					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P36S					Τίτλος εγγράφου: **Πολιτική Μέσων Κοινωνικής Δικτύωσης 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	Ρήτρα 8	Καθορισμένες διεργασίες και διακυβέρνηση βάσει ρόλων για τη διαχείριση δημόσιων επικοινωνιών, με διασφάλιση της ακρίβειας, ροές έγκρισης και κλιμάκωση περιστατικών.
ISO/IEC 27002:2022	Έλεγχοι 5.10, 5.11, 5.35, 5.36	Διέπει τη χρήση και την αποδεκτή χρήση, την εξωτερική επικοινωνία με αρχές/φορείς και την αναφορά συμμόρφωσης.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Κανόνες για τη χρήση συστημάτων/επικοινωνιών, ειδοποιήσεις προς τους χρήστες και διατήρηση αρχείων ελέγχου.
ΓΚΠΔ της ΕΕ	Άρθρα 5, 25, 32, 33	Αρχές επεξεργασίας δεδομένων, προστασία δεδομένων ήδη από τον σχεδιασμό, ασφάλεια της επεξεργασίας και υποχρεώσεις γνωστοποίησης παραβίασης.
Οδηγία NIS2 της ΕΕ	Άρθρο 21	Μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, υποχρεώσεις σε περιστατικά και δημόσια επικοινωνία σχετική με κινδύνους.
Κανονισμός DORA της ΕΕ	Άρθρα 9, 16	Διαχείριση κινδύνων ΤΠΕ και στρατηγική επικοινωνίας για κρίσιμους παρόχους.
COBIT 2019	APO09, DSS05	Διακυβέρνηση συμφωνιών παροχής υπηρεσιών/επικοινωνίας και πρακτικές ασφαλούς επικοινωνίας/διαχείρισης περιστατικών.

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικούς κανόνες και αρμοδιότητες που διέπουν τη χρήση των μέσων κοινωνικής δικτύωσης και κάθε μορφής εξωτερικής επικοινωνίας από το προσωπικό που συνδέεται με τον οργανισμό.

1.2 Διασφαλίζει ότι κάθε δημόσιο μήνυμα —είτε προγραμματισμένο είτε αυθόρμητο— είναι ακριβές, κόσμιο, ασφαλές, νομικά συμμορφούμενο και συνεπές με την εταιρική ταυτότητα.

1.3 Η πολιτική αποσκοπεί στη μείωση των κινδύνων που συνδέονται με ζημία στη φήμη, κανονιστική παράβαση, διαρροή διανοητικής ιδιοκτησίας και μη εξουσιοδοτημένες γνωστοποιήσεις μέσω δημόσια προσβάσιμων διαύλων.

1.4 Επιπλέον, προάγει τη λογοδοσία και τη δομημένη διακυβέρνηση σε κάθε μορφή ψηφιακής επικοινωνίας που αφορά ή επηρεάζει τον οργανισμό.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλους τους εργαζομένους, αναδόχους, ασκούμενους και εκπροσώπους τρίτων μερών που:

2.1.1 Επικοινωνούν εκ μέρους του οργανισμού, είτε επίσημα είτε ανεπίσημα

2.1.2 Αναφέρονται ή υποδηλώνουν σχέση με τον οργανισμό σε δημόσιο πλαίσιο

2.1.3 Χρησιμοποιούν προσωπικούς ή εταιρικούς λογαριασμούς για συμμετοχή σε δημόσιες συζητήσεις που αφορούν τον οργανισμό

2.2 Οι δίαυλοι επικοινωνίας που καλύπτονται περιλαμβάνουν, ενδεικτικά και όχι περιοριστικά:

2.2.1 Πλατφόρμες μέσων κοινωνικής δικτύωσης (π.χ. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Ιστολόγια, wiki, φόρουμ και δημόσιους πίνακες συζήτησης

2.2.3 Ηλεκτρονικό ταχυδρομείο ή απευθείας μηνύματα προς εξωτερικά μέρη (π.χ. πελάτες, ρυθμιστικές αρχές, μέσα ενημέρωσης)

2.2.4 Συνεντεύξεις Τύπου, πάνελ ομιλητών ή εμφανίσεις σε καταγεγραμμένα μέσα

2.2.5 Συμμετοχή σε διαδικτυακές κοινότητες όπου γίνεται αναφορά στον οργανισμό

2.3 Η παρούσα πολιτική διέπει τόσο το περιεχόμενο σε πραγματικό χρόνο όσο και το προγραμματισμένο περιεχόμενο και εφαρμόζεται σε όλες τις συσκευές και τους λογαριασμούς (προσωπικούς ή εταιρικούς) που χρησιμοποιούνται για τη διάδοση της επικοινωνίας.

