					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P35					Τίτλος εγγράφου: **Πολιτική Ασφάλειας IoT / OT P35**							
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**

Ευθυγράμμιση με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	**Ρήτρα/Άρθρο**	**Σχόλιο**
ISO/IEC 27001:2022	Ρήτρα 8	
ISO/IEC 27002:2022	Έλεγχοι 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
ΓΚΠΔ της ΕΕ	Άρθρα 5, 25, 32	
Οδηγία NIS2 της ΕΕ	Άρθρα 21, 23	
Κανονισμός DORA της ΕΕ	Άρθρα 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις υποχρεωτικές απαιτήσεις ασφάλειας πληροφοριών για την εγκατάσταση, λειτουργία, παρακολούθηση και παροπλισμό συστημάτων Internet of Things (IoT) και Operational Technology (OT) εντός του οργανισμού.

1.2 Διασφαλίζει ότι τα συστήματα αυτά εντάσσονται στο ευρύτερο σύστημα διαχείρισης κυβερνοασφάλειας του οργανισμού και προστατεύονται από παραβίαση, κακή χρήση ή δολιοφθορά της λειτουργίας τους.

1.3 Η πολιτική αποσκοπεί στην εφαρμογή ισχυρών τεχνικών, οργανωτικών και διαδικαστικών ελέγχων για την προστασία συστημάτων IoT/OT που διασυνδέονται με φυσικές υποδομές, παραγωγικές διαδικασίες και περιβάλλοντα κρίσιμα για την ασφάλεια.

1.4 Υποστηρίζει κανονιστικές και συμβατικές υποχρεώσεις που αφορούν την κυβερνοασφάλεια, την ασφάλεια, τον περιβαλλοντικό έλεγχο και την επιχειρησιακή συνέχεια.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα συστήματα IoT και OT — είτε ανήκουν στην εταιρεία, είτε είναι μισθωμένα, είτε παρέχονται από τρίτους — που χρησιμοποιούνται στα λειτουργικά, διοικητικά ή παραγωγικά περιβάλλοντα του οργανισμού.

2.2 Τα συστήματα που καλύπτονται περιλαμβάνουν, ενδεικτικά και όχι περιοριστικά:

2.2.1 Συσκευές IoT, όπως περιβαλλοντικοί αισθητήρες, συστήματα ελέγχου πρόσβασης, έξυπνος φωτισμός, εξοπλισμός επιτήρησης και φορετές συσκευές

2.2.2 Πλατφόρμες OT, όπως PLC, SCADA, DCS, τερματικά HMI, διεπαφές MES και ελεγκτές πεδίου

2.2.3 Βιομηχανικά δίκτυα ελέγχου ή στοιχεία που φιλοξενούνται σε περιβάλλον νέφους και παρακολουθούν φυσικές λειτουργίες

2.3 Η πολιτική καλύπτει:

2.3.1 Όλα τα περιβάλλοντα (επιτόπια, edge, διαχειριζόμενα μέσω νέφους)

2.3.2 Όλα τα εμπλεκόμενα μέρη (εσωτερικούς χρήστες, ολοκληρωτές συστημάτων, προμηθευτές τρίτων, αναδόχους)

2.3.3 Όλες τις φάσεις του κύκλου ζωής (σχεδιασμός, προμήθεια, εγκατάσταση, λειτουργία, παροπλισμός)

3. Στόχοι

3.1 Η προστασία της υποδομής IoT και OT από εσωτερικές και εξωτερικές απειλές κυβερνοασφάλειας, συμπεριλαμβανομένων επιθέσεων άρνησης υπηρεσίας, μη εξουσιοδοτημένης πρόσβασης, εξάπλωσης ransomware και παραποίησης firmware.

3.2 Η διασφάλιση ότι οι πλατφόρμες IoT/OT δεν θα αποτελέσουν δίαυλο επιθέσεων γεφύρωσης IT-OT ούτε θα οδηγήσουν σε παραβίαση συστημάτων κρίσιμων για την ασφάλεια.

