					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου						
Αριθμός εγγράφου: P27S					Τίτλος εγγράφου: **Πολιτική Χρήσης Υπηρεσιών 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	Ρήτρα 8	
ISO/IEC 27002:2022	Έλεγχοι 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
ΓΚΠΔ της ΕΕ	Άρθρα 28, 32 και Κεφάλαιο V	
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(f), (i)	
Κανονισμός DORA της ΕΕ	Άρθρα 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο επιτρέπεται η ασφαλής χρήση υπηρεσιών νέφους εντός του οργανισμού. Διασφαλίζει ότι τα δεδομένα που υποβάλλονται σε επεξεργασία ή αποθηκεύονται σε υπηρεσίες νέφους προστατεύονται, ότι ο έλεγχος πρόσβασης εφαρμόζεται κατάλληλα και ότι οι σχετικοί κίνδυνοι αντιμετωπίζονται υπεύθυνα.

1.2 Υποστηρίζει τις ΜΜΕ στην εκπλήρωση των νομικών τους υποχρεώσεων και των προσδοκιών των πελατών για την προστασία ευαίσθητων πληροφοριών, την πρόληψη διαρροής δεδομένων και την αποτελεσματική διαχείριση κινδύνων που σχετίζονται με πλατφόρμες νέφους, χωρίς να απαιτείται υποδομή επιχειρησιακής κλίμακας.

1.3 Η παρούσα πολιτική υποστηρίζει την πιστοποίηση κατά ISO/IEC 27001, τη συμμόρφωση με τον ΓΚΠΔ της ΕΕ και τη διασφάλιση της εφοδιαστικής αλυσίδας μέσω συνεπούς διακυβέρνησης όλων των τρίτων παρόχων υπηρεσιών νέφους.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται:

2.1.1 Σε κάθε υπηρεσία νέφους που χρησιμοποιείται για την αποθήκευση, επεξεργασία ή διαβίβαση εταιρικών δεδομένων

2.1.2 Σε όλο το προσωπικό, τους αναδόχους και τους παρόχους υπηρεσιών που χρησιμοποιούν εργαλεία νέφους για λογαριασμό του οργανισμού

2.1.3 Σε δωρεάν και συνδρομητικές λύσεις νέφους, συμπεριλαμβανομένων πλατφορμών ηλεκτρονικού ταχυδρομείου, διαμοιρασμού εγγράφων, εργαλείων SaaS, πλατφορμών αντιγράφων ασφαλείας, τηλεδιασκέψεων και πλατφορμών πελατών

2.1.4 Σε κάθε συσκευή (σταθερό υπολογιστή, κινητή συσκευή, tablet) που αποκτά πρόσβαση σε εταιρικές πληροφορίες μέσω εφαρμογών νέφους

2.2 Αυτό περιλαμβάνει, ενδεικτικά και όχι περιοριστικά:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 Εργαλεία αντιγράφων ασφαλείας και αποκατάστασης από καταστροφή που βασίζονται σε νέφος

2.2.5 Κοινόχρηστους φακέλους ή εφαρμογές που χρησιμοποιούνται για τιμολόγηση, διαχείριση έργων ή επικοινωνία με πελάτες

3. Στόχοι

3.1 Να αποτρέπεται η μη εξουσιοδοτημένη ή υψηλού κινδύνου χρήση μη εγκεκριμένων υπηρεσιών νέφους.

3.2 Να διασφαλίζεται ότι τα ευαίσθητα ή κανονιστικά ρυθμιζόμενα δεδομένα που αποθηκεύονται σε υπηρεσίες νέφους προστατεύονται με κατάλληλα τεχνικά και οργανωτικά μέτρα.

3.3 Να ορίζονται σαφείς ρόλοι για την έγκριση, τη διαμόρφωση, την παρακολούθηση και την απόσυρση υπηρεσιών νέφους.

3.4 Να ελέγχονται οι ροές δεδομένων και να εφαρμόζονται οι υποχρεώσεις διατήρησης, διαγραφής και προστασίας της ιδιωτικότητας για πληροφορίες που αποθηκεύονται σε υπηρεσίες νέφους.

