					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P36S					Τίτλος εγγράφου: **Πολιτική Κοινωνικών Μέσων και Εξωτερικών Επικοινωνιών**							
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	Ρήτρες 5.1, 5.2, 6.1, 8	Ηγεσία, διαχείριση κινδύνων και επιχειρησιακοί έλεγχοι για τις εξωτερικές επικοινωνίες
ISO/IEC 27002:2022	Έλεγχοι 5.10, 5.11	Αποδεκτή χρήση και ασφάλεια πληροφοριών στις επικοινωνίες
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Κανόνες συμπεριφοράς, έλεγχος, αναφορά περιστατικών και διαχείριση δημόσια προσβάσιμου περιεχομένου και πρόσβασης
ΓΚΠΔ της ΕΕ	Άρθρα 5, 32, 33	Αρχές προστασίας δεδομένων, ασφάλεια και γνωστοποίηση παραβίασης που επηρεάζει τη δημόσια επικοινωνία
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(e), 21(2)(f)	Πολιτικές για τη χρήση συστημάτων και τη διαχείριση κινδύνων στην εφοδιαστική αλυσίδα/στις δημόσιες επικοινωνίες
Κανονισμός DORA της ΕΕ	Άρθρο 14(4)	Υποχρεώσεις επικοινωνίας μετά από περιστατικά

1. Σκοπός

1.1. Η παρούσα πολιτική θεσπίζει υποχρεωτικούς κανόνες για κάθε δημόσια προσβάσιμη επικοινωνία — συμπεριλαμβανομένης της χρήσης κοινωνικών μέσων, της επικοινωνίας με τον Τύπο και του εξωτερικού ψηφιακού περιεχομένου — όταν γίνεται αναφορά στην εταιρεία, το προσωπικό της, τους πελάτες της, τα συστήματά της ή τις εσωτερικές πρακτικές της.

1.2. Η πολιτική συμβάλλει στην προστασία της φήμης της εταιρείας, στη διατήρηση της συμμόρφωσης με νομικές και κανονιστικές υποχρεώσεις και στη μείωση του κινδύνου διαρροής πληροφοριών, παραπληροφόρησης ή περιστατικών ασφάλειας.

1.3. Επιτρέπει στο προσωπικό και στους συνεργάτες να συμμετέχουν θετικά και υπεύθυνα σε διαδικτυακές συζητήσεις, αποφεύγοντας ταυτόχρονα ακούσιες γνωστοποιήσεις ή παραπλανητική παρουσίαση.

1.4. Η πολιτική ενισχύει την ετοιμότητα της SME για πιστοποίηση ISO/IEC 27001, μέσω του ελέγχου των πληροφοριών που καθίστανται διαθέσιμες στο κοινό ή σε εξωτερικά ενδιαφερόμενα μέρη.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλα τα πρόσωπα που συνδέονται με τον οργανισμό, συμπεριλαμβανομένων των εξής:

2.1.1. Εργαζομένων και αναδόχων

2.1.2. Ελεύθερων επαγγελματιών, συμβούλων, προμηθευτών και λοιπών τρίτων

2.1.3. Ασκουμένων ή εργαζομένων μερικής απασχόλησης που εμπλέκονται στην παροχή υπηρεσιών προς πελάτες ή έχουν πρόσβαση σε συστήματα

2.2. Η πολιτική εφαρμόζεται σε κάθε μορφή εξωτερικής επικοινωνίας που αναφέρεται στον οργανισμό, συμπεριλαμβανομένων των εξής:

2.2.1. Αναρτήσεων σε μέσα κοινωνικής δικτύωσης (LinkedIn, Twitter/X, TikTok, Instagram, Facebook κ.λπ.)

2.2.2. Αναρτήσεων σε ιστολόγια, διαδικτυακά φόρουμ, αξιολογήσεων πελατών και νημάτων συζήτησης

2.2.3. Συμμετοχής ως ομιλητή σε εξωτερικές εκδηλώσεις (π.χ. συνέδρια, webinars, podcasts)

2.2.4. Ηλεκτρονικών μηνυμάτων ή μηνυμάτων προς δημοσιογράφους, κυβερνητικούς εκπροσώπους ή influencers

2.2.5. Δημόσια κοινοποιημένων στιγμιοτύπων οθόνης, φωτογραφιών ή βίντεο από χώρους εργασίας

2.3. Η πολιτική εφαρμόζεται επίσης όταν η εν λόγω επικοινωνία πραγματοποιείται:

2.3.1. Από προσωπικές συσκευές ή λογαριασμούς

2.3.2. Εκτός του κανονικού ωραρίου εργασίας

2.3.3. Χωρίς κακόβουλη πρόθεση — ακόμη και ακούσια ή παρεμπίπτοντα σχόλια εμπίπτουν στο πεδίο εφαρμογής, εφόσον αναφέρονται στην εταιρεία

