					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P38					Τίτλος εγγράφου: **Πολιτική Ασφαλών Επικοινωνιών και Πολυπαραγοντικής Αυθεντικοποίησης**							
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	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
ΓΚΠΔ της ΕΕ	Άρθρο 32(1)(b)	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(j)	
Κανονισμός DORA της ΕΕ	Άρθρο 9(2)(d), Άρθρο 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Σκοπός

1.1 Να καθορίσει τις απαιτήσεις για τη χρήση λύσεων πολυπαραγοντικής αυθεντικοποίησης ή συνεχούς αυθεντικοποίησης για την πρόσβαση σε συστήματα, σε ευθυγράμμιση με το Άρθρο 21(2)(j) της Οδηγίας NIS2 της ΕΕ.

1.2 Να θεσπίσει ελέγχους για ασφαλείς φωνητικές, οπτικές, γραπτές επικοινωνίες και επικοινωνίες έκτακτης ανάγκης, ώστε να προστατεύονται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλους τους μηχανισμούς αυθεντικοποίησης και σε όλα τα συστήματα επικοινωνίας (τηλεφωνικές κλήσεις, τηλεδιασκέψεις, ανταλλαγή μηνυμάτων και συστήματα ειδοποίησης έκτακτης ανάγκης) που χρησιμοποιούνται από τον οργανισμό.

2.2 Καλύπτει όλους τους εργαζομένους και τους αναδόχους, καθώς και κάθε εξωτερικό μέρος που χρησιμοποιεί τα κανάλια επικοινωνίας του οργανισμού ή αποκτά πρόσβαση στα δίκτυα και τα πληροφοριακά του συστήματα.

3. Στόχοι

3.1 Να διασφαλίζεται ότι μόνο επαρκώς αυθεντικοποιημένοι χρήστες αποκτούν πρόσβαση σε συστήματα, μειώνοντας τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης μέσω της εφαρμογής πολυπαραγοντικής αυθεντικοποίησης.

3.2 Να διασφαλίζεται ότι οι εσωτερικές επικοινωνίες και οι επικοινωνίες έκτακτης ανάγκης διαβιβάζονται με ασφαλείς μεθόδους (π.χ. κρυπτογραφημένα κανάλια), ώστε να αποτρέπονται η υποκλοπή και η παραποίηση.

3.3 Να επιτυγχάνεται συμμόρφωση με τις απαιτήσεις της Οδηγίας NIS2 της ΕΕ για ισχυρή αυθεντικοποίηση και ασφαλείς επικοινωνίες, ενισχύοντας τη συνολική κυβερνοανθεκτικότητα.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών / Ομάδες Πληροφορικής και Ασφάλειας: Καθορίζουν και διατηρούν τους μηχανισμούς πολυπαραγοντικής αυθεντικοποίησης και τα εργαλεία ασφαλούς επικοινωνίας· διασφαλίζουν την τεχνική εφαρμογή της παρούσας πολιτικής.

4.2 Διαχειριστές Πληροφοριακών Συστημάτων και ΤΠ: Υλοποιούν πολυπαραγοντική αυθεντικοποίηση για τα σχετικά συστήματα και ρυθμίζουν τις εγκεκριμένες πλατφόρμες ασφαλούς επικοινωνίας· παρακολουθούν τη συμμόρφωση.

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

9. Παρακολούθηση και έλεγχος

9.1 Η Ομάδα Ασφάλειας Πληροφοριών πρέπει να παρακολουθεί συνεχώς τα αρχεία καταγραφής αυθεντικοποίησης για απόπειρες σύνδεσης με μονοπαραγοντική αυθεντικοποίηση ή για ανώμαλες αστοχίες πολυπαραγοντικής αυθεντικοποίησης. Τα αρχεία καταγραφής των συστημάτων ασφαλούς επικοινωνίας, όπου εφαρμόζεται, πρέπει επίσης να παρακολουθούνται για απόπειρες μη εξουσιοδοτημένης πρόσβασης ή μεταβολές ρυθμίσεων.

