Autohellas

Autohellas	ΠΟΛΙΤΙΚΕΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ	
	Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων	**Ημερομηνία 1ης έκδοσης: 25/09/2023**

Πολιτική ασφάλειας πληροφοριακών συστημάτων

1. Σκοπός

Ο σκοπός αυτής της πολιτικής ασφαλείας πληροφοριακών συστημάτων είναι να περιγράψει τα μέτρα και τις πρακτικές ασφαλείας για την προστασία των συστημάτων, των δεδομένων και πόρων της Autohellas πληροφορικής από μη εξουσιοδοτημένη πρόσβαση, ζημία, αποκάλυψη ή αλλοίωση. Αυτή η πολιτική σχεδιάστηκε για να διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των περιουσιακών στοιχείων των συστημάτων πληροφορικής.

2. Πεδίο Εφαρμογής

Αυτή η πολιτική ισχύει για όλους τους υπαλλήλους, τους συνεργάτες και οποιαδήποτε άλλα άτομα που έχουν πρόσβαση στους πόρους πληροφορικής της Autohellas, είτε στον χώρο εργασίας είτε από απόσταση.

3. Ευθύνες Ασφαλείας

3.1. Αρμοδιότητες της διοίκησης

Η ανώτερη διοικητική ομάδα είναι υπεύθυνη για:

- Τον καθορισμό και διατήρηση της πολιτικής ασφάλειας πληροφοριακών συστημάτων.
- Την διάθεση των απαραίτητων πόρων για την εφαρμογή μέτρων ασφαλείας.
- Την Διασφάλιση συμμόρφωσης με τους ισχύοντες νόμους και κανονισμούς.

3.2. Αρμοδιότητες Τμήματος Πληροφορικής

Το Τμήμα Πληροφορικής είναι υπεύθυνο για:

- Τον σχεδιασμό, την υλοποίηση και την διατήρηση μέτρων ασφαλείας των πληροφοριακών συστημάτων.
- Την τακτική παρακολούθηση και αξιολόγηση των κινδύνων ασφάλειας των πληροφορικών συστημάτων..
- Αντιμετώπιση και διαχείριση περιστατικών ασφαλείας.

4. Έλεγχος Πρόσβασης

Η πρόσβαση σε πόρους πληροφορικής παρέχεται με βάση τους ρόλους και τις ευθύνες της εργασίας. Οι χρήστες πρέπει να χρησιμοποιούν ισχυρούς, μοναδικούς κωδικούς πρόσβασης και να τους αλλάζουν τακτικά. Η πρόσβαση σε ευαίσθητα δεδομένα και συστήματα πρέπει να περιορίζεται σε εξουσιοδοτημένο προσωπικό.

5. Προστασία Δεδομένων

5.1. Ταξινόμηση Δεδομένων

Τα δεδομένα θα πρέπει να ταξινομούνται με βάση την ευαισθησία τους και θα πρέπει να εφαρμόζονται κατάλληλοι έλεγχοι αναλόγως.

5.2. Κρυπτογράφηση

Τα ευαίσθητα δεδομένα κατά τη μεταφορά και την διατήρησή τους πρέπει να κρυπτογραφούνται χρησιμοποιώντας εγκεκριμένα πρότυπα κρυπτογράφησης.

6. Ασφάλεια Δικτύου

6.1. Τείχη προστασίας και ανίχνευση εισβολών

Τα τείχη προστασίας και τα συστήματα ανίχνευσης εισβολών πρέπει να χρησιμοποιούνται για την προστασία του δικτύου από μη εξουσιοδοτημένη πρόσβαση και κακόβουλη δραστηριότητα.

6.2. Διαχείριση αναβαθμίσεων και ενημερώσεων

Όλο το λογισμικό και το υλικό υπολογιστών θα πρέπει να ενημερώνονται τακτικά και να επιδιορθώνονται για την αντιμετώπιση τρωτών σημείων

7. **Δημιουργία αντιγράφων ασφαλείας δεδομένων**
    - Τα τακτικά αντίγραφα ασφαλείας δεδομένων πρέπει να διεξάγονται και να αποθηκεύονται με ασφάλεια.
    - Οι διαδικασίες αποκατάστασης δεδομένων θα πρέπει να δοκιμάζονται περιοδικά για να διασφαλιστεί η ανάκτηση δεδομένων

8. **Απόκριση Περιστατικών**

    8.1. Αναφορά Περιστατικών
    Όλα τα περιστατικά ασφαλείας πρέπει να αναφέρονται αμέσως στο Τμήμα Πληροφορικής.

    8.2. Αντιμετώπιση Περιστατικών
    Η Autohellas διαθέτει σχέδιο αντιμετώπισης περιστατικών, το οποίο περιλαμβάνει διαδικασίες για τον εντοπισμό, τη διαχείριση και τον μετριασμό των περιστατικών ασφάλειας.

9. **Εκπαίδευση και ευαισθητοποίηση**
    Όλοι οι εργαζόμενοι θα πρέπει να λάβουν εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια για να κατανοήσουν και να αναγνωρίσουν τις απειλές ασφαλείας και τις βέλτιστες πρακτικές.

10. **Μη Συμμόρφωση**
    Οι παραβιάσεις αυτής της πολιτικής ασφαλείας ενδέχεται να οδηγήσουν σε πειθαρχικά μέτρα, συμπεριλαμβανομένης της προσωρινής ή μόνιμης αναστολής της πρόσβασης στο σύστημα πληροφορικής.

11. **Αναθεώρηση Πολιτικής**
    Αυτή η πολιτική θα επανεξετάζεται τακτικά για να διασφαλιστεί η αποτελεσματικότητά της και η συμμόρφωσή της με τις εξελισσόμενες απειλές και κανονισμούς.

Η Autohellas δεσμεύεται να διατηρεί την ασφάλεια και την ακεραιότητα των πληροφοριακών της στοιχείων. Όλοι οι εργαζόμενοι και τα εξουσιοδοτημένα άτομα αναμένεται να τηρούν αυτήν την πολιτική για την προστασία των πόρων τεχνολογίας πληροφοριών του οργανισμού μας.