3. Στόχοι

3.1 Η αποτροπή τυχαίας ή εκούσιας γνωστοποίησης εμπιστευτικών, ευαίσθητων ή ρυθμιζόμενων πληροφοριών μέσω εξωτερικών διαύλων επικοινωνίας.

3.2 Η διασφάλιση ότι οι επίσημες δημόσιες δηλώσεις και το περιεχόμενο μέσων κοινωνικής δικτύωσης είναι ακριβή, εγκεκριμένα και ευθυγραμμισμένα με την εταιρική ταυτότητα, τη δεοντολογία και τη στρατηγική επικοινωνίας.

3.3 Η αποτροπή ζημίας στη φήμη και η διασφάλιση συνέπειας στα μηνύματα μεταξύ εσωτερικών τμημάτων και εξωτερικών πλατφορμών.

3.4 Η συμμόρφωση με τις εφαρμοστέες νομικές υποχρεώσεις που σχετίζονται με δημόσιες δηλώσεις, συμπεριλαμβανομένων ενδεικτικά του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ, του Κανονισμού DORA της ΕΕ και των κανόνων επικοινωνίας που ισχύουν ανά κλάδο.

3.5 Ο καθορισμός σαφών αρμοδιοτήτων, επιτρεπόμενων περιπτώσεων χρήσης και πρωτοκόλλων εφαρμογής για όλο το προσωπικό που συμμετέχει σε δραστηριότητες με δημόσια έκθεση.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Μάρκετινγκ ή Επικοινωνίας / Επικεφαλής Δημοσίων Σχέσεων

4.1.1 Εγκρίνει όλα τα επίσημα εταιρικά μηνύματα για εξωτερική δημοσίευση

4.1.2 Τηρεί χρονοδιάγραμμα περιεχομένου μέσων κοινωνικής δικτύωσης και κατευθυντήριες οδηγίες για τη συνέπεια με την εταιρική ταυτότητα

4.1.3 Παρακολουθεί τις διαδικτυακές αναφορές και την έκθεση στα μέσα που αφορούν τον οργανισμό

4.2 Επικεφαλής Ασφάλειας Πληροφοριών (CISO) / Ομάδα Ασφάλειας

4.2.1 Παρακολουθεί τις ψηφιακές πλατφόρμες για ενδείξεις διαρροής δεδομένων, πλαστοπροσωπίας ή απόπειρες ηλεκτρονικού ψαρέματος

4.2.2 Συντονίζεται με τις ομάδες απόκρισης σε περιστατικά σε περίπτωση επιθέσεων ή παραβιάσεων μέσω μέσων κοινωνικής δικτύωσης

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Εφαρμογή και συμμόρφωση

9.1 Η παρούσα πολιτική είναι υποχρεωτική για όλο το καλυπτόμενο προσωπικό και τα τρίτα μέρη. Η μη συμμόρφωση μπορεί να οδηγήσει σε:

9.1.1 Επίσημες προειδοποιήσεις

9.1.2 Προσωρινή ή μόνιμη ανάκληση πρόσβασης σε πλατφόρμες ή συστήματα

9.1.3 Πειθαρχικά μέτρα, συμπεριλαμβανομένης της αποχώρησης

9.1.4 Δικαστικές ενέργειες, εφόσον η εξωτερική επικοινωνία οδηγεί σε ζημία στη φήμη, παραβίαση δεδομένων ή κανονιστική μη συμμόρφωση

9.2 Πειθαρχικές ενέργειες

9.2.1 Εσωτερικές παραβιάσεις (π.χ. διαρροή εμπιστευτικών δεδομένων, δυσφήμηση του οργανισμού) ενεργοποιούν εμπλοκή του HR, επίσημη διερεύνηση και τεκμηρίωση στον φάκελο εργαζομένου.