3.5 Να μειώνεται η εξάρτηση από προσωπικούς λογαριασμούς ή μη ιχνηλάσιμα εργαλεία, με υποχρεωτική έγκριση όλων των συστημάτων νέφους που χρησιμοποιούνται για επιχειρησιακούς σκοπούς.

3.6 Να τηρούνται οι απαιτήσεις των ISO/IEC 27001:2022, ΓΚΠΔ της ΕΕ, Οδηγίας NIS2 της ΕΕ και Κανονισμού DORA της ΕΕ για τη διαχείριση εξωτερικών εξαρτήσεων από υπηρεσίες νέφους.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Εγκρίνει τη χρήση όλων των νέων υπηρεσιών νέφους

4.1.2 Ανασκοπεί τους κινδύνους που σχετίζονται με παρόχους υπηρεσιών νέφους και τύπους υπηρεσιών

4.1.3 Διασφαλίζει την εφαρμογή της πολιτικής και ασκεί εποπτεία στις αποφάσεις περί εξαιρέσεων

4.2 Εξωτερικός πάροχος υπηρεσιών πληροφορικής ή τεχνική υποστήριξη

4.2.1 Αξιολογεί και υλοποιεί ασφαλή διαμόρφωση για υπηρεσίες νέφους

4.2.2 Ρυθμίζει λογαριασμούς, ελέγχους πρόσβασης και αντίγραφα ασφαλείας

4.2.3 Παρακολουθεί τη συμμόρφωση με την πολυπλοκότητα κωδικών πρόσβασης, τον πολυπαραγοντικό έλεγχο ταυτότητας και τις ρυθμίσεις 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 από τον Γενικό Διευθυντή, σε συντονισμό με τον Εξωτερικό πάροχο υπηρεσιών πληροφορικής.

9.2 Επίσημη ανασκόπηση πρέπει επίσης να πραγματοποιείται:

9.2.1 Μετά από περιστατικό ασφάλειας που σχετίζεται με υπηρεσίες νέφους (π.χ. παραβίαση, απώλεια δεδομένων)

9.2.2 Όταν εισάγεται νέα κύρια πλατφόρμα νέφους

9.2.3 Εάν μεταβληθούν νομικές ή κανονιστικές απαιτήσεις (π.χ. επικαιροποιήσεις του ΓΚΠΔ της ΕΕ, της NIS2 ή του DORA)

9.2.4 Εάν οι δραστηριότητες παρακολούθησης αποκαλύψουν κακή χρήση ή νέους κινδύνους

9.3 Ο GM πρέπει να διασφαλίζει ότι:

9.3.1 Το Μητρώο Υπηρεσιών Νέφους επικαιροποιείται με νέες ή αποσυρμένες υπηρεσίες

9.3.2 Οι νομικές απαιτήσεις και οι απαιτήσεις ιδιωτικότητας εξακολουθούν να τηρούνται

9.3.3 Όλες οι αλλαγές γνωστοποιούνται στους σχετικούς χρήστες και στα ενδιαφερόμενα μέρη

9.4 Οι αρχειοθετημένες προηγούμενες εκδόσεις πρέπει να αποθηκεύονται με ασφαλή τρόπο και οι παλαιές εκδόσεις της πολιτικής πρέπει να διαχειρίζονται σύμφωνα με την P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων του οργανισμού.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική πρέπει να χρησιμοποιείται σε συντονισμό με τις ακόλουθες πολιτικές ασφάλειας πληροφοριών ευθυγραμμισμένες με ΜΜΕ:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τη λογοδοσία για την έγκριση υπηρεσιών νέφους και τη διαχείριση σχέσεων με παρόχους.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Υποστηρίζει ασφαλείς πρακτικές σύνδεσης, διαχείρισης συνεδριών και ανάκλησης πρόσβασης που απαιτούνται για πλατφόρμες νέφους.

10.1.3 P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Διέπει τον τρόπο με τον οποίο τα δεδομένα σε νέφος δημιουργούν αντίγραφα ασφαλείας, διατηρούνται και διαγράφονται σύμφωνα με τις νομικές υποχρεώσεις.

