					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P26					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**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρα 8	Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί τυπικούς ελέγχους για υπηρεσίες τρίτων μερών που επηρεάζουν το ISMS
ISO/IEC 27002:2022	Έλεγχοι 5.19–5.22	Πολιτική και διαδικασίες για σχέσεις με προμηθευτές· διαχείριση κινδύνων προμηθευτών· διαχείριση παροχής υπηρεσιών προμηθευτών· παρακολούθηση και ανασκόπηση προμηθευτών
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Υπηρεσίες εξωτερικών συστημάτων· διαχείριση διαμόρφωσης από προγραμματιστές· διασυνδέσεις συστημάτων· ασφάλεια προσωπικού τρίτων μερών
ΓΚΠΔ της ΕΕ	Άρθρα 28, 32, 33	Υποχρεώσεις εκτελούντος την επεξεργασία, ασφάλεια της επεξεργασίας, κοινοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(e–f)	Διαχείριση προμηθευτών βάσει κινδύνου και εποπτεία ασφάλειας
Κανονισμός DORA της ΕΕ	Άρθρα 28, 30	Κίνδυνος ΤΠΕ από τρίτα μέρη, εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ
COBIT 2019	BAI05, DSS02, MEA03	Διαχείριση της υποστήριξης οργανωτικών αλλαγών· διαχείριση αιτημάτων υπηρεσιών και περιστατικών· παρακολούθηση, αξιολόγηση και εκτίμηση της συμμόρφωσης

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις απαιτήσεις ασφάλειας πληροφοριών για τη σύναψη, διαχείριση και διατήρηση ασφαλών σχέσεων με τρίτους προμηθευτές και τρίτους παρόχους υπηρεσιών.

1.2 Διασφαλίζει ότι όλοι οι προμηθευτές που έχουν πρόσβαση σε δεδομένα, συστήματα ή υποδομές του οργανισμού υπόκεινται σε αυστηρούς ελέγχους ασφάλειας, συμβατικές δικλίδες ασφαλείας και συνεχή εποπτεία σε όλο τον κύκλο ζωής της υπηρεσίας.

1.3 Η πολιτική υποστηρίζει τους Ελέγχους 5.19 έως 5.22 του Παραρτήματος Α του ISO/IEC 27001, ενσωματώνοντας απαιτήσεις ασφάλειας στη διαδικασία προμηθειών, στη διαδικασία ένταξης, στη δέουσα επιμέλεια, στη διαχείριση συμβάσεων, στην παρακολούθηση υπηρεσιών και στις διαδικασίες τερματισμού.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλους τους τρίτους προμηθευτές, αναδόχους, παρόχους υπηρεσιών νέφους και οργανισμούς παροχής υπηρεσιών που επεξεργάζονται ή αποκτούν πρόσβαση σε πληροφοριακά περιουσιακά στοιχεία του οργανισμού

2.1.2 Όλους τους εσωτερικούς ρόλους που εμπλέκονται στην αξιολόγηση προμηθευτών, στη διαδικασία ένταξης, στη σύναψη συμβάσεων, στη διαχείριση κινδύνων, στην παρακολούθηση ή στον τερματισμό

2.1.3 Όλες τις σχέσεις με προμηθευτές που περιλαμβάνουν πρόσβαση σε ευαίσθητα δεδομένα, διασύνδεση με υπηρεσίες παραγωγής ή υποστήριξη κρίσιμων επιχειρησιακών λειτουργιών

2.2 Καλύπτει τόσο τους άμεσους προμηθευτές όσο και τους υπεργολάβους τους, όπου εφαρμόζεται, και περιλαμβάνει λογισμικό τρίτων, υποδομές, υποστήριξη και διαχειριζόμενες υπηρεσίες.

3. Στόχοι

3.1 Να διασφαλίζεται ότι οι κίνδυνοι ασφάλειας που συνδέονται με προμηθευτές αναγνωρίζονται, αξιολογούνται και μετριάζονται με συνέπεια σε όλο τον κύκλο ζωής της σχέσης.

3.2 Να ενσωματώνονται τυποποιημένες απαιτήσεις ασφάλειας σε όλες τις συμβάσεις προμηθευτών, συμπεριλαμβανομένων των υποχρεώσεων γνωστοποίησης παραβίασης, των ρητρών δικαιώματος ελέγχου και των αρμοδιοτήτων για την προστασία δεδομένων.

3.3 Να απαιτείται τυπική δέουσα επιμέλεια και τεκμηριωμένη αξιολόγηση κινδύνου πριν από τη συνεργασία με νέους προμηθευτές ή την ανανέωση συμφωνιών παροχής υπηρεσιών υψηλού κινδύνου.

3.4 Να θεσπίζονται μηχανισμοί για τη συνεχή παρακολούθηση της συμμόρφωσης των προμηθευτών, συμπεριλαμβανομένων των ανασκοπήσεων επιδόσεων, των ελέγχων και της κλιμάκωσης περιστατικών.

