					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P26S					Τίτλος εγγράφου: **Πολιτική Ασφάλειας Τρίτων Μερών και Προμηθευτών P26S**							
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	Clause 8	Λειτουργικοί έλεγχοι για σχέσεις με τρίτα μέρη και προμηθευτές
ISO/IEC 27002:2022	Controls 5.19–5.22	Έλεγχοι ασφάλειας προμηθευτών, συμβατικοί όροι ασφάλειας, διαχείριση αλλαγών, παρακολούθηση και ανασκόπηση
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Απόκτηση, διαδικασίες παραμετροποίησης, συμφωνίες διασύνδεσης και έλεγχοι για εξωτερικό προσωπικό
ΓΚΠΔ της ΕΕ	Άρθρα 28, 32	Συμφωνίες επεξεργασίας δεδομένων, απαιτήσεις ασφάλειας για εκτελούντες την επεξεργασία
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(a)(b)(i), 23(1)	Διαχείριση κινδύνων εφοδιαστικής αλυσίδας, εποπτεία υπηρεσιών τρίτων μερών
Κανονισμός DORA της ΕΕ	Άρθρα 5(1)(2), 28(1)(2)	Διαχείριση κινδύνων ΤΠΕ για τρίτους παρόχους υπηρεσιών
COBIT 2019	APO10, APO12, DSS05	Διαχείριση προμηθευτών και ενσωμάτωση κινδύνων

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις υποχρεωτικές απαιτήσεις ασφάλειας για τη σύναψη, διαχείριση και λήξη σχέσεων με τρίτα μέρη και προμηθευτές που έχουν πρόσβαση σε δεδομένα, συστήματα ή υπηρεσίες του οργανισμού ή τα επηρεάζουν.

1.2 Διασφαλίζει ότι οι εξωτερικοί πάροχοι — συμπεριλαμβανομένων προμηθευτών υποστήριξης ΤΠ, παρόχων υπηρεσιών νέφους, προγραμματιστών λογισμικού και αναδόχων επιχειρησιακών διαδικασιών — διαχειρίζονται τα περιουσιακά στοιχεία της εταιρείας με ασφάλεια και σύμφωνα με τις εφαρμοστέες νομικές και κανονιστικές απαιτήσεις και τα σχετικά πρότυπα.

1.3 Η παρούσα πολιτική μειώνει κινδύνους όπως διαρροές δεδομένων, μη εξουσιοδοτημένες αλλαγές σε συστήματα, κανονιστικά πρόστιμα ή διακοπή της επιχειρησιακής λειτουργίας που προκαλούνται από μη ασφαλείς ή ανεπαρκώς ελεγχόμενες ρυθμίσεις με τρίτα μέρη.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα τρίτα μέρη που:

2.1.1 Παρέχουν λογισμικό, υποδομή, υπηρεσίες φιλοξενίας ή υπηρεσίες νέφους

2.1.2 Αποκτούν πρόσβαση ή διαχειρίζονται εσωτερικά συστήματα, συσκευές ή εφαρμογές

2.1.3 Διαχειρίζονται δεδομένα, έγγραφα ή αντίγραφα ασφαλείας της εταιρείας

2.1.4 Υποστηρίζουν επιχειρησιακές λειτουργίες, ανθρώπινο δυναμικό, οικονομικές λειτουργίες ή υπηρεσίες πελατών

2.2 Εφαρμόζεται επίσης σε:

2.2.1 Εσωτερικό προσωπικό που συμμετέχει στην επιλογή, ανάθεση ή εποπτεία προμηθευτών

2.2.2 Κάθε μέλος του προσωπικού που διαχειρίζεται την ένταξη προμηθευτών, τις συμβάσεις, τις προσβάσεις ή τις ανασκοπήσεις

2.2.3 Κάθε σύστημα ή διαδικασία που εξαρτάται από στοιχεία ή υπηρεσίες τρίτων μερών

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλοι οι προμηθευτές συμμορφώνονται με σαφώς καθορισμένες απαιτήσεις ασφάλειας.

3.2 Να απαιτείται οι συμβάσεις με προμηθευτές να περιλαμβάνουν εκτελεστές υποχρεώσεις ασφάλειας, προστασίας της ιδιωτικότητας και απόκρισης σε περιστατικά.

