντίγραφα ασφαλείας που πρέπει να ανακτηθούν από τα κτίρια της ELTRAK.

Τα αντίγραφα ασφαλείας φυλάσσονται σε ασφαλές περιβάλλον.

3.8 Παρακολούθηση

Οι καταχωρήσεις καταγραφής περιέχουν τουλάχιστον τις ακόλουθες πληροφορίες για κάθε συμβάν, όπου είναι διαθέσιμες:

- Αναγνωριστικό χρήστη
- Ημερομηνία και ώρα συμβάντος
- Ταυτότητα συστήματος (π.χ. όνομα ή/και διεύθυνση IP)
- Πληροφορίες που σχετίζονται με το συμβάν (μήνυμα ή κωδικός)
- Ένδειξη επιτυχίας ή αποτυχίας συμβάντος.

Τα αρχεία καταγραφής που καταγράφουν εξαιρέσεις και συμβάντα που σχετίζονται με την ασφάλεια διατηρούνται για τουλάχιστον έξι (6) μήνες, όπως απαιτείται από τη σχετική νομοθεσία (βλ. *ISMS-PO-11Πολιτική Καταγραφής και Παρακολούθησης*).

Η πρόσβαση στα αρχεία καταγραφής προστατεύεται από μη εξουσιοδοτημένη πρόσβαση.

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

Όπου είναι απαραίτητο, τα διαβαθμισμένα δεδομένα πρέπει να φυλάσσονται ξεχωριστά από τα μη διαβαθμισμένα.

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

Το αρχείο καταγραφής πρέπει να περιλαμβάνει (βλ. *ISMS-PO-11 Πολιτική Καταγραφής και Παρακολούθησης*):

- Χρόνοι δημιουργίας αντιγράφων ασφαλείας, μαζί με λεπτομέρειες σχετικά με τον τρόπο αλλαγής του μέσου δημιουργίας αντιγράφων ασφαλείας.
- Τα συμβάντα εκκίνησης και τερματισμού λειτουργίας οποιουδήποτε συστήματος και οποιουδήποτε εμπλεκόμενου χρήστη.
- Σφάλματα συστήματος (τύπος, ημερομηνία, ώρα), μαζί με διορθωτικές ενέργειες.

Τα αρχεία πρέπει να ελέγχονται τακτικά για να διασφαλίζεται ότι ακολουθούνται οι απαραίτητες διαδικασίες.

Τα ρολόγια των υπολογιστών συγχρονίζονται για να διασφαλίζεται η ακρίβεια των αρχείων καταγραφής του συστήματος.

3.9 Διαχείριση δικτύου

Η σωστή διαχείριση δικτύου είναι ζωτικής σημασίας για την παροχή υπηρεσιών.

Οι συνδέσεις με την υποδομή δικτύου της ELTRAK πραγματοποιούνται με ελεγχόμενο τρόπο.

Τα ασύρματα δίκτυα εφαρμόζουν ελέγχους προστασίας δεδομένων που διέρχονται από αυτά, καθώς και αποτρέπουν την μη εξουσιοδοτημένη πρόσβαση.

Υπάρχουν σαφείς αρμοδιότητες και διαδικασίες για την απομακρυσμένη πρόσβαση στα Πληροφοριακά Συστήματα της ELTRAK.

Η αρχιτεκτονική δικτύου καταγράφεται και αποθηκεύεται μαζί με τις ρυθμίσεις υλισμικού και λογισμικού που αποτελούν το δίκτυο.

Ο εξοπλισμός δικτύου καταγράφεται στον *Κατάλογο Αγαθών (Asset Inventory)*.

Σε τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το χρόνο), το λογισμικό δοκιμάζεται και τυχόν περιττά προγράμματα και υπηρεσίες τερματίζονται.

Το ασύρματο δίκτυο της ELTRAK εφαρμόζει τεχνικές κρυπτογράφησης για τα δεδομένα που χειρίζεται. Χρησιμοποιείται το πρωτόκολλο ασύρματου δικτύου WPA-2.