3.5 Να διαχειρίζονται οι αλλαγές στις υπηρεσίες προμηθευτών και να εφαρμόζεται ασφαλής διαδικασία αποχώρησης και επιστροφής/καταστροφής δεδομένων κατά τον τερματισμό.

3.6 Να ευθυγραμμίζονται οι έλεγχοι ασφάλειας τρίτων μερών με τις εφαρμοστέες κανονιστικές και συμβατικές υποχρεώσεις, συμπεριλαμβανομένων του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ, του Κανονισμού DORA της ΕΕ και του ISO/IEC 27001.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει την ευθυγράμμισή της με το συνολικό Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), το πλαίσιο διαχείρισης κινδύνων και τη στρατηγική συμμόρφωσης.

4.1.2 Εγκρίνει τις βαθμίδες ταξινόμησης προμηθευτών, τα αποτελέσματα ανασκοπήσεων ασφάλειας και τις εξαιρέσεις υψηλού κινδύνου.

4.1.3 Συμμετέχει στην κλιμάκωση σοβαρών περιστατικών προμηθευτών και στις διαπραγματεύσεις συμβάσεων για κρίσιμες υπηρεσίες.

4.2 Προμήθειες και διαχείριση προμηθευτών

4.2.1 Διασφαλίζουν ότι όλες οι νέες και ανανεωμένες συμβάσεις προμηθευτών ενσωματώνουν εγκεκριμένες ρήτρες ασφάλειας και προστασίας δεδομένων.

4.2.2 Τηρούν το κεντρικό μητρώο προμηθευτών και συντονίζονται με τη Νομική Υπηρεσία και τη Συμμόρφωση για την τεκμηρίωση του κινδύνου τρίτων μερών.

4.2.3 Εκκινούν τις διαδικασίες ένταξης και διασφαλίζουν την ευθυγράμμιση με τις αξιολογήσεις ασφάλειας πριν από τη σύναψη της σύμβασης.

[... 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 ή νωρίτερα σε περίπτωση:

9.1.1 Ουσιωδών αλλαγών στη στρατηγική προμηθειών ή στο οικοσύστημα προμηθευτών

9.1.2 Επικαιροποιήσεων σε νομικά ή κανονιστικά πλαίσια (π.χ. Κανονισμός DORA της ΕΕ, ΓΚΠΔ της ΕΕ)

9.1.3 Σημαντικών περιστατικών τρίτων μερών, παραβιάσεων δεδομένων ή αστοχιών ελέγχου

9.1.4 Ευρημάτων από αξιολόγηση κινδύνου ή από εξωτερικούς φορείς πιστοποίησης

9.2 Η διαδικασία ανασκόπησης ανήκει από κοινού στον Επικεφαλής Ασφάλειας Πληροφοριών (CISO), στις Προμήθειες, στη Νομική Υπηρεσία και στις λειτουργίες διαχείρισης κινδύνων.

9.3 Όλες οι αναθεωρήσεις της πολιτικής πρέπει να τεκμηριώνονται στο Μητρώο Ελέγχου Εγγράφων του ISMS, να υπόκεινται σε έλεγχο εκδόσεων και να γνωστοποιούνται στα σχετικά ενδιαφερόμενα μέρη μέσω των διαύλων διακυβέρνησης προμηθευτών και των προγραμμάτων ευαισθητοποίησης εργαζομένων.

9.4 Οι καταργημένες εκδόσεις πρέπει να αρχειοθετούνται για ελάχιστο διάστημα τριών ετών, για σκοπούς ιχνηλασιμότητας και νομικής συμμόρφωσης.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 – Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει τη συνολική δέσμευση για την ασφάλεια όλων των λειτουργιών του οργανισμού, συμπεριλαμβανομένης της εξάρτησης από τρίτους προμηθευτές και εξωτερικούς παρόχους υπηρεσιών.

10.2 P6 – Πολιτική Διαχείρισης Κινδύνων. Καθοδηγεί την αναγνώριση, αξιολόγηση και μείωση του κινδύνου που συνδέεται με σχέσεις τρίτων μερών, συμπεριλαμβανομένων των εγγενών ή συστημικών κινδύνων από οικοσυστήματα προμηθευτών.

10.3 P17 – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας. Εφαρμόζεται σε όλους τους προμηθευτές που χειρίζονται δεδομένα προσωπικού χαρακτήρα, απαιτώντας κατάλληλους συμβατικούς όρους, δικλίδες ασφαλείας διαβίβασης και αρχές προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό.

10.4 P4 – Πολιτική Ελέγχου Πρόσβασης. Ρυθμίζει τον τρόπο με τον οποίο το προσωπικό τρίτων μερών αποκτά πρόσβαση στα συστήματα του οργανισμού, εφαρμόζοντας δικαιώματα βάσει ρόλων, ελέγχους συνεδριών και διαδικασίες ανάκλησης.

10.5 P22 – Πολιτική Καταγραφής και Παρακολούθησης. Απαιτεί η πρόσβαση προμηθευτών σε συστήματα να παρακολουθείται, να καταγράφεται και να ανασκοπείται, ιδίως σε περιβάλλοντα όπου υφίστανται προνομιούχες δραστηριότητες ή δραστηριότητες επικεντρωμένες σε δεδομένα.

