					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P35S					Τίτλος εγγράφου: **Πολιτική Ασφάλειας IoT / OT**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 6.1, 6.2, 8	
ISO/IEC 27002:2022	Έλεγχοι 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
ΓΚΠΔ της ΕΕ	Άρθρο 32	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a), (d), (f)	
Κανονισμός DORA της ΕΕ	Άρθρο 9(2), 10(1)	

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει τους υποχρεωτικούς κανόνες για την ασφαλή χρήση και διαχείριση των συστημάτων Διαδικτύου των Πραγμάτων (IoT) και Λειτουργικής Τεχνολογίας (OT) εντός του οργανισμού. Οι συσκευές αυτές μπορεί να περιλαμβάνουν έξυπνους αισθητήρες, κάμερες ασφαλείας, μηχανήματα παραγωγής, ελεγκτές HVAC ή οποιαδήποτε βιομηχανικά συστήματα συνδεδεμένα στο δίκτυο.

1.2. Σκοπός της παρούσας πολιτικής είναι να:

1.2.1. προστατεύει τις φυσικές και ψηφιακές λειτουργίες από διακοπή ή χειραγώγηση μέσω ανεπαρκώς ασφαλισμένων συνδεδεμένων συσκευών,

1.2.2. διασφαλίζει την ασφαλή εγκατάσταση, παρακολούθηση και συντήρηση των συστημάτων IoT και OT,

1.2.3. διασφαλίζει τη συμμόρφωση με το ISO/IEC 27001:2022, την Οδηγία NIS2 της ΕΕ και τα συναφή κανονιστικά πλαίσια,

1.2.4. παρέχει πρακτικούς και εφαρμόσιμους ελέγχους για ΜΜΕ που λειτουργούν σε περιβάλλοντα γραφείου, αποθήκης ή παραγωγής.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλα τα πρόσωπα που εμπλέκονται στον σχεδιασμό, την εγκατάσταση, τη ρύθμιση παραμέτρων, τη χρήση, την υποστήριξη ή τη διάθεση συσκευών IoT ή OT. Αυτό περιλαμβάνει:

2.1.1. εργαζομένους, αναδόχους ή ασκούμενους με φυσική ή απομακρυσμένη πρόσβαση στις συσκευές,

2.1.2. προμηθευτές, λοιπά τρίτα μέρη ή τεχνικούς παροχής υπηρεσιών που εγκαθιστούν ή συντηρούν συνδεδεμένα συστήματα,

2.1.3. τον Γενικό Διευθυντή ή μέλη του προσωπικού που είναι υπεύθυνα για την εποπτεία των πολιτικών ασφάλειας.

2.2. Η πολιτική καλύπτει:

2.2.1. συσκευές IoT, όπως έξυπνες κλειδαριές, συστήματα επιτήρησης, έξυπνους μετρητές ή εκτυπωτές,

2.2.2. συστήματα OT, συμπεριλαμβανομένων των Προγραμματιζόμενων Λογικών Ελεγκτών (PLC), συστημάτων Εποπτικού Ελέγχου και Συλλογής Δεδομένων (SCADA) ή βιομηχανικών πυλών,

2.2.3. τον υποστηρικτικό εξοπλισμό, τις εφαρμογές διαχείρισης και τα δίκτυα επικοινωνίας που χρησιμοποιούνται από τα συστήματα αυτά.

2.3. Η παρούσα πολιτική εφαρμόζεται σε όλες τις τοποθεσίες εργασίας: περιβάλλοντα γραφείου, απομακρυσμένες εγκαταστάσεις, χώρους παραγωγής και πλατφόρμες νέφους που διασυνδέονται με τις εν λόγω συσκευές.

3. Στόχοι

3.1. Ασφαλής εγκατάσταση: Να διασφαλίζεται ότι όλα τα συστήματα IoT/OT ρυθμίζονται με ασφαλή τρόπο πριν τεθούν σε παραγωγική λειτουργία.

3.2. Περιορισμός έκθεσης: Να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση, η κακή χρήση ή η κατάληψη ελέγχου συνδεδεμένων συσκευών μέσω της εφαρμογής ισχυρών ελέγχων πρόσβασης και τμηματοποίησης δικτύου.

3.3. Συνεχής παρακολούθηση: Να διατηρείται ορατότητα στις λειτουργίες IoT/OT μέσω καταγραφής δραστηριότητας και παρακολούθησης για ασυνήθιστη συμπεριφορά.

3.4. Λογοδοσία προμηθευτών: Να διασφαλίζεται ότι οι τρίτοι πάροχοι ακολουθούν ασφαλείς πρακτικές εγκατάστασης, ρύθμισης παραμέτρων και συντήρησης.