3.10 Ανάπτυξη και συντήρηση συστήματος

Τα προσωπικά δεδομένα που μπορούν να χρησιμοποιηθούν κατά την ανάπτυξη και τον έλεγχο λογισμικού πρέπει να προστατεύονται. Η πρόσβαση σε αυτά πρέπει να ελέγχεται σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων.

Όπου είναι εφικτό, τα δεδομένα πρέπει να χρησιμοποιούνται αποπροσωποποιημένα.

Εάν τα δεδομένα υποβάλλονται σε επεξεργασία κατά την ανάπτυξη ή τον έλεγχο λογισμικού της ELTRAK, τότε πρέπει να εφαρμόζονται συγκεκριμένα μέτρα, όπως:

- Διαδικασία αδειοδότησης.
- Αφαίρεση όλων των λειτουργικών δεδομένων από το σύστημα δοκιμών μετά τη χρήση.
- Πλήρης καταγραφή όλων των σχετικών δραστηριοτήτων.
- Οποιεσδήποτε προσωπικές ή εμπιστευτικές πληροφορίες πρέπει να προστατεύονται σαν να επρόκειτο για δεδομένα που χρησιμοποιούνται από ένα ενεργό-παραγωγικό σύστημα πληροφοριών.

3.11 Ετήσια αποτίμηση αδυναμιών

Τουλάχιστον μία φορά το χρόνο, πρέπει να διενεργείται αποτίμηση αδυναμιών των συστημάτων πληροφοριών. Η αποτίμηση αδυναμιών θα πρέπει να περιλαμβάνει τα ακόλουθα:

- Συστηματικές δοκιμές διείσδυσης.
- Σάρωση του δικτύου, εντοπισμός και καταγραφή όλων των συσκευών που μπορούν να ανιχνευτούν.

- Ανάλυση δικτύου, συμπεριλαμβανομένων των ευάλωτων διακοπτών και πυλών.
- Ανάλυση αδυναμιών, ενημερώσεων κώδικα, ευάλωτων κωδικών πρόσβασης και υπηρεσιών δικτύου.
- Ανάλυση εκμετάλλευσης αδυναμιών.

4 Υποδομή Πληροφοριακών Συστημάτων

4.1 Ασφαλείς περιοχές

Η Αποτίμηση Επικινδυνότητας καθορίζει το κατάλληλο επίπεδο προστασίας που πρέπει να υπάρχει για την επαρκή προστασία των δεδομένων που είναι αποθηκευμένα στις εγκαταστάσεις της ELTRAK.

Η *ISMS-PO-15 Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας* καθορίζει τα μέτρα προστασίας που πρέπει να ληφθούν για τη δημιουργία ενός ασφαλούς χώρου και εξηγεί πώς πρέπει να τον φροντίζει κανείς, ώστε αυτός ο χώρος να παραμένει ασφαλής.

Σε περίπτωση περιστατικού ασφαλείας (βλ. *ISMS-PR-05 Διαδικασία Διαχείρισης Περιστατικών Ασφαλείας*) ή εάν ένα μέλος του προσωπικού αποχωρήσει από την ELTRAK χωρίς να ακολουθήσει την κατάλληλη διαδικασία απόλυσης, οι κωδικοί πρόσβασης του συστήματος, καθώς και οι κωδικοί συναγερμού, πρέπει να αλλάξουν αμέσως.

4.2 Ασφάλεια εγγράφων και εξοπλισμού

Οποιαδήποτε εμπιστευτικά έγγραφα φυλάσσονται σε ασφαλή (κλειδωμένα) ντουλάπια. Μόνο εξουσιοδοτημένοι υπάλληλοι της ELTRAK έχουν πρόσβαση σε αυτά.

