

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

YSOFT ΠΛΗΡΟΦΟΡΙΚΗ Α.Ε.

Πλαίσιο: ISO/IEC 27001:2022 ρήτρα 5.2 και A.5.1 · ISO/IEC 27701 · ΓΚΠΔ άρθρο 24

Κωδικός εγγράφου: YS-ISMS-POL-00 (πρώην ΔΚ-ΔΔ01-01)

Έκδοση: 2.0 — Οκτώβριος 2026

Σοφούλη Θεμιστοκλή 28, 546 55 Θεσσαλονίκη · ΑΦΜ 800822138 · Δ.Ο.Υ. ΦΑΕ Θεσσαλονίκης · ΓΕΜΗ 142127506000

ΤΙΤΛΟΣ ΕΓΓΡΑΦΟΥ	Πολιτική Ασφάλειας Πληροφοριών
ΕΙΔΟΣ ΕΓΓΡΑΦΟΥ	Πολιτική ανώτατου επιπέδου του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) και του Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας (ΣΔΠΠ)
ΚΩΔΙΚΟΣ ΕΓΓΡΑΦΟΥ	YS-ISMS-POL-00
ΟΝΟΜΑ ΑΡΧΕΙΟΥ	YSOFT_ISMS_POL-00_Information-Security-Policy_v2.0.docx
ΘΕΣΗ ΣΤΟ ΑΠΟΘΕΤΗΡΙΟ	ISO › 11_ISO27001-27701 › 01_Current (PIMS_27701 και ISMS)
ΕΚΔΟΣΗ	2.0 — αντικαθιστά την έκδοση 1.0 της 01/02/2022 (ΔΚ-ΔΔ01-01)
ΗΜΕΡΟΜΗΝΙΑ	11/10/2026
ΔΙΑΒΑΘΜΙΣΗ	Δημόσιο — κοινοποιείται σε όλο το προσωπικό και διατίθεται σε κάθε ενδιαφερόμενο μέρος

ΣΥΝΤΑΞΗ	ΕΓΚΡΙΣΗ
Υπεύθυνος Συστήματος ΣΔΑΠ / ΣΔΠΠ YSOFT ΠΛΗΡΟΦΟΡΙΚΗ Α.Ε.	Διοίκηση YSOFT ΠΛΗΡΟΦΟΡΙΚΗ Α.Ε. Θεόφιλος Μυλωνάς, Πρόεδρος & Διευθύνων Σύμβουλος

ΔΗΛΩΣΗ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ. Η πολιτική είναι δημόσιο έγγραφο και μπορεί να δοθεί σε πελάτες, συνεργάτες και αρχές. Οι θεματικές πολιτικές και τα πρότυπα στα οποία παραπέμπει είναι εσωτερικά έγγραφα.

Περιεχόμενα

Πίνακας Επανεκδόσεων

ΕΚΔΟΣΗ	ΗΜΕΡ/ΝΙΑ	ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΑΛΛΑΓΗΣ	ΕΓΚΡΙΣΗ
1.0	01/02/2022	Πρώτη έκδοση (κωδ. ΔΚ-ΔΔ01/01), στο όνομα «ΥSS ΙΚΕ», κατά ISO 27001:2013, έδρα Ν. Ζέρβα 10.	Υπ. Συστήματος
2.0	11/10/2026	Πλήρης αναθεώρηση: επωνυμία YSOFT ΠΛΗΡΟΦΟΡΙΚΗ Α.Ε., έδρα Σοφούλη Θεμιστοκλή 28, ISO/IEC 27001:2022 και ISO/IEC 27701. Νέα κεφάλαια: πλαίσιο στόχων με μετρήσιμους στόχους, ρόλοι, ρόλος της YSOFT ως εκτελούσας (Renticom, έργα πελατών), χάρτης θεματικών πολιτικών, προμηθευτές και cloud, τεχνητή νοημοσύνη, δεσμεύσεις συμμόρφωσης και συνεχούς βελτίωσης. Αφαιρέθηκαν οι αρχές προστασίας δεδομένων, που μεταφέρθηκαν στην Πολιτική Προστασίας Προσωπικών Δεδομένων (YS-PIMS-POL-01).	Διοίκηση