3. Στόχοι

3.1. Προστασία φήμης: Αποτροπή βλάβης στην εικόνα της εταιρείας μέσω μη εξουσιοδοτημένης ή ακατάλληλης δημόσιας επικοινωνίας

3.2. Ασφάλεια δεδομένων: Αποφυγή ακούσιας έκθεσης ευαίσθητων δεδομένων, εσωτερικών συστημάτων ή στοιχείων πελατών μέσω κοινωνικών μέσων ή δημόσιων διαύλων

3.3. Νομική και κανονιστική συμμόρφωση: Διασφάλιση ότι κάθε δημόσιο περιεχόμενο που αναφέρεται στην εταιρεία συμμορφώνεται με τη σχετική νομοθεσία περί προστασίας δεδομένων και εξωτερικής επικοινωνίας

3.4. Επαγγελματική συμπεριφορά: Προώθηση υπεύθυνης συμμετοχής σε διαδικτυακές συζητήσεις και επαφές με τα μέσα ενημέρωσης, ακόμη και μέσω προσωπικών λογαριασμών

3.5. Ετοιμότητα για περιστατικά: Παροχή σαφών και εφαρμόσιμων ενεργειών σε περίπτωση ακούσιας γνωστοποίησης ή παραβίασης της πολιτικής

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής (GM)

4.1.1. Έχει την ευθύνη της παρούσας πολιτικής και την εγκρίνει

4.1.2. Ανασκοπεί και εγκρίνει κάθε δημόσια δήλωση, επικοινωνία με τον Τύπο ή συνέντευξη στα μέσα ενημέρωσης

4.1.3. Διασφαλίζει ότι η παρούσα πολιτική κοινοποιείται με σαφήνεια σε όλους τους εργαζομένους και τα τρίτα μέρη

4.1.4. Διερευνά και αντιμετωπίζει κάθε παραβίαση της παρούσας πολιτικής, σε συντονισμό με τις διαδικασίες απόκρισης σε περιστατικά

4.2. Ορισμένος εργαζόμενος ή υπεύθυνος επικοινωνίας (εφόσον έχει οριστεί)

4.2.1. Υποστηρίζει τον GM στην ανασκόπηση περιεχομένου πριν από εξωτερική δημοσίευση (π.χ. αναρτήσεις ιστολογίου, θέματα ομιλιών)

4.2.2. Τηρεί αρχεία καταγραφής εγκεκριμένων δραστηριοτήτων στα μέσα ενημέρωσης ή αναρτήσεων σε μέσα κοινωνικής δικτύωσης υψηλού κινδύνου

4.2.3. Παρακολουθεί, στο μέτρο των διαθέσιμων δυνατοτήτων, γνωστές αναφορές στην εταιρεία στο διαδίκτυο για κινδύνους φήμης ή 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. Ετήσια ανασκόπηση

9.1.1. Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον Γενικό Διευθυντή (GM)

9.1.2. Η ανασκόπηση πρέπει να διασφαλίζει την ευθυγράμμιση με επικαιροποιημένες νομικές υποχρεώσεις, τις τάσεις επικοινωνίας του κλάδου και τις εσωτερικές επιχειρησιακές αλλαγές

9.2. Ανασκοπήσεις βάσει εναυσμάτων

9.2.1. Η παρούσα πολιτική πρέπει να επικαιροποιείται άμεσα μετά από:

9.2.1.1. Σημαντικό περιστατικό στα κοινωνικά μέσα ή ζήτημα φήμης

9.2.1.2. Αλλαγή σε προμηθευτές ή άλλους τρίτους που διαχειρίζονται επικοινωνίες

9.2.1.3. Νέα νομοθεσία ή κανονιστικές υποχρεώσεις σχετικά με τη διαδικτυακή επικοινωνία, τα μέσα ενημέρωσης ή την εταιρική ταυτότητα

9.3. Τεκμηρίωση αλλαγών

9.3.1. Όλες οι επικαιροποιήσεις πρέπει να καταγράφονται, συμπεριλαμβανομένων της ημερομηνίας αναθεώρησης, της σύνοψης αλλαγών και της έγκρισης από τον GM

9.3.2. Πρέπει να τηρείται ιστορικό εκδόσεων για σκοπούς ελέγχου και πιστοποίησης

9.4. Διανομή επικαιροποιήσεων

9.4.1. Όλο το προσωπικό και οι ανάδοχοι πρέπει να ενημερώνονται για κάθε αλλαγή της πολιτικής

9.4.2. Οι επικαιροποιημένες εκδόσεις πρέπει να κοινοποιούνται μέσω ηλεκτρονικού ταχυδρομείου ή εσωτερικών πυλών

9.4.3. Κάθε προμηθευτής δημόσιας επικοινωνίας πρέπει να επιβεβαιώνει την αποδοχή των επικαιροποιημένων όρων πριν από τη συνέχιση της εργασίας

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική λειτουργεί σε συντονισμό με τις ακόλουθες πολιτικές SME:

10.1.1. P3S – Πολιτική Αποδεκτής Χρήσης: Ορίζει την αποδεκτή συμπεριφορά κατά τη χρήση πλατφορμών επικοινωνίας, συμπεριλαμβανομένης της πρόσβασης σε κοινωνικά μέσα κατά τις ώρες εργασίας

10.1.2. P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι το προσωπικό εκπαιδεύεται να αναγνωρίζει τους κινδύνους υπερβολικής κοινοποίησης, ηλεκτρονικού ψαρέματος ή διαδικτυακών απειλών για τη φήμη

10.1.3. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι δεδομένα προσωπικού χαρακτήρα και δεδομένα πελατών δεν κοινοποιούνται σε εξωτερικές επικοινωνίες, σε ευθυγράμμιση με τον ΓΚΠΔ και άλλες νομικές απαιτήσεις

10.1.4. P30S – Πολιτική αντιμετώπισης περιστατικών (P30): Διέπει την απόκριση σε ακούσια δημόσια γνωστοποίηση, διαδικτυακές απειλές ή επιθέσεις στη φήμη που προκύπτουν από κακή χρήση κοινωνικών μέσων

10.1.5. P37S – Πολιτική Νομικής και Κανονιστικής Συμμόρφωσης: Καθορίζει τις ευρύτερες νομικές και συμβατικές υποχρεώσεις του οργανισμού κατά τη δημόσια κοινοποίηση περιεχομένου

10.2. Οι πολιτικές αυτές πρέπει να εφαρμόζονται από κοινού, ώστε να διατηρείται ασφαλής, επαγγελματική και νομικά συμμορφούμενη εξωτερική παρουσία.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 5.1 – Ηγεσία και δέσμευση: Απαιτεί εποπτεία από τη διοίκηση επί των κινδύνων φήμης και πληροφοριών

11.1.2. Ρήτρα 6.1 – Διαχείριση κινδύνων: Περιλαμβάνει την έκθεση σε κινδύνους που σχετίζονται με την επικοινωνία

11.1.3. Ρήτρα 8.1 – Επιχειρησιακός έλεγχος: Καλύπτει τους κανόνες για τον τρόπο με τον οποίο οι πληροφορίες κοινοποιούνται εξωτερικά

11.2. ISO/IEC 27002

11.2.1. Έλεγχος 5.10 – Αποδεκτή χρήση πληροφοριών και περιουσιακών στοιχείων

11.2.2. Έλεγχος 5.11 – Ασφάλεια πληροφοριών στις επικοινωνίες

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Κανόνες συμπεριφοράς: Διέπει την κατάλληλη συμπεριφορά για τη χρήση πληροφοριακών πόρων

11.3.2. AU-7 – Μείωση δεδομένων ελέγχου και παραγωγή αναφορών: Υποστηρίζει την παρακολούθηση της δημόσιας χρήσης συστημάτων

11.3.3. IR-6 – Αναφορά περιστατικών: Επιβάλλει την απόκριση σε παραβιάσεις φήμης και επικοινωνίας

11.3.4. AC-22 – Δημόσια προσβάσιμο περιεχόμενο: Διασφαλίζει τον έλεγχο των εξωτερικών δημοσιεύσεων και της πρόσβασης

11.4. ΓΚΠΔ της ΕΕ (2016/679)

11.4.1. Άρθρο 5 – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (ακρίβεια, ακεραιότητα, λογοδοσία)

11.4.2. Άρθρο 32 – Ασφάλεια της επεξεργασίας: Απαιτεί δικλίδες ασφαλείας για τη δημόσια κοινοποίηση

11.4.3. Άρθρο 33 – Γνωστοποίηση παραβίασης: Ενεργοποιείται εφόσον δεδομένα προσωπικού χαρακτήρα εκτεθούν μέσω εξωτερικής επικοινωνίας

11.5. Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1. Άρθρο 21(2)(e) – Πολιτικές για τη χρήση πληροφοριακών συστημάτων, συμπεριλαμβανομένων των πλατφορμών επικοινωνίας

11.5.2. Άρθρο 21(2)(f) – Πολιτικές για τη διαχείριση κινδύνων κυβερνοασφάλειας στην εφοδιαστική αλυσίδα και στις δημόσιες πλατφόρμες

11.6. Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1. Άρθρο 14(4) – Υποχρεώσεις επικοινωνίας προς πελάτες, τρίτα μέρη και αρχές μετά από λειτουργικά περιστατικά

11.7. COBIT 2019

11.7.1. APO09 – Διαχείριση συμφωνιών παροχής υπηρεσιών: Καλύπτει την εποπτεία προμηθευτών και τρίτων μερών που σχετίζονται με την επικοινωνία

11.7.2. DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Περιλαμβάνει την προστασία δημόσια προσβάσιμων ψηφιακών περιουσιακών στοιχείων

11.7.3. EDM03 – Διασφάλιση βελτιστοποίησης κινδύνου: Τονίζει τη διαχείριση κινδύνων φήμης και συμμόρφωσης που σχετίζονται με την επικοινωνία