3.3 Η εφαρμογή των αρχών security by design και άμυνας σε βάθος σε όλο τον κύκλο ζωής αυτών των τεχνολογιών.

3.4 Η υποστήριξη αξιόπιστης, ασφαλούς και ελέγξιμης ενσωμάτωσης των πλατφορμών IoT και OT στο Κέντρο Επιχειρήσεων Ασφάλειας (SOC) του οργανισμού και στα σχέδια απόκρισης σε περιστατικά.

3.5 Η διασφάλιση ότι κάθε εγκατάσταση ευθυγραμμίζεται με τους ελέγχους του ISO/IEC 27001 και τη σχετική τομεακή καθοδήγηση (π.χ. IEC 62443, ISO 27019, NIST SP 800-82).

4. Ρόλοι και αρμοδιότητες

4.1 Chief Information Security Officer (CISO) / Επικεφαλής Ασφάλειας Πληροφοριών

4.1.1 Καθορίζει πολιτικές και τεχνικά πρότυπα για την κυβερνοασφάλεια IoT/OT

4.1.2 Ασκεί εποπτεία στις αξιολογήσεις κινδύνου, στην επικύρωση των ελέγχων και στον διατμηματικό συντονισμό

4.2 Μηχανικοί OT / Διευθυντές Εγκαταστάσεων και Μονάδων Παραγωγής

4.2.1 Επικυρώνουν τις ρυθμίσεις των συστημάτων OT και διασφαλίζουν την τήρηση της πολιτικής στους χώρους παραγωγής

4.2.2 Διατηρούν φυσικές και λογικές δικλίδες προστασίας για την ακεραιότητα και την ασφάλεια των συστημάτων OT

[... 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 Η παρούσα πολιτική πρέπει να υποβάλλεται σε ανασκόπηση τουλάχιστον μία φορά ετησίως και να επικαιροποιείται με βάση:

9.1.1 Αλλαγές στην αρχιτεκτονική, στους προμηθευτές ή στις πλατφόρμες συστημάτων OT ή IoT

9.1.2 Σημαντικές κανονιστικές επικαιροποιήσεις (π.χ. αναθεωρήσεις του DORA, της NIS2 ή τομεακών οδηγιών)

9.1.3 Την εμφάνιση νέων ευπαθειών ή προτύπων απειλών σε συστήματα ελέγχου

9.1.4 Ευρήματα από εσωτερικούς ή εξωτερικούς ελέγχους, δοκιμές διείσδυσης ή ασκήσεις red team

9.2 Ο CISO, ο Επικεφαλής Ασφάλειας OT και οι αρμόδιοι επικεφαλής τμημάτων είναι υπεύθυνοι για την από κοινού εκκίνηση της διαδικασίας ανασκόπησης.

9.3 Έκτακτες ανασκοπήσεις πρέπει να ενεργοποιούνται μετά από:

9.3.1 Κάθε περιστατικό σχετικό με IoT/OT που οδηγεί σε αστοχία συστήματος ή απώλεια δεδομένων

9.3.2 Εισαγωγή σημαντικού νέου εξοπλισμού, λογισμικού παρακολούθησης ή πλατφορμών firmware

9.3.3 Ενσωμάτωση έξυπνου edge computing ή αυτοματισμού ενισχυμένου με TN σε επίπεδο πεδίου

9.4 Όλες οι αλλαγές πολιτικής πρέπει:

9.4.1 Να τεκμηριώνονται στο ιστορικό εκδόσεων και στο Μητρώο Αλλαγών Πολιτικών

9.4.2 Να γνωστοποιούνται σε όλους τους επηρεαζόμενους χρήστες, προμηθευτές και χειριστές IT/OT

9.4.3 Να εγκρίνονται εκ νέου από την Εκτελεστική Διοίκηση

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική εφαρμόζεται σε συνδυασμό με τις ακόλουθες πολιτικές ασφάλειας πληροφοριών και υποστηρίζεται από αυτές:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις θεμελιώδεις αρχές ασφάλειας που επεκτείνονται και στην ασφάλεια συστημάτων IoT και OT.