1. Σκοπός και δέσμευση της Διοίκησης

Η YSOFT ΠΛΗΡΟΦΟΡΙΚΗ Α.Ε. («YSOFT» ή «η Εταιρεία») αναπτύσσει, υποστηρίζει και λειτουργεί πληροφοριακά συστήματα για πελάτες του δημόσιου και του ιδιωτικού τομέα και παρέχει την πλατφόρμα SaaS Renticom σε εταιρείες ενοικίασης οχημάτων. Οι πελάτες μας εμπιστεύονται σε εμάς τα συστήματα και τα δεδομένα τους· η ασφάλεια των πληροφοριών είναι επομένως προϋπόθεση της δουλειάς μας και όχι πρόσθετη υπηρεσία.

Η Διοίκηση της YSOFT δεσμεύεται:

- να προστατεύει την **εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα** των πληροφοριών της Εταιρείας, των πελατών και των συνεργατών της, ανάλογα με τον κίνδυνο·
- να προστατεύει την **ιδιωτικότητα** των φυσικών προσώπων των οποίων τα δεδομένα επεξεργάζεται, είτε ως υπεύθυνη επεξεργασίας είτε ως εκτελούσα για λογαριασμό πελατών·
- να **τηρεί τις εφαρμοστέες απαιτήσεις**: νομοθεσία, κανονισμούς, συμβατικές υποχρεώσεις προς πελάτες και τις απαιτήσεις των προτύπων ISO/IEC 27001 και ISO/IEC 27701·
- να διαθέτει τους **πόρους** (ανθρώπους, χρόνο, εργαλεία, εκπαίδευση) που χρειάζεται το Σύστημα Διαχείρισης·
- να **βελτιώνει συνεχώς** την αποτελεσματικότητα του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) και του Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας (ΣΔΠΠ).

2. Πεδίο εφαρμογής

Η πολιτική εφαρμόζεται σε όλες τις πληροφορίες, σε ηλεκτρονική ή έντυπη μορφή, σε όλα τα πληροφοριακά συστήματα και τις υπηρεσίες cloud, στα γραφεία της Σοφούλη Θεμιστοκλή 28 στη Θεσσαλονίκη, στην τηλεργασία και στους χώρους πελατών. Δεσμεύει τη Διοίκηση, όλους τους εργαζόμενους και κάθε εξωτερικό συνεργάτη, υπεργολάβο ή προμηθευτή που έχει πρόσβαση σε πληροφορίες της YSOFT ή των πελατών της.

Το πεδίο του πιστοποιημένου Συστήματος Διαχείρισης είναι:

Ανάλυση, ανάπτυξη, ενοποίηση, δοκιμή, εγκατάσταση και συντήρηση εφαρμογών λογισμικού και ολοκληρωμένων πληροφοριακών συστημάτων. Παροχή συμβουλευτικών και υποστηρικτικών υπηρεσιών στον τομέα της τεχνολογίας και της πληροφορικής. Παροχή υπηρεσιών συμμόρφωσης με τον Γενικό Κανονισμό για την Προστασία Δεδομένων.

Η λειτουργία της πλατφόρμας Renticom ως υπηρεσίας (SaaS) καλύπτεται από τα μέτρα αυτής της πολιτικής. Η ρητή συμπερίληψή της στο πεδίο του πιστοποιητικού εξετάζεται στην επόμενη ανασκόπηση της Διοίκησης.