Τα έγγραφα που φυλάσσονται σε γραφεία προσβάσιμα σε όλο το προσωπικό ή/και εξωτερικούς επισκέπτες πρέπει να προστατεύονται από μέτρα ελέγχου φυσικής πρόσβασης, όπως:

- Κλειδωμένα ντουλάπια και κλειδιά αποθηκευμένα μακριά από το συρτάρι.
- Ασφαλείς περιοχές που προστατεύονται (π.χ., κλειδωμένος χώρος αρχείων).

Ο εξοπλισμός υπολογιστών πρέπει να βρίσκεται σε κατάλληλες φυσικές τοποθεσίες για:

- Περιορισμό των περιβαλλοντικών κινδύνων (π.χ. θερμότητα, φωτιά, καπνός, νερό, σκόνη κ.λπ.).
- Μείωση κινδύνου κλοπής.
- Περιορισμό του κινδύνου μη εξουσιοδοτημένων ατόμων να βλέπουν πληροφορίες σε οθόνες.

4.3 Διαχείριση κύκλου ζωής εξοπλισμού

Η ELTRAK και οι προμηθευτές της πρέπει να διασφαλίζουν ότι ο εξοπλισμός των πληροφοριακών συστημάτων συντηρείται σύμφωνα με τις οδηγίες του κατασκευαστή και σύμφωνα με τεκμηριωμένες εσωτερικές διαδικασίες, ώστε να διασφαλίζεται ότι παραμένει σε καλή κατάσταση.

5 Πρόσβαση σε Πληροφοριακά Συστήματα

5.1 Γενικά

Οι κωδικοί πρόσβασης των χρηστών στις πληροφορίες αλλάζουν τακτικά, σύμφωνα με την *ISMS-PO-02 Πολιτική Ελέγχου Πρόσβασης* και την *ISMS-PO-14 Πολιτική Κωδικών Πρόσβασης* ή όποτε το λογισμικό ζητά ρητά από έναν χρήστη να αλλάξει τον κωδικό πρόσβασης.

Η πρόσβαση στα πληροφοριακά συστήματα της ELTRAK προστατεύεται μέσω των ακόλουθων μέτρων ασφαλείας (η λίστα είναι ενδεικτική):

- Κάθε χρήστης έχει όνομα χρήστη και κωδικό πρόσβασης.
- Απαγορεύεται η χρήση κοινόχρηστων λογαριασμών.
- Η διαδικασία ανάκτησης κωδικού πρόσβασης προστατεύεται.
- Η πρόσβαση των χρηστών στα πληροφοριακά συστήματα παρακολουθείται και καταγράφεται.
- Κάθε χρήστης έχει ρόλους στα πληροφοριακά συστήματα που του παρέχουν πρόσβαση σύμφωνα με τις αρμοδιότητές του.
- Δεν επιτρέπεται η ανταλλαγή κωδικών πρόσβασης μεταξύ χρηστών.
- Υπάρχουν διαδικασίες για την ορθή χρήση των κωδικών πρόσβασης των διαχειριστών.

Όταν ένας εργαζόμενος αποχωρεί από την ELTRAK, η πρόσβασή του στα πληροφοριακά συστήματα πρέπει να αναστέλλεται μετά την ολοκλήρωση της τελευταίας ημέρας εργασίας του. Είναι ευθύνη του τμήματος Ανθρώπινου Δυναμικού να ζητήσει την αναστολή των δικαιωμάτων πρόσβασης μέσω του Υπεύθυνου Ασφάλειας Πληροφοριών.

5.2 Έλεγχος πρόσβασης σε διακομιστές και λογισμικό

Η πρόσβαση στους διακομιστές ελέγχεται μέσω μιας ασφαλούς διαδικασίας σύνδεσης που συμμορφώνεται με την *ISMS-PO-02 Πολιτική Ελέγχου Πρόσβασης* και την *ISMS-PR-08 Διαδικασία Ελέγχου Πρόσβασης*.

Η πρόσβαση στα συστήματα πληροφοριών γίνεται μέσω ενός μοναδικού ονόματος χρήστη που μπορεί να συσχετιστεί με ένα συγκεκριμένο άτομο.