10.1.2 P3 – Πολιτική Αποδεκτής Χρήσης: Καθορίζει περιορισμούς στη χρήση προσωπικών και μη εξουσιοδοτημένων συσκευών, συμπεριλαμβανομένων των λειτουργικών περιβαλλόντων.

10.1.3 P6 – Πολιτική Διαχείρισης Κινδύνων: Καθοδηγεί την αξιολόγηση, αποδοχή και μετριασμό κινδύνων που σχετίζονται με ενσωματωμένα συστήματα και συστήματα ελέγχου.

10.1.4 P12 – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Διασφαλίζει ότι όλα τα συστήματα IoT και OT καταγράφονται επίσημα και τους ανατίθενται υπεύθυνοι ιδιοκτήτες.

10.1.5 P20 – Πολιτική Προστασίας Τερματικών / Κακόβουλου Λογισμικού: Εφαρμόζεται σε συνδεδεμένους ελεγκτές, έξυπνες πύλες και συστήματα edge στην παραγωγή.

10.1.6 P22 – Πολιτική Καταγραφής και Παρακολούθησης: Επεκτείνεται στις διαδικασίες συλλογής και ανασκόπησης αρχείων καταγραφής για περιβάλλοντα OT.

10.1.7 P30 – Πολιτική Απόκρισης σε Περιστατικά: Καθορίζει άμεσα τον τρόπο με τον οποίο πρέπει να κλιμακώνονται και να διαχειρίζονται παραβιάσεις, ανωμαλίες ή αστοχίες συστημάτων IoT/OT.

10.1.8 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Παρέχει μηχανισμούς διασφάλισης για την επικύρωση της διαρκούς συμμόρφωσης με την παρούσα πολιτική.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική ευθυγραμμίζεται με διεθνώς αναγνωρισμένα πρότυπα και κανονιστικά πλαίσια που διασφαλίζουν την ασφάλεια, την ανθεκτικότητα και τη συμμόρφωση συστημάτων Internet of Things (IoT) και Operational Technology (OT) σε βιομηχανικά, παραγωγικά και επιχειρησιακά περιβάλλοντα.

11.2 ISO/IEC 27002:2022 – Έλεγχοι 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Έλεγχος 5.7 – Πληροφορίες απειλών: Υποστηρίζει την παρακολούθηση περιβαλλόντων OT και τον εντοπισμό ευπαθειών ειδικών για IoT.

11.2.2 Έλεγχος 5.23 – Ασφάλεια πληροφοριών για τη χρήση υπηρεσιών νέφους: Εφαρμόζεται όταν συσκευές IoT διασυνδέονται με πλατφόρμες νέφους για τηλεμετρία, έλεγχο ή ανάλυση.

11.2.3 Έλεγχος 5.27 – Ασφαλής αρχιτεκτονική συστημάτων και αρχές μηχανικής: Διέπει τις αρχές ασφαλούς σχεδιασμού για ενσωματωμένα συστήματα και δίκτυα ελέγχου.

11.2.4 Έλεγχος 5.31 – Ασφάλεια στις διαδικασίες ανάπτυξης και υποστήριξης: Επιβάλλει επικύρωση λογισμικού/firmware, ελέγχους ενημερώσεων και απαιτήσεις για προμηθευτές σε εγκαταστάσεις OT.

11.2.5 Έλεγχος 5.36 – Συμμόρφωση με νομικές και συμβατικές απαιτήσεις: Διασφαλίζει τη συμμόρφωση των περιουσιακών στοιχείων OT με απαιτήσεις ασφάλειας, περιβάλλοντος και κανονιστικών υποχρεώσεων.