3. Αρχές ασφάλειας πληροφοριών

ΑΡΧΗ	ΤΙ ΣΗΜΑΙΝΕΙ ΣΤΗΝ ΠΡΑΞΗ
Με βάση τον κίνδυνο	Τα μέτρα επιλέγονται με τεκμηριωμένη εκτίμηση κινδύνων (PRC-01), που επαναλαμβάνεται κάθε χρόνο και σε κάθε σημαντική αλλαγή. Η Διοίκηση αποδέχεται ρητά τους υπολειπόμενους κινδύνους.
Ανάγκη γνώσης και ελάχιστα δικαιώματα	Κάθε πρόσωπο έχει πρόσβαση μόνο σε ό,τι χρειάζεται για τον ρόλο του, με ατομικό λογαριασμό και πολυπαραγοντική ταυτοποίηση. Τα δικαιώματα επισκοπούνται κάθε εξάμηνο.
Ασφάλεια και ιδιωτικότητα από τον σχεδιασμό	Κάθε νέο προϊόν, έργο ή αλλαγή εξετάζεται για ασφάλεια και προστασία δεδομένων από την ανάλυση, όχι μετά την παράδοση.
Ταξινόμηση πληροφοριών	Οι πληροφορίες ταξινομούνται (Δημόσιο, Εσωτερικό, Εμπιστευτικό, Αυστηρά εμπιστευτικό) και ο χειρισμός τους ακολουθεί την ταξινόμηση (POL-02).
Ευθύνη του καθενός	Κάθε εργαζόμενος και συνεργάτης είναι υπεύθυνος για την ασφάλεια των πληροφοριών που χειρίζεται και αναφέρει αμέσως κάθε περιστατικό ή αδυναμία.

ΑΡΧΗ	ΤΙ ΣΗΜΑΙΝΕΙ ΣΤΗΝ ΠΡΑΞΗ
Εμπιστοσύνη με έλεγχο προς προμηθευτές	Προμηθευτές και πάροχοι cloud αξιολογούνται πριν από την ανάθεση, δεσμεύονται συμβατικά και επανεξετάζονται περιοδικά· για κάθε κρίσιμη υπηρεσία cloud υπάρχει σχέδιο εξόδου.
Συνέχεια	Οι κρίσιμες υπηρεσίες έχουν ορισμένους χρόνους ανάκαμψης· τα αντίγραφα ασφαλείας και τα σχέδια ανάκαμψης δοκιμάζονται.
Τεκμηρίωση και λογοδοσία	Ό,τι κάνουμε για την ασφάλεια και την ιδιωτικότητα καταγράφεται, ώστε να μπορεί να αποδειχθεί σε πελάτες, φορείς πιστοποίησης και αρχές.

4. Στόχοι ασφάλειας πληροφοριών

Η Διοίκηση ορίζει κάθε χρόνο μετρήσιμους στόχους ασφάλειας πληροφοριών και ιδιωτικότητας, με υπεύθυνο, πόρους, προθεσμία και τρόπο μέτρησης (ρήτρα 6.2 ISO/IEC 27001). Οι στόχοι καταγράφονται στο Σύστημα Μέτρησης Δεικτών (REG-001) και ανασκοπούνται στην ετήσια ανασκόπηση της Διοίκησης. Το πλαίσιο των στόχων είναι το εξής:

ΣΤΟΧΟΣ	ΜΕΤΡΗΣΗ	ΤΙΜΗ-ΣΤΟΧΟΣ
Πολυπαραγοντική ταυτοποίηση σε όλους τους λογαριασμούς	Λογαριασμοί με MFA / σύνολο ενεργών λογαριασμών	100%
Έγκαιρη εφαρμογή κρίσιμων ενημερώσεων ασφαλείας	Κρίσιμες ευπάθειες που κλείνουν εντός 30 ημερών	≥ 95%
Πλήρης επισκόπηση δικαιωμάτων πρόσβασης	Εξαμηνιαίες επισκοπήσεις που καλύπτουν όλους τους λογαριασμούς	2 / έτος, 100% κάλυψη
Δοκιμασμένη επαναφορά δεδομένων	Επιτυχείς δοκιμές επαναφοράς κρίσιμων συστημάτων	1 / τρίμηνο
Ενημερωμένο προσωπικό	Εργαζόμενοι που ολοκλήρωσαν τις ετήσιες εκπαιδεύσεις ασφαλείας και ιδιωτικότητας	100%
Αποτελεσματικός χειρισμός περιστατικών	Παραβιάσεις δεδομένων που γνωστοποιήθηκαν εκτός προθεσμίας (72 ώρες / σύμβαση)	0
Ελεγμένοι προμηθευτές	Κρίσιμοι προμηθευτές ΤΠΕ με ετήσια επαναξιολόγηση και σύμβαση επεξεργασίας όπου απαιτείται	100%
Έγκαιρη απάντηση στα υποκείμενα	Αιτήματα υποκειμένων που απαντήθηκαν εντός ενός μηνός	100%