5.3 Απομακρυσμένη πρόσβαση προμηθευτών/συνεργατών

Η απομακρυσμένη πρόσβαση των προμηθευτών/συνεργατών στα συστήματα πληροφοριών της ELTRAK ελέγχεται (βλ. *ISMS-PO-02 Πολιτική Ελέγχου Πρόσβασης* και *ISMS-PR-08 Διαδικασία Ελέγχου Πρόσβασης*).

Οποιεσδήποτε αλλαγές στις συνδέσεις των προμηθευτών/συνεργατών πρέπει να κοινοποιούνται αμέσως στον Υπεύθυνο Ασφάλειας Πληροφοριών, ώστε η πρόσβαση να μπορεί να ελεγχθεί ή να διακοπεί.

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

Οι προμηθευτές/συνεργάτες πρέπει να επικοινωνούν με τον Υπεύθυνο Ασφάλειας Πληροφοριών πριν συνδεθούν στο δίκτυο της ELTRAK. Πρέπει να τηρείται αρχείο της δραστηριότητάς τους.

Οποιοδήποτε λογισμικό απομακρυσμένης πρόσβασης πρέπει να απενεργοποιείται όταν δεν χρησιμοποιείται.

6 Λογισμικό

Η ELTRAK χρησιμοποιεί λογισμικό με άδεια χρήσης. Η ELTRAK δεν δέχεται τη χρήση λογισμικού χωρίς άδεια χρήσης.

7 Συμμόρφωση με τους κανόνες προστασίας προσωπικών δεδομένων

Η ELTRAK οφείλει να συμμορφώνεται με τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) και τη νομοθεσία για την προστασία των προσωπικών δεδομένων (Νόμος 4624/2019).

Η Νομική Ομάδα είναι υπεύθυνη να διασφαλίζει ότι όλες οι απαιτήσεις της ισχύουσας νομοθεσίας κοινοποιούνται στον Υπεύθυνο Ασφάλειας Πληροφοριών.

Επιπλέον, εφαρμόζεται Πολιτική Απορρήτου Εργαζομένων για την ενημέρωση των εργαζομένων της ELTRAK σχετικά με την προστασία των προσωπικών τους δεδομένων.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών και η Νομική Ομάδα είναι υπεύθυνες για την αναθεώρηση των πολιτικών και των διαδικασιών, προκειμένου να επιτευχθεί συμμόρφωση με τις κανονιστικές απαιτήσεις.

8 Πειθαρχική Διαδικασία

Πρέπει να διασφαλίζεται ότι οι πολιτικές και οι διαδικασίες ασφαλείας τηρούνται από όλους τους χρήστες και τους συνεργάτες της ELTRAK.

Η πειθαρχική διαδικασία ενεργοποιείται σε περίπτωση παραβίασης της ασφάλειας πληροφοριών και μετά τη διεξαγωγή πλήρους έρευνας. Η έρευνα αυτή τεκμηριώνεται.

Αυτή η πειθαρχική διαδικασία διασφαλίζει τη δίκαιη μεταχείριση των εργαζομένων, λαμβάνοντας υπόψη τους ακόλουθους παράγοντες:

- τη φύση της παραβίασης.
- την επίδραση της παραβίασης στην ELTRAK.
- την εκπαίδευση που έλαβε ο εργαζόμενος (ποιότητα και ποσότητα εκπαίδευσης).
- εάν ο εργαζόμενος έχει διαπράξει παραβίαση ασφάλειας στο παρελθόν.
- σχετικούς νομικούς παράγοντες.

9 Έλεγχος Πολιτικής

Ο Υπεύθυνος Ασφάλειας Πληροφοριών ή/και ο Εσωτερικός Ελεγκτής της ELTRAK διενεργεί ελέγχους σε τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το χρόνο) για να διασφαλίσει ότι η παρούσα πολιτική τηρείται πλήρως.