3.5. Κανονιστική συμμόρφωση: Να τεκμηριώνεται πλήρης ευθυγράμμιση με τα εφαρμοστέα πρότυπα, όπως το ISO 27001, ο ΓΚΠΔ της ΕΕ (εφόσον συλλέγονται δεδομένα προσωπικού χαρακτήρα) και η Οδηγία NIS2 της ΕΕ για την ανθεκτικότητα κρίσιμων υποδομών.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής (GM)

4.1.1. Έχει τη συνολική ευθύνη για την ασφάλεια των συστημάτων IoT και OT.

4.1.2. Εγκρίνει την παρούσα πολιτική και διασφαλίζει την εφαρμογή της σε όλους τους χώρους εργασίας.

4.1.3. Επαληθεύει ότι οι προμηθευτές και οι ανάδοχοι ακολουθούν ασφαλείς πρακτικές αρχικής ρύθμισης και συντήρησης.

4.1.4. Εγκρίνει τη δικτυακή πρόσβαση για κάθε σύστημα IoT/OT.

4.2. Ορισμένος εργαζόμενος ή Υπεύθυνος Λειτουργίας (εφόσον έχει οριστεί)

4.2.1. Έχει την εποπτεία της απογραφής, της τοποθέτησης και της ρύθμισης παραμέτρων των συσκευών IoT/OT.

4.2.2. Καταγράφει για κάθε συσκευή τη θέση της, την ανάθεσή της στο δίκτυο και την τεκμηρίωση υποστήριξης.

4.2.3. Διασφαλίζει ότι οποιεσδήποτε αλλαγές, όπως ενημερώσεις υλικολογισμικού ή αντικαταστάσεις συσκευών, τεκμηριώνονται.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1. Ετήσια ανασκόπηση

9.1.1. Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον GM.

9.1.2. Η ανασκόπηση πρέπει να αξιολογεί κατά πόσον η πολιτική παραμένει αποτελεσματική, καλύπτει τους τρέχοντες τύπους συσκευών και ευθυγραμμίζεται με νέους κινδύνους ή τεχνολογίες.

9.2. Επικαιροποιήσεις βάσει εναυσμάτων

9.2.1. Η επικαιροποίηση της πολιτικής πρέπει επίσης να δρομολογείται όταν:

9.2.2. εισάγονται νέοι τύποι συστημάτων IoT ή OT,

9.2.3. οι προμηθευτές εκδίδουν ειδοποιήσεις ασφαλείας ή ανακοινώσεις λήξης κύκλου ζωής,

9.2.4. ένα περιστατικό ή έλεγχος εντοπίζει κενά στους ελέγχους IoT/OT,

9.2.5. νέοι νόμοι ή πρότυπα επιβάλλουν πρόσθετες απαιτήσεις.

9.3. Τεκμηρίωση και έλεγχος εκδόσεων

9.3.1. Όλες οι επικαιροποιήσεις πρέπει να τεκμηριώνονται, συμπεριλαμβανομένων της ημερομηνίας, του αριθμού έκδοσης και της σύνοψης των αλλαγών.

9.3.2. Ο GM πρέπει να διατηρεί ιστορικές εκδόσεις της πολιτικής για σκοπούς ελέγχου.

9.4. Κοινοποίηση αλλαγών

9.4.1. Κάθε επικαιροποίηση της πολιτικής πρέπει να κοινοποιείται σε όλο το σχετικό προσωπικό και στους προμηθευτές.

9.4.2. Οι επικαιροποιημένες εκδόσεις πρέπει να είναι προσβάσιμες μέσω κοινόχρηστων φακέλων ή έντυπου υλικού στους χώρους εγκατάστασης ή στα κέντρα ελέγχου.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική πρέπει να εφαρμόζεται σε ευθυγράμμιση με τις ακόλουθες συναφείς πολιτικές της ΜΜΕ:

10.1.1. P4S – Πολιτική Ελέγχου Πρόσβασης: εφαρμόζει ελέγχους σύνδεσης σε επίπεδο συσκευής, χρήση ισχυρών κωδικών πρόσβασης και διαδικασίες εξουσιοδοτημένης πρόσβασης για πλατφόρμες IoT και OT.

10.1.2. P9S – Πολιτική Τηλεργασίας: αποτρέπει τη χρήση απομακρυσμένης πρόσβασης σε πίνακες διαχείρισης IoT/OT μέσω ανασφαλών ή μη εγκεκριμένων διαύλων.

10.1.3. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: εφαρμόζεται όταν συσκευές IoT, όπως κάμερες ασφαλείας, επεξεργάζονται ή καταγράφουν δεδομένα προσωπικού χαρακτήρα, διασφαλίζοντας τη συμμόρφωση με τον ΓΚΠΔ της ΕΕ.