5. Ρόλοι και αρμοδιότητες

ΡΟΛΟΣ	ΑΡΜΟΔΙΟΤΗΤΕΣ
Διοίκηση	Εγκρίνει την πολιτική και τους στόχους, διαθέτει πόρους, αποδέχεται τους υπολειπόμενους κινδύνους, διενεργεί την ανασκόπηση του συστήματος τουλάχιστον μία φορά τον χρόνο.
Υπεύθυνος Συστήματος ΣΔΑΠ / ΣΔΠΠ	Συντονίζει το σύστημα, τηρεί την τεκμηρίωση, εκτίμηση κινδύνων και Δήλωση Εφαρμοσιμότητας, οργανώνει εκπαιδεύσεις και εσωτερικές επιθεωρήσεις, αναφέρει στη Διοίκηση.
Σημείο επαφής για την ιδιωτικότητα / ΥΠΔ (εφόσον οριστεί)	Συμβουλεύει για την προστασία δεδομένων, χειρίζεται αιτήματα υποκειμένων και παραβιάσεις, επικοινωνεί με την ΑΠΔΠΧ. Ο ρόλος ασκείται χωρίς σύγκρουση συμφέροντος.
DevOps & Security / IT	Υλοποιεί και παρακολουθεί τα τεχνικά μέτρα, διαχειρίζεται λογαριασμούς, ενημερώσεις, αντίγραφα και συμβάντα.
Υπεύθυνοι έργων και προϊόντων	Εφαρμόζουν την ασφαλή ανάπτυξη και την ιδιωτικότητα από τον σχεδιασμό· τηρούν τις απαιτήσεις ασφαλείας κάθε σύμβασης.

ΡΟΛΟΣ	ΑΡΜΟΔΙΟΤΗΤΕΣ
Κάθε εργαζόμενος και συνεργάτης	Τηρεί την πολιτική και τις θεματικές πολιτικές, ολοκληρώνει τις εκπαιδεύσεις, αναφέρει αμέσως περιστατικά και αδυναμίες.

6. Θεματικές πολιτικές και πρότυπα

Η πολιτική εξειδικεύεται στα παρακάτω έγγραφα, που εγκρίνει η Διοίκηση και είναι διαθέσιμα στο προσωπικό στο αποθετήριο του συστήματος:

ΚΩΔΙΚΟΣ	ΕΓΓΡΑΦΟ	ΑΠΕΥΘΥΝΕΤΑΙ ΣΕ
POL-01	Πολιτική Αποδεκτής Χρήσης	Όλους
POL-02	Πολιτική Ταξινόμησης, Χειρισμού, Διατήρησης και Διαγραφής Πληροφοριών	Όλους
POL-03	Πολιτική Κωδικών Πρόσβασης και MFA	Όλους
POL-04	Πολιτική Συσκευών, BYOD, Τηλεργασίας και Απομακρυσμένης Πρόσβασης	Όλους
POL-05	Πολιτική Καθαρού Γραφείου, Καθαρής Οθόνης και Φυσικής Ασφάλειας	Όλους
GDL-AI	Οδηγία Χρήσης Εργαλείων Τεχνητής Νοημοσύνης	Όλους
YS-PIMS-POL-01	Πολιτική Προστασίας Προσωπικών Δεδομένων	Όλους
YS-PIMS-TOM-01	Εγχειρίδιο Τεχνικών και Οργανωτικών Μέτρων	Όλους · πελάτες κατόπιν αιτήματος
MAN-01, PRC-01 έως PRC-03	Εγχειρίδιο ΣΔΑΠ · Κίνδυνοι · Συμβάντα και παραβιάσεις · Πόροι	Διοίκηση, Υπ. Συστήματος, IT
STD-01 έως STD-06	Πρότυπα: λειτουργία IT, προσβάσεις, αντίγραφα και συνέχεια, δίκτυο και cloud, ασφαλής ανάπτυξη, προμηθευτές	IT, προγραμματιστές, Διοίκηση

