Ε.02 Πολιτική Ασφάλειας Πληροφοριών

1. ΣΚΟΠΟΣ

Η παρούσα Πολιτική Ασφάλειας Πληροφοριών καθορίζει τις βασικές αρχές, στόχους και υποχρεώσεις της SAFCO ΑΕ για την προστασία των πληροφοριών, των συστημάτων και των δικτύων που υποστηρίζουν τη λειτουργία της. Στοχεύει στη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών περιουσιακών στοιχείων της εταιρείας, σύμφωνα με τις απαιτήσεις του προτύπου **ISO 27001:2022** και της **οδηγίας NIS2**.

Η πολιτική αυτή υποστηρίζεται και συμπληρώνεται από τις ακόλουθες επιμέρους πολιτικές και διαδικασίες:

- Πολιτική Διαχείρισης Πρόσβασης (Access Control Policy)
- Πολιτική Αντιγράφων Ασφαλείας (Backup Policy)
- Διαδικασία Απομακρυσμένης Πρόσβασης & RDP υπό Εποπτεία
- Διαδικασία Χειρισμού Περιστατικών Ασφάλειας (Incident Response Plan)
- Μητρώο Περιουσιακών Στοιχείων & Εκτίμηση Κινδύνου (Asset Register & Risk Assessment)
- Πολιτική Χρήσης Εξοπλισμού και Email (Acceptable Use Policy)

2. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η πολιτική εφαρμόζεται σε όλα τα:

- Πληροφοριακά συστήματα (π.χ. FHS, CMMS, ERP GALAXY, AIMMS, Office365)
- Υπολογιστικά μέσα (Η/Υ, tablets, laptops, τηλεπικοινωνιακές συσκευές)
- Υπαλλήλους και εξωτερικούς συνεργάτες (IT, λογιστήριο, συντήρηση κ.λπ.)
- Φυσικές εγκαταστάσεις και υποδομές (Server room, UPS, γεννήτρια, αποθηκευτικοί χώροι)
- Διαδικασίες ανεφοδιασμού, τιμολόγησης και επικοινωνίας με αεροπορικές εταιρείες και προμηθευτές

3. ΑΡΧΕΣ ΚΑΙ ΔΕΣΜΕΥΣΕΙΣ

Η SAFCO ΑΕ δεσμεύεται:

- Να τηρεί τις αρχές της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών
- Να συμμορφώνεται με τη σχετική εθνική και ευρωπαϊκή νομοθεσία (GDPR, NIS2)
- Να προστατεύει τις κρίσιμες πληροφορίες από απώλεια, αλλοίωση, μη εξουσιοδοτημένη πρόσβαση ή διακοπή
- Να εφαρμόζει τεχνικά και οργανωτικά μέτρα ασφαλείας (VPN, διαχείριση χρηστών, RDP υπό εποπτεία, backup, κρυπτογράφηση)
- Να εκπαιδεύει το προσωπικό σε θέματα ασφάλειας και να ενθαρρύνει κουλτούρα ασφάλειας

4. ΡΟΛΟΙ ΚΑΙ ΥΠΕΥΘΥΝΟΤΗΤΕΣ

- **Γενικός Διευθυντής:** Έγκριση πολιτικής και διασφάλιση εφαρμογής
- **CISO:** Σχεδιασμός και παρακολούθηση της ασφάλειας πληροφοριών
- **ISMS Coordinator:** Υποστήριξη εφαρμογής πολιτικής και τεκμηρίωσης
- **IT Administrator:** Διαχείριση πρόσβασης, απομακρυσμένων συνδέσεων και φυσικής/λογικής ασφάλειας συστημάτων
- **Όλοι οι εργαζόμενοι:** Τήρηση της πολιτικής, αναφορά συμβάντων, ασφαλής χρήση εξοπλισμού

Ε.02 Πολιτική Ασφάλειας Πληροφοριών

5. ΚΑΤΗΓΟΡΙΕΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΧΕΙΡΙΣΜΟΣ

Οι πληροφορίες της SAFCO AE διακρίνονται σε:

- **Δημόσιες** (π.χ. ανακοινώσεις ιστοσελίδας)
- **Εσωτερικής χρήσης** (π.χ. διαδικασίες, templates)
- **Εμπιστευτικές** (π.χ. πελατειακά δεδομένα, τεχνικές εκθέσεις, συμβάσεις)
- **Άκρως εμπιστευτικές** (π.χ. διαπιστευτήρια, IP διευθύνσεις, access logs, έγγραφα ασφαλείας)

Η πρόσβαση σε κάθε κατηγορία γίνεται με βάση την αρχή **"ανάγκης για γνώση"** και ελέγχεται μέσω role-based access.

6. ΤΕΧΝΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

- Χρήση μοναδικών username/password με πολιτική ισχυρού κωδικού
- Δικαίωμα πρόσβασης βάσει ρόλου και θέσης (FHS, CMMS, ERP, Galaxy)
- VPN για απομακρυσμένη εργασία με χρήση 2FA όπου είναι διαθέσιμο
- Περιορισμός πρόσβασης εξωτερικών συνεργατών με εποπτεία (π.χ. AnyDesk, RDP Logging)
- Backup σε offsite μέσο με δοκιμή αποκατάστασης
- UPS και γεννήτρια για αδιάλειπτη λειτουργία κρίσιμων υποδομών
- Μηχανισμοί audit trail και logging στα κύρια συστήματα

7. ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ & ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ

- Ορισμός διαδικασίας **Incident Response** με εμπλοκή CISO / IT / Διοίκησης
- Ενημέρωση της Διοίκησης για κάθε σοβαρό περιστατικό (π.χ. κυβερνοεπίθεση, παραβίαση πρόσβασης)
- Τήρηση καταγραφής περιστατικών (Incident Log)
- Υλοποίηση σχεδίου **Backup & Recovery** και επικαιροποίηση του ετησίως
- Αξιολόγηση ανάγκης για **Disaster Recovery Plan (DRP)**

8. ΕΠΙΚΟΙΝΩΝΙΑ & ΕΚΠΑΙΔΕΥΣΗ

- Εκπαίδευση προσωπικού ανά 2 έτη σε βασικές αρχές (Core Principles JIG, ISO awareness)
- Ειδικές ενημερώσεις σε νέες απειλές ή αλλαγές συστημάτων
- Επικοινωνία με εποπτικές αρχές και προμηθευτές (JIG, Fuel Suppliers, AIA) για θέματα ασφαλείας

9. ΠΑΡΑΚΟΛΟΥΘΗΣΗ – ΕΠΙΘΕΩΡΗΣΗ – ΒΕΛΤΙΩΣΗ

- Εσωτερικές επιθεωρήσεις ISMS μία φορά τον χρόνο
- Επανεξέταση της Πολιτικής από τον Γενικό Διευθυντή και τον CISO
- Τεκμηρίωση μη συμμορφώσεων και διορθωτικών ενεργειών

Η Πολιτική αυτή τίθεται σε ισχύ από την ημερομηνία υπογραφής της και κοινοποιείται σε όλο το προσωπικό.

Εγκρίθηκε από: Διοίκηση SAFCO AE
Υπογραφή: .....
Ονοματεπώνυμο / Θέση: Κωνσταντίνος Τερζάκης
Ημερομηνία: 23.07.2025