3.3 Να αξιολογούνται και να τεκμηριώνονται οι κίνδυνοι των προμηθευτών πριν από την υπογραφή συμφωνιών ή τη χορήγηση πρόσβασης.

3.4 Να διενεργούνται τακτικές ανασκοπήσεις σε προμηθευτές υψηλού κινδύνου ή κρίσιμης σημασίας για την επιβεβαίωση της συμμόρφωσης.

3.5 Να καθιερώνεται επίσημη διαδικασία για εξαιρέσεις, διαχείριση περιστατικών και επικαιροποίηση συμβάσεων.

3.6 Να υποστηρίζεται η συμμόρφωση με τις απαιτήσεις των ISO/IEC 27001:2022, ΓΚΠΔ, NIS2 και DORA που σχετίζονται με τη διακυβέρνηση προμηθευτών.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Έχει την τελική ευθύνη για την επιλογή προμηθευτών και τη συμμόρφωση με τις απαιτήσεις ασφάλειας

4.1.2 Εγκρίνει συμβάσεις, εξαιρέσεις και κλιμακώσεις που αφορούν προμηθευτές

4.1.3 Εποπτεύει την απόκριση σε περιστατικά και τη λήψη αποφάσεων όταν οι προμηθευτές δεν εκπληρώνουν τις υποχρεώσεις τους

4.2 Πάροχος Υπηρεσιών ΤΠ ή Εσωτερικό Σημείο Επαφής για την Ασφάλεια

4.2.1 Αξιολογεί την τεχνική πρόσβαση που ζητείται από προμηθευτές

4.2.2 Εφαρμόζει κανόνες ελέγχου πρόσβασης, ανασκοπεί αρχεία καταγραφής και επαληθεύει την ασφαλή διαχείριση δεδομένων

4.2.3 Ανασκοπεί τεκμήρια ελέγχων ασφάλειας, πιστοποιήσεων ή αποτελεσμάτων ελέγχου, όπου εφαρμόζεται

[... 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 ανασκοπείται τουλάχιστον ετησίως από τον Γενικό Διευθυντή, με τη συμμετοχή του παρόχου υπηρεσιών ΤΠ ή του υπευθύνου διαχείρισης προμηθευτών.

9.2 Η πολιτική πρέπει επίσης να ανασκοπείται:

9.2.1 Μετά από κάθε σημαντική αλλαγή σε νομικές, κανονιστικές ή συμβατικές υποχρεώσεις

9.2.2 Κατόπιν περιστατικού ασφάλειας που σχετίζεται με προμηθευτή ή ευρήματος ελέγχου

9.2.3 Κατά την εισαγωγή νέων κατηγοριών προμηθευτών (π.χ. κρίσιμες πλατφόρμες SaaS)

9.3 Όλες οι επικαιροποιήσεις πρέπει να:

9.3.1 Τεκμηριώνονται με ιστορικό εκδόσεων και αιτιολόγηση

9.3.2 Εγκρίνονται από τον Γενικό Διευθυντή

9.3.3 Γνωστοποιούνται στο σχετικό εσωτερικό προσωπικό και στους υπευθύνους διαχείρισης προμηθευτών

9.3.4 Τηρούνται μαζί με τις προηγούμενες εκδόσεις σύμφωνα με την Πολιτική P14S – Διατήρηση και Ασφαλής Διάθεση Δεδομένων

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η αποτελεσματικότητα της παρούσας πολιτικής εξαρτάται από τον συντονισμό με τις ακόλουθες πολιτικές ασφάλειας πληροφοριών για ΜΜΕ:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τη λογοδοσία για την εποπτεία προμηθευτών και την εφαρμογή συμβατικών υποχρεώσεων.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Παρέχει τους κανόνες περιορισμού πρόσβασης που πρέπει να εφαρμόζονται όταν παρέχεται σε προμηθευτές πρόσβαση σε συστήματα.

10.1.3 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι οι προμηθευτές που διαχειρίζονται δεδομένα προσωπικού χαρακτήρα συμμορφώνονται με τις αρχές προστασίας δεδομένων και τις νομικές απαιτήσεις.

10.1.4 P14S – Πολιτική Διατήρησης και Ασφαλούς Διάθεσης Δεδομένων: Εφαρμόζεται σε κάθε δεδομένο ή αρχείο που κοινοποιείται σε προμηθευτές ή αποθηκεύεται από αυτούς και διέπει την ασφαλή διάθεση μετά τη λήξη της σύμβασης.

