					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P41					Τίτλος εγγράφου: **Πολιτική Διαχείρισης Κινδύνου Εξάρτησης από Προμηθευτές**							
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	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
ΓΚΠΔ της ΕΕ	Άρθ. 28, Άρθ. 32(1)(d)	
Οδηγία NIS2 της ΕΕ	Άρθ. 21(2)(d), Άρθ. 21(3), Άρθ. 22	
Κανονισμός DORA της ΕΕ	Άρθ. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Σκοπός

1.1 Η παρούσα πολιτική ενισχύει τις πρακτικές ασφάλειας της εφοδιαστικής αλυσίδας του οργανισμού, θεσπίζοντας διαδικασία για την αναγνώριση και διαχείριση κρίσιμων εξαρτήσεων από προμηθευτές και παρόχους υπηρεσιών, όπως απαιτείται από το άρθρο 21(3) της Οδηγίας NIS2 της ΕΕ και από τις αξιολογήσεις κινδύνου της εφοδιαστικής αλυσίδας σε επίπεδο Ένωσης.

1.2 Η παρούσα πολιτική διασφαλίζει ότι οι κίνδυνοι που προκύπτουν από συγκέντρωση ή εξάρτηση από έναν μόνο προμηθευτή είναι κατανοητοί και μετριάζονται, και ότι τυχόν κίνδυνοι εφοδιαστικής αλυσίδας που είναι ειδικοί για τον τομέα δραστηριότητας (όπως επισημαίνονται από αρμόδιες αρχές βάσει του άρθρου 22 της Οδηγίας NIS2 της ΕΕ) ενσωματώνονται στη διαχείριση κινδύνων και στον σχεδιασμό επιχειρησιακής συνέχειας.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλους τους ουσιώδεις προμηθευτές και παρόχους υπηρεσιών από τους οποίους ο οργανισμός εξαρτάται για κρίσιμες λειτουργίες, ιδίως στην εφοδιαστική αλυσίδα ΤΠΕ (υλισμικό, λογισμικό, υπηρεσίες νέφους, τηλεπικοινωνίες, διαχειριζόμενες υπηρεσίες).

2.2 Καλύπτει τις εσωτερικές λειτουργίες, συμπεριλαμβανομένων των προμηθειών, της διαχείρισης προμηθευτών, της διαχείρισης κινδύνων και των σχετικών επιχειρησιακών τμημάτων. Περιλαμβάνει επίσης τους ίδιους τους προμηθευτές στον βαθμό που απαιτείται για τη συλλογή πληροφοριών κινδύνου. Ως «κρίσιμοι προμηθευτές» νοούνται εκείνοι των οποίων η αστοχία ή η παραβίαση της ασφάλειας θα μπορούσε να επηρεάσει σημαντικά την ικανότητά μας να παρέχουμε υπηρεσίες ή να τηρούμε νομικές υποχρεώσεις.

3. Στόχοι

3.1 Ο οργανισμός αποκτά ορατότητα στις εξαρτήσεις της εφοδιαστικής αλυσίδας, ιδίως μέσω του εντοπισμού ενιαίων σημείων αστοχίας ή υψηλού κινδύνου συγκέντρωσης στη βάση προμηθευτών μας (π.χ. εξάρτηση από έναν πάροχο νέφους για όλες τις υπηρεσίες).

3.2 Ο οργανισμός εφαρμόζει μέτρα για τη μείωση και διαχείριση κινδύνων που σχετίζονται με προμηθευτές, όπως διαφοροποίηση, σχέδια αντιμετώπισης έκτακτης ανάγκης ή απαίτηση για ενισχυμένους ελέγχους από τους προμηθευτές, ενισχύοντας έτσι την ανθεκτικότητα έναντι αστοχιών προμηθευτών ή επιθέσεων που προέρχονται από την εφοδιαστική αλυσίδα.

3.3 Ο οργανισμός ευθυγραμμίζεται με τις απαιτήσεις της Οδηγίας NIS2 της ΕΕ, ενσωματώνοντας στα οργανωτικά πλαίσια λήψης αποφάσεων για τον κίνδυνο τα αποτελέσματα τυχόν συντονισμένων αξιολογήσεων κινδύνου ασφάλειας για κρίσιμες εφοδιαστικές αλυσίδες (σύμφωνα με το άρθρο 22) και διασφαλίζοντας ότι η προσέγγισή του στον κίνδυνο της εφοδιαστικής αλυσίδας είναι τεκμηριωμένη και αποδείξιμη.