10.1.4. P30S – Πολιτική Αντιμετώπισης Περιστατικών (P30): καθορίζει τις διαδικασίες για την ανίχνευση, την αναφορά και την επίλυση περιστατικών IoT ή OT, συμπεριλαμβανομένης της ύποπτης παραποίησης ή επιχειρησιακής αστοχίας.

10.1.5. P36S – Πολιτική για τα Μέσα Κοινωνικής Δικτύωσης και τις Εξωτερικές Επικοινωνίες: διασφαλίζει ότι δεν κοινοποιούνται εξωτερικά πληροφορίες για συσκευές ή για τη διάταξη του δικτύου χωρίς έγκριση.

10.2. Κάθε συναφής πολιτική ενισχύει την εφαρμογή και την πρακτική χρήση της παρούσας πολιτικής, παρέχοντας στοχευμένη διαδικαστική καθοδήγηση.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 6.1 – Αναγνώριση και αντιμετώπιση κινδύνων: Απαιτεί οι κίνδυνοι που σχετίζονται με τα συστήματα IoT και OT να αξιολογούνται και να μετριάζονται συστηματικά.

11.1.2. Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Διασφαλίζει ασφαλή επιχειρησιακό έλεγχο επί των συνδεδεμένων συσκευών.

11.2. ISO/IEC 27002

11.2.1. Έλεγχος 5.23 – Ασφάλεια πληροφοριών για τη χρήση της Λειτουργικής Τεχνολογίας (OT): Καθορίζει την ασφαλή χρήση της OT σε φυσικά και ψηφιακά περιβάλλοντα.

11.2.2. Έλεγχος 5.31 – Ασφαλής διαμόρφωση των πληροφοριακών συστημάτων: Απαιτεί ρυθμίσεις σκλήρυνσης για συσκευές IoT/OT και αποφυγή ανασφαλών προεπιλογών.

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Ακεραιότητα λογισμικού, υλικολογισμικού και πληροφοριών: Απαιτεί επικύρωση της ακεραιότητας του υλικολογισμικού και των ενημερώσεων.

11.3.2. CM-7 – Ελάχιστη λειτουργικότητα: Οι συσκευές δεν πρέπει να έχουν ενεργοποιημένες αχρησιμοποίητες ή ανασφαλείς λειτουργίες.

11.3.3. AC-6 – Αρχή του ελαχίστου προνομίου: Η πρόσβαση στις συσκευές πρέπει να περιορίζεται μόνο σε εξουσιοδοτημένους χρήστες.

11.3.4. PE-20 – Παρακολούθηση περιουσιακών στοιχείων: Φυσική και επιχειρησιακή παρακολούθηση των περιουσιακών στοιχείων IoT και OT.

11.3.5. SC-7 – Προστασία ορίων: Τμηματοποίηση και έλεγχος των δικτυακών επικοινωνιών για συνδεδεμένα συστήματα.

11.4. ΓΚΠΔ της ΕΕ (2016/679)

11.4.1. Άρθρο 32 – Ασφάλεια της επεξεργασίας: Εάν συλλέγονται δεδομένα προσωπικού χαρακτήρα, όπως μέσω καμερών επιτήρησης, ο οργανισμός πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια της εν λόγω επεξεργασίας.

11.5. Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1. Άρθρο 21(2)(a) – Μέτρα διαχείρισης κινδύνων

11.5.2. Άρθρο 21(2)(d) – Ασφαλής ρύθμιση παραμέτρων και χρήση συσκευών

11.5.3. Άρθρο 21(2)(f) – Ασφάλεια εφοδιαστικής αλυσίδας και συστημάτων

11.6. Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1. Άρθρο 9(2) – Πεδίο εφαρμογής της διαχείρισης κινδύνων ΤΠΕ: Περιλαμβάνει βιομηχανικές και ενσωματωμένες συσκευές που χρησιμοποιούνται σε επιχειρησιακά περιβάλλοντα.

11.6.2. Άρθρο 10(1) – Συνέχεια ΤΠΕ: Απαιτεί οι ρυθμίσεις των συσκευών να υποστηρίζουν την ανθεκτικότητα και τις λειτουργίες ανάκαμψης.

11.7. COBIT 2019

11.7.1. DSS01 – Διαχείριση λειτουργιών: Εφαρμόζεται στην εποπτεία των τεχνολογικών λειτουργιών, συμπεριλαμβανομένων των φυσικών συσκευών.

11.7.2. DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Διασφαλίζει ότι τα συνδεδεμένα συστήματα παρακολουθούνται και προστατεύονται κατάλληλα.

11.7.3. APO13 – Διαχείριση ασφάλειας: Ενισχύει τις πολιτικές για τη διασφάλιση των επιχειρησιακών περιουσιακών στοιχείων στις ΜΜΕ.