10.1.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι κάθε δεδομένο προσωπικού χαρακτήρα που αποθηκεύεται σε υπηρεσίες νέφους υφίσταται χειρισμό σύμφωνα με τις αρχές του ΓΚΠΔ της ΕΕ.

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Παρέχει δομημένες διαδικασίες για την απόκριση σε περιστατικά ασφάλειας που σχετίζονται με υπηρεσίες νέφους, συμπεριλαμβανομένης της συλλογής τεκμηρίων και της εξωτερικής γνωστοποίησης.

10.2 Οι πολιτικές αυτές, από κοινού, διασφαλίζουν ότι η χρήση υπηρεσιών νέφους είναι ασφαλής, συμμορφούμενη και λειτουργικά ανθεκτική.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 8.1 – Απαιτεί από τους οργανισμούς να εφαρμόζουν επιχειρησιακούς ελέγχους για τις πρακτικές διαχείρισης δεδομένων, συμπεριλαμβανομένων εκείνων που σχετίζονται με συστήματα νέφους.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 5.23 – Επιβάλλει διακυβέρνηση για τη χρήση υπηρεσιών νέφους και εργαλείων SaaS τρίτων μερών.

11.2.2 Έλεγχος 5.24 – Απαιτεί καθορισμένη πολιτική χρήσης υπηρεσιών νέφους ευθυγραμμισμένη με τον κίνδυνο και τις κανονιστικές απαιτήσεις.

11.2.3 Έλεγχος 5.25 – Απαιτεί από τους οργανισμούς να διασφαλίζουν ότι οι έλεγχοι ασφάλειας σε περιβάλλοντα νέφους καλύπτουν τις ανάγκες του οργανισμού.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – Απαιτεί επίσημες πολιτικές χρήσης για εξωτερικά συστήματα όπως οι υπηρεσίες νέφους.

11.3.2 SC-12, SC-13 – Αφορούν την κρυπτογράφηση για δεδομένα κατά τη μεταφορά και δεδομένα σε αποθήκευση εντός περιβαλλόντων νέφους.

11.3.3 SR-5 – Καλύπτει ελέγχους κινδύνου για υπηρεσίες νέφους και τρίτα μέρη εντός της εφοδιαστικής αλυσίδας.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 28 – Απαιτεί από παρόχους νέφους που ενεργούν ως εκτελούντες την επεξεργασία να τηρούν δεσμευτικές συμβατικές υποχρεώσεις.

11.4.2 Άρθρο 32 – Επιβάλλει τεχνικά και οργανωτικά μέτρα για την επεξεργασία δεδομένων σε περιβάλλον νέφους.

11.4.3 Κεφάλαιο V – Απαγορεύει μη εξουσιοδοτημένες διεθνείς διαβιβάσεις δεδομένων προσωπικού χαρακτήρα που αποθηκεύονται σε υπηρεσίες νέφους.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(f), (i) – Απαιτεί από ουσιώδεις και σημαντικές οντότητες να εφαρμόζουν κατάλληλες πολιτικές για την ασφάλεια υπηρεσιών νέφους και τον έλεγχο της εφοδιαστικής αλυσίδας.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 5(2) – Απαιτεί από χρηματοοικονομικές ΜΜΕ να ενσωματώνουν την ασφάλεια υπηρεσιών νέφους στα πλαίσια διαχείρισης κινδύνων ΤΠΕ.

11.6.2 Άρθρο 28 – Θεσπίζει κανόνες εποπτείας για κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των προμηθευτών υπηρεσιών νέφους.

11.7 COBIT 2019

11.7.1 DSS01 – «Διαχείριση λειτουργιών» καλύπτει τη λειτουργική ακεραιότητα των υπηρεσιών νέφους.

11.7.2 DSS05 – «Διαχείριση υπηρεσιών ασφάλειας» περιλαμβάνει μέτρα προστασίας και παρακολούθηση ειδικά για υπηρεσίες νέφους.

11.7.3 BAI04 – «Διαχείριση διαθεσιμότητας και χωρητικότητας» διασφαλίζει επιχειρησιακή συνέχεια και απόδοση σε περιβάλλοντα νέφους.