4. Ρόλοι και αρμοδιότητες

4.1 Γραφείο Διαχείρισης Προμηθευτών (VMO): Είναι υπεύθυνο για το μητρώο εξαρτήσεων από προμηθευτές και συντονίζει τις αξιολογήσεις κινδύνου. Διασφαλίζει ότι, κατά τη διαδικασία ένταξης και σε περιοδική βάση, κάθε βασικός προμηθευτής αξιολογείται ως προς την κρισιμότητα και το επίπεδο εξάρτησης.

4.2 Διαχείριση Κινδύνων (Επιτροπή Επιχειρησιακών Κινδύνων): Ανασκοπεί τον κίνδυνο συγκέντρωσης και τις αναλύσεις εξάρτησης, εγκρίνει στρατηγικές αντιμετώπισης κινδύνων (π.χ. έγκριση προσθήκης εναλλακτικού προμηθευτή ή διατήρησης πρόσθετου αποθέματος για κρίσιμα εξαρτήματα). Ενσωματώνει τον κίνδυνο της εφοδιαστικής αλυσίδας στο συνολικό Μητρώο Κινδύνων και υποβάλλει αναφορές στην Ανώτατη Διοίκηση.

[... 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 Το μητρώο εξαρτήσεων και οι αξιολογήσεις κινδύνου υπόκεινται σε εσωτερικό έλεγχο σε ετήσια βάση. Ο Εσωτερικός Έλεγχος επαληθεύει ότι όλοι οι κρίσιμοι προμηθευτές έχουν καταχωριστεί, ότι οι βαθμολογήσεις κινδύνου τους είναι επικαιροποιημένες και ότι υπάρχουν σχέδια μετριασμού τα οποία εφαρμόζονται και εξελίσσονται. Ελέγχει επίσης ότι οι εξωτερικές εισροές αξιολόγησης κινδύνου (εκθέσεις του άρθρου 22 κ.λπ.) έχουν ληφθεί δεόντως υπόψη.

9.2 Η αποτελεσματικότητα των μέτρων διαφοροποίησης και αντιμετώπισης έκτακτης ανάγκης δοκιμάζεται περιοδικά. Για παράδειγμα, μπορεί να διενεργείται προγραμματισμένη προσομοίωση κατά την οποία θεωρείται ότι ένας σημαντικός προμηθευτής αποτυγχάνει, προκειμένου να ελεγχθούν τα σχέδια επιχειρησιακής συνέχειας και οι εναλλακτικές ρυθμίσεις μας (παρόμοια με άσκηση Ανάκαμψης από Καταστροφή (DR), αλλά για διακοπή προμηθευτή). Τα αποτελέσματα αυτών των δοκιμών τεκμηριώνονται και οι τυχόν αδυναμίες αποκαθίστανται.

9.3 Μετρικές: Η λειτουργία Διαχείρισης Κινδύνων παρακολουθεί μετρικές όπως «% κρίσιμων υπηρεσιών για τις οποίες είναι διαθέσιμος τουλάχιστον ένας εναλλακτικός προμηθευτής ή λύση» ή «Οι 5 σημαντικότερες εξαρτήσεις από προμηθευτές και η τάση του κινδύνου τους». Οι μετρικές αυτές περιλαμβάνονται σε πίνακες ελέγχου κινδύνων προς την ηγεσία. Στόχος είναι η πτωτική τάση του κινδύνου εξάρτησης με την πάροδο του χρόνου· εάν οι μετρικές δείχνουν αυξανόμενη εξάρτηση, αυτό πρέπει να ενεργοποιεί σχετική συζήτηση στη διοίκηση.

10. Ανασκόπηση και συντήρηση

10.1 Η παρούσα πολιτική ανασκοπείται τουλάχιστον ετησίως από τις ομάδες Διαχείρισης Προμηθευτών και Διαχείρισης Κινδύνων. Η ανασκόπηση ενσωματώνει κάθε αλλαγή στο τοπίο προμηθευτών (π.χ. εάν νέος προμηθευτής καταστεί κρίσιμος ή εάν παλαιός αποσυρθεί σταδιακά) και κάθε νέα κανονιστική απαίτηση σχετικά με την εξωτερική ανάθεση ή τον κίνδυνο τρίτων μερών.