11.2.6 Οι έλεγχοι αυτοί, στο σύνολό τους, καθορίζουν βέλτιστες πρακτικές για την ασφάλεια συστημάτων IoT/OT σε όλο τον κύκλο ζωής τους, συμπεριλαμβανομένων του σχεδιασμού αρχιτεκτονικής, της ασφαλούς εγκατάστασης, της εφαρμογής ενημερώσεων, της ανίχνευσης ανωμαλιών και της συμμόρφωσης με τομεακές απαιτήσεις.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Προστασία ορίων: Διασφαλίζει ότι τα δίκτυα OT είναι τμηματοποιημένα και προστατευμένα από μη εξουσιοδοτημένη πρόσβαση.

11.3.2 SI-4 – Παρακολούθηση συστημάτων: Απαιτεί την υλοποίηση μηχανισμών συνεχούς παρακολούθησης και ανίχνευσης ανωμαλιών σε περιβάλλοντα ICS.

11.3.3 CM-2 – Βασική γραμμή ρυθμίσεων: Επιβάλλει έλεγχο ρυθμίσεων και σκλήρυνση συσκευών σε πλατφόρμες IoT/OT.

11.3.4 AC-6 – Ελάχιστο προνόμιο: Εφαρμόζεται στην πρόσβαση χρηστών και στην απομακρυσμένη υποστήριξη από προμηθευτές ενσωματωμένων συστημάτων ελέγχου.

11.3.5 PL-8 – Αρχιτεκτονικές ασφάλειας και ιδιωτικότητας: Διέπει τον σχεδιασμό ασφαλούς ενσωμάτωσης συστημάτων, ιδίως σε έργα εκσυγχρονισμού OT.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 5 – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα: Εφαρμόζεται σε πλατφόρμες IoT που επεξεργάζονται δεδομένα από αισθητήρες ή δεδομένα συμπεριφοράς που συνδέονται με φυσικά πρόσωπα.

11.4.2 Άρθρο 25 – Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού: Απαιτεί ενσωματωμένες δικλίδες προστασίας της ιδιωτικότητας στον σχεδιασμό προϊόντων IoT και στο firmware.

11.4.3 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Επιβάλλει κρυπτογράφηση, έλεγχο πρόσβασης και ασφαλείς επικοινωνίες για τις μεταδόσεις δεδομένων έξυπνων συσκευών.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρα 21 και 23: Επιβάλλουν υποχρεώσεις ασφάλειας σε βασικές και σημαντικές οντότητες που χρησιμοποιούν συστήματα OT. Αυτές περιλαμβάνουν αξιολόγηση κινδύνου, αναφορά περιστατικών και επικύρωση της εφοδιαστικής αλυσίδας των προμηθευτών IoT/OT και της ακεραιότητας του firmware.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 9 – Διαχείριση κινδύνων ΤΠΕ: Απαιτεί την ασφαλή ενσωμάτωση ενσωματωμένων συστημάτων και τεχνολογιών OT στο πρόγραμμα διακυβέρνησης κινδύνων ΤΠΕ.

11.6.2 Άρθρο 10 – Απαιτήσεις ασφάλειας ΤΠΕ: Επιβάλλει προστατευτικά μέτρα για διασυνδεδεμένες πλατφόρμες OT που χρησιμοποιούνται σε χρηματοοικονομικά και κρίσιμα περιβάλλοντα παροχής υπηρεσιών.

11.7 COBIT 2019

11.7.1 DSS05.01 – Προστασία από κακόβουλο λογισμικό: Περιλαμβάνει ανίχνευση και απόκριση σε απειλές ειδικές για ICS και σε εκστρατείες κακόβουλου λογισμικού IoT.

11.7.2 BAI09.01 – Καθορισμός και διατήρηση απαιτήσεων ασφάλειας: Αντιστοιχίζεται στην ασφαλή προμήθεια και λειτουργία έξυπνων ή ενσωματωμένων υποδομών.

11.7.3 APO13.02 – Καθορισμός και διατήρηση σχεδίου ασφάλειας πληροφοριών: Απαιτεί τη συμπερίληψη των συστημάτων OT και των ευπαθειών τους στη συνολική στρατηγική κυβερνοασφάλειας του οργανισμού.