10.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών. Καθορίζει τις διαδικασίες κλιμάκωσης και τις απαιτήσεις αναφοράς παραβιάσεων για συμβάντα ασφάλειας που προέρχονται από προμηθευτές ή για κοινές διερευνήσεις που αφορούν συστήματα τρίτων μερών.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001: Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί τυπικούς ελέγχους για υπηρεσίες τρίτων μερών που επηρεάζουν το ISMS.

11.2 ISO/IEC 27002:2022 – Έλεγχοι 5.19 έως 5.22:

11.2.1 Έλεγχος 5.19 του Παραρτήματος Α – Πολιτική και διαδικασίες για σχέσεις με προμηθευτές: Επιβάλλει ελέγχους για τη διαχείριση αλληλεπιδράσεων με προμηθευτές.

11.2.2 Έλεγχος 5.20 του Παραρτήματος Α – Διαχείριση κινδύνων προμηθευτών: Εστιάζει στην αναγνώριση, αξιολόγηση και συνεχή εποπτεία της στάσης κινδύνου των προμηθευτών.

11.2.3 Έλεγχος 5.21 του Παραρτήματος Α – Διαχείριση παροχής υπηρεσιών προμηθευτών: Απαιτεί ευθυγράμμιση επιδόσεων και ασφάλειας με τις συμβατικές προσδοκίες.

11.2.4 Έλεγχος 5.22 του Παραρτήματος Α – Παρακολούθηση και ανασκόπηση προμηθευτών: Ενισχύει την ανάγκη για συνεχή επικύρωση και επανεξέταση της συμμόρφωσης τρίτων μερών.

11.3 NIST SP 800-53 Rev.:

11.3.1 SA-9 – Υπηρεσίες εξωτερικών συστημάτων: Καθορίζει απαιτήσεις ασφάλειας και κινδύνου για συστήματα που λειτουργούν από εξωτερικές οντότητες.

11.3.2 SA-10 – Διαχείριση διαμόρφωσης από προγραμματιστές: Εφαρμόζεται όταν τρίτα μέρη παραδίδουν λογισμικό ή περιβάλλοντα.

11.3.3 CA-3 – Διασυνδέσεις συστημάτων: Απαιτεί εποπτεία και συμφωνία για τις ροές δεδομένων συστημάτων μεταξύ οντοτήτων.

11.3.4 PS-7 – Ασφάλεια προσωπικού τρίτων μερών: Διασφαλίζει ότι οι ανάδοχοι και το προσωπικό προμηθευτών ελέγχονται και παρακολουθούνται κατάλληλα.

11.4 ΓΚΠΔ της ΕΕ (2016/679):

11.4.1 Άρθρο 28 – Υποχρεώσεις εκτελούντος την επεξεργασία: Απαιτεί έγγραφες συμφωνίες με τους εκτελούντες την επεξεργασία, συμπεριλαμβανομένων τεχνικών και οργανωτικών μέτρων.

11.4.2 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Επιβάλλει κατάλληλες δικλίδες ασφαλείας τόσο για υπευθύνους επεξεργασίας όσο και για εκτελούντες την επεξεργασία.

11.4.3 Άρθρο 33 – Κοινοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα: Απαιτεί άμεση κοινοποίηση από προμηθευτές σε περίπτωση παραβίασης.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555):

11.5.1 Άρθρο 21(2)(e–f): Απαιτεί διαχείριση προμηθευτών βάσει κινδύνου και εποπτεία ασφάλειας, ιδίως στις ψηφιακές αλυσίδες εφοδιασμού ουσιωδών και σημαντικών οντοτήτων.

11.6 Κανονισμός DORA της ΕΕ (2022/2554):

11.6.1 Άρθρο 28 – Κίνδυνος ΤΠΕ από τρίτα μέρη: Επιβάλλει υποχρεώσεις για αξιολόγηση κινδύνου, συμβατικούς όρους ασφάλειας και στρατηγικές εξόδου για παρόχους χρηματοοικονομικών υπηρεσιών.

11.6.2 Άρθρο 30 – Εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ: Καθιερώνει ενισχυμένες απαιτήσεις παρακολούθησης και εποπτείας για βασικούς προμηθευτές.

11.7 COBIT 2019:

11.7.1 BAI05 – Διαχείριση της υποστήριξης οργανωτικών αλλαγών: Διασφαλίζει ότι οι μεταβάσεις μεταξύ προμηθευτών διέπονται από ασφαλή διακυβέρνηση.

11.7.2 DSS02 – Διαχείριση αιτημάτων υπηρεσιών και περιστατικών: Εφαρμόζεται σε ζητήματα που αναφέρονται από προμηθευτές και στην ενσωμάτωση του χειρισμού περιστατικών.

11.7.3 MEA03 – Παρακολούθηση, αξιολόγηση και εκτίμηση της συμμόρφωσης: Ενισχύει τη μέτρηση επιδόσεων προμηθευτών και την παρακολούθηση της συμμόρφωσης.