7. Η YSOFT ως εκτελούσα την επεξεργασία

Όταν η YSOFT επεξεργάζεται πληροφορίες για λογαριασμό πελατών — στην πλατφόρμα Renticom και στα έργα ανάπτυξης, συντήρησης και υποστήριξης — εφαρμόζει τα μέτρα αυτής της πολιτικής και επιπλέον:

- επεξεργάζεται τα δεδομένα **μόνο κατ' εντολή του πελάτη** και για τον σκοπό της σύμβασης·
- χρησιμοποιεί υπεκτελούντες μόνο όπως ορίζει η σύμβαση επεξεργασίας (για το Renticom: Παράρτημα III του DPA) και ενημερώνει τον πελάτη πριν από κάθε αλλαγή·
- ενημερώνει τον πελάτη για κάθε παραβίαση **χωρίς αδικαιολόγητη καθυστέρηση** και τον συνδράμει στις υποχρεώσεις του·
- εφαρμόζει τις απαιτήσεις ασφαλείας της σύμβασης ή της διακήρυξης, όταν είναι αυστηρότερες από τις δικές της·
- στη λήξη της σύμβασης επιστρέφει ή διαγράφει τα δεδομένα και το βεβαιώνει γραπτώς.

8. Συμμόρφωση

Η YSOFT τηρεί Μητρώο Νομοθεσίας και Υποχρεώσεων που ανασκοπείται ετησίως. Ενδεικτικά εφαρμόζονται: ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 και ο ν. 4624/2019· ο ν. 3471/2006 για τις ηλεκτρονικές επικοινωνίες· ο ν. 5160/2024 (NIS2) στις απαιτήσεις που μεταφέρουν οι πελάτες στην αλυσίδα εφοδιασμού· ο Κανονισμός (ΕΕ) 2024/1689 για την τεχνητή νοημοσύνη και ο ν. 5321/2026· η νομοθεσία για την πνευματική ιδιοκτησία και οι όροι αδειών λογισμικού· οι συμβατικές υποχρεώσεις προς πελάτες.

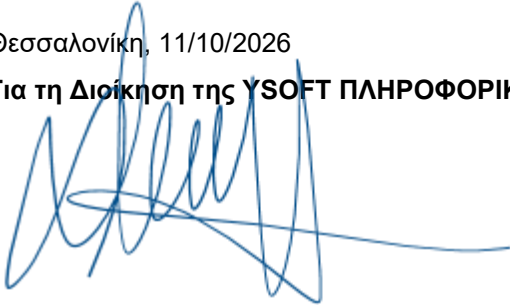
Η μη τήρηση της πολιτικής από εργαζόμενους αντιμετωπίζεται με την πειθαρχική διαδικασία του Εσωτερικού Κανονισμού και, για συνεργάτες, σύμφωνα με τη σύμβασή τους.

9. Επικοινωνία, διαθεσιμότητα και ανασκόπηση

- Η πολιτική κοινοποιείται σε κάθε νέο εργαζόμενο πριν από την πρόσβασή του σε πληροφορίες και σε όλο το προσωπικό μετά από κάθε αναθεώρηση, με βεβαίωση παραλαβής.
- Είναι διαθέσιμη σε πελάτες, συνεργάτες και κάθε ενδιαφερόμενο μέρος κατόπιν αιτήματος και μπορεί να αναρτηθεί στον ιστότοπο της Εταιρείας.
- Ανασκοπείται **τουλάχιστον μία φορά τον χρόνο** στην ανασκόπηση της Διοίκησης, καθώς και μετά από σημαντική αλλαγή στην Εταιρεία, στις υπηρεσίες, στην υποδομή, στη νομοθεσία ή μετά από σοβαρό περιστατικό.

Θεσσαλονίκη, 11/10/2026

Για τη Διοίκηση της YSOFT ΠΛΗΡΟΦΟΡΙΚΗ Α.Ε.



Θεόφιλος Μυλωνάς · Πρόεδρος & Διευθύνων Σύμβουλος