10.1.5 P30S – Πολιτική Απόκρισης σε Περιστατικά: Καθορίζει τον τρόπο απόκρισης όταν προμηθευτής προκαλεί ή εμπλέκεται σε περιστατικό ασφάλειας, συμπεριλαμβανομένων διαδικασιών κλιμάκωσης και διαχείρισης τεκμηρίων.

10.2 Οι πολιτικές αυτές λειτουργούν συμπληρωματικά, ώστε ο κίνδυνος που σχετίζεται με προμηθευτές να ελέγχεται σε όλο τον κύκλο ζωής της σύμβασης.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Απαιτεί την εφαρμογή λειτουργικών ελέγχων, συμπεριλαμβανομένων εκείνων που εφαρμόζονται στις σχέσεις με τρίτα μέρη και προμηθευτές.

11.2 ISO/IEC 27002

11.2.1 Control 5.19 – Διασφαλίζει ότι τα μέτρα ασφάλειας προμηθευτών ευθυγραμμίζονται με τις απαιτήσεις του οργανισμού.

11.2.2 Control 5.20 – Απαιτεί επίσημες συμφωνίες που καλύπτουν όρους ασφάλειας, αρμοδιότητες και υποχρεώσεις σε περίπτωση παραβίασης.

11.2.3 Control 5.21 – Ελέγχει αλλαγές στις υπηρεσίες προμηθευτών που μπορεί να επηρεάσουν τη στάση ασφάλειας.

11.2.4 Control 5.22 – Απαιτεί παρακολούθηση και ανασκόπηση των υπηρεσιών προμηθευτών και της συμμόρφωσής τους.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Διέπει την απόκτηση εξωτερικών συστημάτων και υπηρεσιών, απαιτώντας αξιολογήσεις κινδύνου και καθορισμένες προσδοκίες.

11.3.2 SA-10 – Ελέγχει διαδικασίες παραμετροποίησης και αλλαγών που αφορούν συστήματα υπό τη διαχείριση τρίτων μερών.

11.3.3 CA-3 – Απαιτεί συμφωνίες διασύνδεσης για συστήματα που περιλαμβάνουν εξωτερικές οντότητες.

11.3.4 PS-7 – Καθορίζει απαιτήσεις ελέγχου καταλληλότητας και λογοδοσίας για εξωτερικό προσωπικό.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 28 – Απαιτεί συμφωνίες επεξεργασίας δεδομένων με προμηθευτές που ενεργούν ως εκτελούντες την επεξεργασία.

11.4.2 Άρθρο 32 – Επιβάλλει κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας για όλους τους εκτελούντες την επεξεργασία δεδομένων.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(a), (b), (i) – Επιβάλλει διαχείριση κινδύνων της αλυσίδας εφοδιασμού ΤΠΕ και ελέγχους για τρίτα μέρη.

11.5.2 Άρθρο 23(1) – Απαιτεί τεκμηριωμένη εποπτεία υπηρεσιών τρίτων μερών για ουσιώδεις και σημαντικές οντότητες.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 5(1) – Απαιτεί πλαίσιο διαχείρισης κινδύνων ΤΠΕ που καλύπτει όλους τους κρίσιμους τρίτους παρόχους.

11.6.2 Άρθρο 5(2) – Προβλέπει συμβατικούς και λειτουργικούς ελέγχους για εξαρτήσεις από υπηρεσίες ΤΠΕ.

11.6.3 Άρθρο 28(1), (2) – Καθορίζει κανόνες εποπτείας για τον κίνδυνο τρίτων παρόχων ΤΠΕ στον χρηματοοικονομικό τομέα.

11.7 COBIT 2019

11.7.1 APO10 – «Διαχείριση Προμηθευτών» περιγράφει ελέγχους ανάθεσης και προσδοκίες διαχείρισης σχέσεων.

11.7.2 APO12 – «Διαχείριση Κινδύνου» ενσωματώνει τον κίνδυνο προμηθευτών στη διακυβέρνηση κινδύνων του οργανισμού.

11.7.3 DSS05 – «Διαχείριση Υπηρεσιών Ασφάλειας» εφαρμόζεται σε διαχειριζόμενους τρίτους παρόχους και παρόχους υπηρεσιών εξωτερικής ανάθεσης.