10.2 Εάν τομεακές αρχές εκδώσουν επικαιροποιημένη καθοδήγηση ή εάν κάποιο περιστατικό αναδείξει κενά (για παράδειγμα, εάν διακοπή προμηθευτή είχε μεγαλύτερο αντίκτυπο από τον αναμενόμενο, υποδεικνύοντας ότι η αξιολόγηση κινδύνου υποεκτίμησε την εξάρτηση), η πολιτική επικαιροποιείται ώστε να βελτιώνονται τα κριτήρια ή οι στρατηγικές μετριασμού.

10.3 Οι αναθεωρημένες εκδόσεις της πολιτικής πρέπει να εγκρίνονται από την Ανώτατη Διοίκηση. Οι σημαντικές αλλαγές γνωστοποιούνται σε όλα τα σχετικά τμήματα και το εκπαιδευτικό υλικό επικαιροποιείται αναλόγως ώστε να αποτυπώνει τις νέες διαδικασίες ή απαιτήσεις.

11. Συναφείς πολιτικές και διασυνδέσεις

11.1 P01 – Πολιτική Ασφάλειας Πληροφοριών. Αναθέτει λογοδοσία για τη διακυβέρνηση της εξάρτησης από προμηθευτές.

11.2 P02 – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης. Αποσαφηνίζει την κυριότητα των αποφάσεων για τον κίνδυνο προμηθευτών.

11.3 P06 – Πολιτική Διαχείρισης Κινδύνων. Ενσωματώνει τον κίνδυνο συγκέντρωσης στα επιχειρησιακά μητρώα κινδύνων.

11.4 P26 – Πολιτική Πρόσβασης Τρίτων Μερών και Εξωτερικών Χρηστών και Ασφάλειας Προμηθευτών. Καθορίζει τη βασική γραμμή ασφάλειας· η P41 προσθέτει ελέγχους εξάρτησης/συγκέντρωσης.

11.5 P27 – Πολιτική Χρήσης Υπηρεσιών Νέφους. Εφαρμόζει κριτήρια εξάρτησης στην υιοθέτηση υπηρεσιών νέφους και στα σχέδια εξόδου.

11.6 P28 – Πολιτική Εξωτερικής Ανάθεσης Ανάπτυξης. Καλύπτει κινδύνους εξάρτησης στην εξωτερική ανάπτυξη/μηχανική.

11.7 P32 – Πολιτική Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή. Προβλέπει σενάρια διακοπής ή υποκατάστασης προμηθευτή.

11.8 P37 – Πολιτική Νομικής και Κανονιστικής Συμμόρφωσης. Διασφαλίζει ότι οι συμβάσεις και οι υποχρεώσεις αποτυπώνουν ελέγχους εξάρτησης.

12. Αναφορές

12.1 Οδηγία NIS2 (ΕΕ 2022/2555), άρθρο 21(3) (απαιτεί τη συνεκτίμηση ευπαθειών ειδικών για κάθε άμεσο προμηθευτή/πάροχο υπηρεσιών και της ποιότητας της κυβερνοασφάλειάς τους, συμπεριλαμβανομένων των αποτελεσμάτων συντονισμένων αξιολογήσεων κινδύνου της εφοδιαστικής αλυσίδας)

12.2 Οδηγία NIS2, άρθρο 22(1) (συντονισμένες αξιολογήσεις κινδύνου ασφάλειας κρίσιμων εφοδιαστικών αλυσίδων σε επίπεδο Ένωσης – ενημερώνουν τις οντότητες για κινδύνους προμηθευτών σε επίπεδο κλάδου)

12.3 Εκτελεστικός Κανονισμός της Επιτροπής (ΕΕ) 2024/2690, Παράρτημα Ενότητα 5 (απαιτήσεις ασφάλειας εφοδιαστικής αλυσίδας για οντότητες, συμπεριλαμβανομένων κριτηρίων επιλογής προμηθευτών, διαφοροποίησης και συμβατικών υποχρεώσεων)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – συστάσεις για τον εντοπισμό κρίσιμων προμηθευτών και τη διαχείριση σχετικών κινδύνων

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022