9.2 Ο Εσωτερικός Έλεγχος ανασκοπεί σε ετήσια βάση την τήρηση των απαιτήσεων υλοποίησης πολυπαραγοντικής αυθεντικοποίησης, διασφαλίζοντας ότι όλα τα κρίσιμα συστήματα την επιβάλλουν, και επαληθεύει ότι για τις ευαίσθητες επικοινωνίες χρησιμοποιούνται αποκλειστικά εγκεκριμένα ασφαλή κανάλια. Τα ευρήματα αναφέρονται στη διοίκηση μαζί με σχετικές συστάσεις.

10. Ανασκόπηση και συντήρηση

10.1 Η παρούσα πολιτική ανασκοπείται τουλάχιστον ετησίως, καθώς και μετά από κάθε μείζον περιστατικό ασφάλειας ή κάθε νέο αναγνωρισμένο κίνδυνο που σχετίζεται με την αυθεντικοποίηση ή τις επικοινωνίες (π.χ. νέοι φορείς επίθεσης κατά της πολυπαραγοντικής αυθεντικοποίησης, εντοπισμός χρήσης μη ασφαλών καναλιών επικοινωνίας).

10.2 Οι αναθεωρήσεις πραγματοποιούνται όταν απαιτείται, ώστε να αντιμετωπίζονται οι εξελισσόμενες τεχνολογίες (π.χ. υιοθέτηση πιο ανθεκτικών λύσεων συνεχούς αυθεντικοποίησης) ή να διασφαλίζεται συμμόρφωση με επικαιροποιημένη κανονιστική καθοδήγηση (όπως μελλοντικές συστάσεις της ENISA για ασφαλείς επικοινωνίες).

11. Συναφείς πολιτικές και διασυνδέσεις

11.1 P01 – Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει τις δικλίδες αυθεντικοποίησης και επικοινωνιών σε επίπεδο οργανισμού.

11.2 P04 – Πολιτική Ελέγχου Πρόσβασης. Θεσπίζει τη διακυβέρνηση πρόσβασης που η πολυπαραγοντική αυθεντικοποίηση του P38 εφαρμόζει στην πράξη.

11.3 P11 – Πολιτική Διαχείρισης Λογαριασμών Χρηστών και Προνομίων. Συνδέει την πολυπαραγοντική αυθεντικοποίηση με τον κύκλο ζωής της προνομιούχας πρόσβασης.

11.4 P18 – Πολιτική Κρυπτογραφικών Ελέγχων. Παρέχει τις εγκεκριμένες μεθόδους κρυπτογράφησης και διαχείρισης κλειδιών για ασφαλείς επικοινωνίες.

11.5 P21 – Πολιτική Ασφάλειας Δικτύου. Διασφαλίζει τα κανάλια μεταφοράς που χρησιμοποιούνται για φωνή, βίντεο και ανταλλαγή μηνυμάτων.

11.6 P22 – Πολιτική Καταγραφής και Παρακολούθησης. Παρακολουθεί συμβάντα αυθεντικοποίησης και χρήση ασφαλών καναλιών.

11.7 P32 – Πολιτική Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή. Διασφαλίζει τις επικοινωνίες έκτακτης ανάγκης κατά τη διάρκεια κρίσεων.

11.8 P08 – Πολιτική Εκπαίδευσης και Ευαισθητοποίησης για την Ασφάλεια Πληροφοριών. Εκπαιδεύει τους χρήστες σχετικά με την πολυπαραγοντική αυθεντικοποίηση και την ασφαλή χρήση των καναλιών επικοινωνίας.

12. Αναφορές

12.1 Οδηγία NIS2 (ΕΕ 2022/2555), Άρθρο 21(2), σημείο (j) (χρήση πολυπαραγοντικής αυθεντικοποίησης και ασφαλών επικοινωνιών)

12.2 Εκτελεστικός Κανονισμός της Επιτροπής (ΕΕ) 2024/2690, Παράρτημα, Ενότητα 11 (απαιτήσεις ελέγχου πρόσβασης, συμπεριλαμβανομένης της πολυπαραγοντικής αυθεντικοποίησης για προνομιούχους λογαριασμούς)

12.3 ISO/IEC 27001:2022 και ISO/IEC 27002: