					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P27					Τίτλος εγγράφου: **Πολιτική Χρήσης Υπηρεσιών Υπολογιστικού Νέφους**							
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	Clause 8	Απαιτήσεις επιχειρησιακού σχεδιασμού και ελέγχου για το περιβάλλον υπολογιστικού νέφους.
ISO/IEC 27002:2022	Controls 5.23–5.25	Απαιτήσεις για τη χρήση, την πολιτική και την ασφάλεια των υπηρεσιών νέφους.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Χρήση εξωτερικών συστημάτων, συμβατικές και τεχνικές απαιτήσεις, κρυπτογραφικές προστασίες, προστασία εφοδιαστικής αλυσίδας.
ΓΚΠΔ της ΕΕ	Articles 28, 32, Chapter V	Απαιτήσεις για εκτελούντες την επεξεργασία σε περιβάλλον νέφους, ασφάλεια της επεξεργασίας, διαβιβάσεις δεδομένων.
Οδηγία NIS2 της ΕΕ	Article 21(2)(f, i)	Απαιτήσεις για τον κίνδυνο τρίτων μερών και την εφοδιαστική αλυσίδα.
Κανονισμός DORA της ΕΕ	Articles 5(2), 28	Εποπτεία κινδύνων ΤΠΕ και τρίτων μερών (υπολογιστικού νέφους) για χρηματοοικονομικές οντότητες.
COBIT 2019	BAI04, DSS01, DSS05	Διαθεσιμότητα υπηρεσιών νέφους, λειτουργίες και διαχείριση ασφάλειας.

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις υποχρεωτικές απαιτήσεις του οργανισμού για την ασφαλή, συμμορφούμενη και υπεύθυνη χρήση υπηρεσιών υπολογιστικού νέφους στα μοντέλα παροχής Infrastructure as a Service (IaaS), Platform as a Service (PaaS) και Software as a Service (SaaS).

1.2 Η πολιτική αποσκοπεί στη διασφάλιση ότι οι υπηρεσίες νέφους υιοθετούνται και διέπονται από κατάλληλο πλαίσιο διακυβέρνησης, με τρόπο που προστατεύει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριακών περιουσιακών στοιχείων, ενώ παράλληλα καλύπτει κανονιστικές, νομικές και συμβατικές υποχρεώσεις.

1.3 Ορίζει ελέγχους για τη διαχείριση του κινδύνου που συνδέεται με το νέφος, την προστασία δεδομένων, την παρακολούθηση της συμμόρφωσης των παρόχων και την εξάλειψη μη εξουσιοδοτημένης χρήσης. Υποστηρίζει επίσης την επιχειρησιακή καινοτομία μέσω πλατφορμών νέφους, ευθυγραμμίζοντας την ασφάλεια, τη λειτουργική αξιοπιστία και τη σχέση κόστους-αποτελεσματικότητας.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλους τους εργαζομένους, αναδόχους, τρίτους παρόχους υπηρεσιών και εξωτερικούς συμβούλους που προμηθεύονται, ρυθμίζουν, προσπελαύνουν, διαχειρίζονται ή χρησιμοποιούν υπηρεσίες νέφους για λογαριασμό του οργανισμού.

2.2 Εφαρμόζεται σε όλα τα περιβάλλοντα όπου υποβάλλονται σε επεξεργασία δεδομένα ή φόρτοι εργασίας του οργανισμού, συμπεριλαμβανομένων των εξής:

2.2.1 Αναπτύξεις δημόσιου, ιδιωτικού, υβριδικού και κοινοτικού νέφους

2.2.2 Όλα τα μοντέλα υπηρεσιών νέφους (IaaS, PaaS, SaaS)

2.2.3 Αρχιτεκτονικές πολλαπλού νέφους και ομοσπονδιοποιημένες αρχιτεκτονικές

2.2.4 Χρήση σκιώδους πληροφορικής (shadow IT) ή προσωπικών λογαριασμών νέφους για επιχειρησιακούς σκοπούς

2.3 Καλύπτει όλα τα επίπεδα ταξινόμησης δεδομένων και εφαρμόζεται τόσο σε εσωτερικά συστήματα όσο και σε πλατφόρμες που φιλοξενούνται από προμηθευτές, όπου αποθηκεύονται ή υποβάλλονται σε επεξεργασία δεδομένα ιδιοκτησίας του οργανισμού ή ρυθμιζόμενα δεδομένα.

3. Στόχοι

3.1 Να διασφαλίζεται η ασφαλής και συνεπής χρήση τεχνολογιών νέφους μέσω σαφώς καθορισμένων οδηγιών χρήσης, βασικών γραμμών ασφάλειας και ρόλων διακυβέρνησης.

3.2 Να ελαχιστοποιούνται οι λειτουργικοί και κανονιστικοί κίνδυνοι που συνδέονται με το υπολογιστικό νέφος, συμπεριλαμβανομένων της μη εξουσιοδοτημένης πρόσβασης, των παραβιάσεων δεδομένων, της εσφαλμένης διαμόρφωσης, της μη συμμόρφωσης και της διακοπής υπηρεσιών.

3.3 Να εφαρμόζονται απαιτήσεις ασφάλειας και ιδιωτικότητας για όλους τους παρόχους νέφους και να επαληθεύεται η συμμόρφωση μέσω συμβατικών ρητρών, αξιολογήσεων και δικαιωμάτων ελέγχου.

3.4 Να καθίσταται δυνατή η κλιμακούμενη και ανθεκτική υιοθέτηση υπηρεσιών νέφους χωρίς συμβιβασμό του προφίλ κινδύνου, των νομικών απαιτήσεων ή της επιχειρησιακής συνέχειας.

3.5 Να ευθυγραμμίζονται η διακυβέρνηση και η χρήση του νέφους με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) του οργανισμού, τις νομικές υποχρεώσεις (π.χ. ΓΚΠΔ της ΕΕ, Κανονισμός DORA της ΕΕ), τις κλαδικές οδηγίες και τις αναγνωρισμένες βέλτιστες πρακτικές του κλάδου (π.χ. NIST, COBIT).

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Εγκρίνει την Πολιτική Χρήσης Υπηρεσιών Υπολογιστικού Νέφους και τον στρατηγικό οδικό χάρτη υιοθέτησης υπηρεσιών νέφους.

4.1.2 Ανασκοπεί και εγκρίνει εξαιρέσεις υψηλού κινδύνου από τις τυπικές απαιτήσεις διακυβέρνησης νέφους.

4.1.3 Διασφαλίζει ότι οι πρωτοβουλίες νέφους λαμβάνουν επαρκή χρηματοδότηση, εποπτεία και ενσωμάτωση στα εταιρικά πλαίσια διαχείρισης κινδύνων.

4.2 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.2.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και του οργανωσιακού Μητρώου Υπηρεσιών Νέφους.

4.2.2 Εγκρίνει την ένταξη νέων παρόχων νέφους βάσει δέουσας επιμέλειας και αξιολόγησης κινδύνου.

4.2.3 Ανασκοπεί την τεκμηρίωση συμμόρφωσης των παρόχων και επικυρώνει την ευθυγράμμιση με τις απαιτήσεις ασφάλειας.

[... 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 και να επικαιροποιείται, όπου απαιτείται, ώστε να διασφαλίζεται η συνεχής ευθυγράμμιση με:

9.1.1 εξελισσόμενες νομικές και κανονιστικές απαιτήσεις (π.χ. ΓΚΠΔ της ΕΕ, Οδηγία NIS2 της ΕΕ, Κανονισμός DORA της ΕΕ)

9.1.2 αλλαγές στα πρότυπα ISO/IEC 27001 ή ISO/IEC 27002

9.1.3 επικαιροποιήσεις στην αρχιτεκτονική νέφους, στο τοπίο απειλών ή στο χαρτοφυλάκιο υπηρεσιών του οργανισμού

9.1.4 διερευνήσεις περιστατικών, αποτελέσματα ελέγχων ή διδάγματα από τη λειτουργική χρήση

9.2 Ο CISO είναι υπεύθυνος για την έναρξη της ανασκόπησης και τη σύγκληση των συναφών ενδιαφερόμενων μερών, συμπεριλαμβανομένων των εξής:

9.2.1 Αρχιτέκτονας Ασφάλειας Νέφους

9.2.2 Ομάδα Νομικής και Συμμόρφωσης

9.2.3 Υπεύθυνοι Προμηθειών και διαχειριστές προμηθευτών

9.2.4 Ιδιοκτήτες υπηρεσιών και Λειτουργίες Πληροφορικής

9.3 Όλες οι επικαιροποιήσεις πρέπει:

9.3.1 να ελέγχονται ως προς την έκδοση και να φέρουν ημερομηνία

9.3.2 να εγκρίνονται από την Ανώτατη Διοίκηση

9.3.3 να κοινοποιούνται στα επηρεαζόμενα μέρη, συμπεριλαμβανομένων εργαζομένων, αναδόχων και τρίτων μερών

9.3.4 να αρχειοθετούνται σύμφωνα με τις εσωτερικές πολιτικές τεκμηρίωσης

9.4 Ενδιάμεσες ανασκοπήσεις μπορούν να ενεργοποιούνται από:

9.4.1 νέες συνεργασίες με παρόχους υπηρεσιών νέφους (CSP) ή σημαντικές μετεγκαταστάσεις

9.4.2 αναδυόμενες απειλές για την υποδομή νέφους

9.4.3 ουσιώδεις μεταβολές σε συμβατικές, νομικές ή κλαδικές υποχρεώσεις

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική συνδέεται στενά και εξαρτάται από τις ακόλουθες εσωτερικές πολιτικές:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις υπερκείμενες αρχές που διέπουν την ασφαλή λειτουργία συστημάτων και υπηρεσιών, τις οποίες η παρούσα πολιτική εφαρμόζει στο πλαίσιο του νέφους.

10.1.2 P5 – Πολιτική Διαχείρισης Αλλαγών: Όλες οι αλλαγές διαμόρφωσης σε περιβάλλον νέφους πρέπει να ακολουθούν τις διαδικασίες ελέγχου αλλαγών που ορίζονται στην P5.

10.1.3 P13 – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθορίζει τον τρόπο αξιολόγησης των δεδομένων πριν από τη μεταφορά τους στο νέφος και τον τρόπο εφαρμογής ελέγχων όπως η κρυπτογράφηση και η τοποθεσία αποθήκευσης.

10.1.4 P18 – Πολιτική Κρυπτογραφικών Ελέγχων: Παρέχει πρότυπα για την κρυπτογράφηση, τη διαχείριση κλειδιών και τη χρήση κρυπτογραφικών αλγορίθμων, τα οποία εφαρμόζονται άμεσα στις διαμορφώσεις των υπηρεσιών νέφους.

10.1.5 P22 – Πολιτική Καταγραφής και Παρακολούθησης: Καθορίζει απαιτήσεις για τη συλλογή, τη διατήρηση και την ανάλυση αρχείων καταγραφής, οι οποίες πρέπει να εφαρμόζονται σε περιβάλλοντα νέφους.

10.1.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών: Ορίζει διαδικασίες κλιμάκωσης, περιορισμού και αποκατάστασης για περιστατικά ασφάλειας που σχετίζονται με το νέφος.

10.1.7 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Υποστηρίζει την ετοιμότητα για έλεγχο και τη συνεχή διασφάλιση ότι οι έλεγχοι νέφους εφαρμόζονται και παρακολουθούνται.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001: Clause 8.1 – Operational Planning and Control: Απαιτεί από τους οργανισμούς να εφαρμόζουν και να ελέγχουν τις διεργασίες που απαιτούνται για την ικανοποίηση των απαιτήσεων ασφάλειας πληροφοριών, συμπεριλαμβανομένων εκείνων που αφορούν περιβάλλοντα νέφους.

11.2 ISO/IEC 27002:2022 – Controls 5.23 to 5.25:

11.2.1 Annex A Control 5.23 – Use of Cloud Services: Απαιτεί αξιολόγηση βάσει κινδύνου, επίσημη εξουσιοδότηση και τεκμηρίωση της χρήσης υπηρεσιών νέφους.

11.2.2 Annex A Control 5.24 – Cloud Use Policy: Απαιτεί τη θέσπιση και εφαρμογή επίσημων πολιτικών χρήσης υπηρεσιών νέφους, ευθυγραμμισμένων με τις ανάγκες και τους κινδύνους του οργανισμού.

11.2.3 Annex A Control 5.25 – Security in Cloud Services: Επιβάλλει την ενσωμάτωση της ασφάλειας, των συμβατικών προστασιών και της παρακολούθησης των φόρτων εργασίας και των δεδομένων που φιλοξενούνται σε περιβάλλον νέφους.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Use of External Systems: Απαιτεί καθορισμένους κανόνες και όρους για την πρόσβαση σε πόρους του οργανισμού από εξωτερικά ή βασισμένα σε περιβάλλον νέφους συστήματα.

11.3.2 SA-9(5) – External Information System Services: Επιβάλλει συμβατικές απαιτήσεις ασφάλειας, εποπτεία και συνεχή παρακολούθηση της συμμόρφωσης για συστήματα νέφους τρίτων μερών.

11.3.3 SC-12 to SC-28 – Cryptographic Protections, Boundary Defense, and Transmission Integrity: Ευθυγραμμίζονται με απαιτήσεις κρυπτογράφησης, ταυτότητας και πρόσβασης για υπηρεσίες που φιλοξενούνται σε περιβάλλον νέφους και για δεδομένα σε μεταφορά.

11.3.4 SR-5 – Supply Chain Protection: Υποστηρίζει την αξιολόγηση και τον συμβατικό έλεγχο των παρόχων υπηρεσιών νέφους (CSP) που συμμετέχουν στην παροχή υπηρεσιών.

11.4 ΓΚΠΔ της ΕΕ (2016/679):

11.4.1 Article 28 – Processor Obligations: Απαιτεί επίσημες συμβάσεις με παρόχους νέφους για τη διασφάλιση της ασφάλειας, της εμπιστευτικότητας και της δυνατότητας ελέγχου της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

11.4.2 Article 32 – Security of Processing: Υποστηρίζει την εφαρμογή κρυπτογράφησης, ελέγχων πρόσβασης, καταγραφής και άλλων δικλίδων ασφαλείας σε περιβάλλοντα νέφους.

11.4.3 Chapter V – International Data Transfers: Επιβάλλει τη νόμιμη διαβίβαση δεδομένων εκτός ΕΕ/ΕΟΧ με χρήση δικλίδων ασφαλείας όπως οι Τυποποιημένες Συμβατικές Ρήτρες (SCCs) ή αποφάσεις επάρκειας.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555):

11.5.1 Article 21(2)(f, i): Απαιτεί από τις οντότητες να διαχειρίζονται τους κινδύνους από τρίτους παρόχους υπηρεσιών νέφους και να διασφαλίζουν την ακεραιότητα της ψηφιακής εφοδιαστικής αλυσίδας μέσω συμβατικών και τεχνικών μέτρων.

11.6 Κανονισμός DORA της ΕΕ (2022/2554):

11.6.1 Article 5(2) – Governance of ICT Risks: Επιβάλλει την ενσωμάτωση του κινδύνου ΤΠΕ από τρίτα μέρη, συμπεριλαμβανομένων των υπηρεσιών νέφους, στη συνολική διακυβέρνηση κινδύνων.

11.6.2 Article 28 – Oversight of Critical ICT Third-Party Providers: Απαιτεί από τις χρηματοοικονομικές οντότητες να παρακολουθούν, να ελέγχουν και να αναφέρουν τις εξαρτήσεις από παρόχους νέφους, το επίπεδο ασφάλειας και την ανθεκτικότητά τους.

11.7 COBIT 2019:

11.7.1 BAI04 – Manage Availability and Capacity: Διασφαλίζει ότι οι υπηρεσίες νέφους είναι ανθεκτικές, παρακολουθούνται και πληρούν καθορισμένα κριτήρια απόδοσης.

11.7.2 DSS01 – Manage Operations: Υποστηρίζει την επιχειρησιακή ενσωμάτωση, τον χειρισμό περιστατικών και τις βασικές γραμμές διαμόρφωσης σε πλατφόρμες που φιλοξενούνται σε περιβάλλον νέφους.

11.7.3 DSS05 – Manage Security Services: Καθοδηγεί την εφαρμογή ελέγχων ασφάλειας ειδικών για το νέφος, την παρακολούθηση και την πρόληψη περιστατικών σε ψηφιακές υπηρεσίες.