9.2.2 Όπου εφαρμόζεται, η Νομική Υπηρεσία επιδιώκει αστικά ένδικα μέσα ή ειδοποιεί τις αρμόδιες αρχές για εγκληματική δραστηριότητα (π.χ. πλαστοπροσωπία, διαρροές σχετιζόμενες με κατάχρηση προνομιακής πληροφόρησης).

9.3 Παρακολούθηση συμμόρφωσης

9.3.1 Οι Ομάδες Ασφάλειας και Επικοινωνίας πρέπει να διενεργούν συνεχή παρακολούθηση των εξής:

9.3.1.1 Αναφορών στην εταιρική ταυτότητα σε κύριες πλατφόρμες

9.3.1.2 Ανεπίσημης χρήσης εταιρικών εικόνων ή εμπορικών σημάτων

9.3.1.3 Γνωστών κινδύνων (π.χ. δυσαρεστημένοι εργαζόμενοι, απόπειρες πλαστοπροσωπίας)

9.3.2 Η παρακολούθηση πρέπει να συμμορφώνεται με τη νομοθεσία και τους κανονισμούς περί ιδιωτικότητας των εργαζομένων, ενώ όλες οι επισημασμένες περιπτώσεις πρέπει να επαληθεύονται από ανθρώπινο αξιολογητή.

9.4 Αναφορά παρατυπιών και κακής χρήσης

9.4.1 Κάθε εργαζόμενος που υποψιάζεται παραβίαση της παρούσας πολιτικής ενθαρρύνεται να την αναφέρει στην Ομάδα Ασφάλειας Πληροφοριών, στη Νομική Υπηρεσία ή ανώνυμα μέσω της πύλης αναφοράς παρατυπιών.

9.4.2 Απαγορεύονται αυστηρά τα αντίποινα κατά αναφερόντων και υπόκεινται σε άμεση πειθαρχική ενέργεια.

10. Απαιτήσεις ανασκόπησης και επικαιροποίησης

10.1 Η παρούσα πολιτική πρέπει να ανασκοπείται ετησίως ή νωρίτερα εάν:

10.1.1 Υπάρχουν σημαντικές αλλαγές στις κανονιστικές απαιτήσεις (π.χ. νέοι νόμοι της ΕΕ για τις ψηφιακές επικοινωνίες)

10.1.2 Υιοθετούνται νέες πλατφόρμες κοινωνικής δικτύωσης ή δίαυλοι επικοινωνίας

10.1.3 Υπάρχει σημαντικό περιστατικό ή επαναλαμβανόμενες παραβιάσεις που υποδεικνύουν κενά στις διεργασίες

10.1.4 Υπάρχει οργανωτική ή διοικητική αλλαγή στις λειτουργίες Δημοσίων Σχέσεων, Νομικής Υπηρεσίας ή Ασφάλειας

10.2 Η ανασκόπηση πρέπει να διενεργείται από κοινού από:

10.2.1 Τον Επικεφαλής Μάρκετινγκ / Δημοσίων Σχέσεων

10.2.2 Τον CISO ή τον Επικεφαλής Κινδύνων Ασφάλειας

10.2.3 Τους Υπεύθυνους Νομικής και Κανονιστικής Συμμόρφωσης

10.3 Οι επικαιροποιήσεις πρέπει να τεκμηριώνονται στο Μητρώο Αλλαγών Πολιτικής και να γνωστοποιούνται μέσω εσωτερικών διαύλων ευαισθητοποίησης. Όταν επέρχονται ουσιώδεις αλλαγές, όλο το επηρεαζόμενο προσωπικό πρέπει να επαναβεβαιώνει τη βεβαίωση αποδοχής της πολιτικής.

11. Συναφείς πολιτικές και διασυνδέσεις

11.1 Η παρούσα πολιτική υποστηρίζεται από και διασυνδέεται με τα ακόλουθα στοιχεία του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) του οργανισμού:

11.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις υπερκείμενες αρχές για τη διαφύλαξη πληροφοριών, συμπεριλαμβανομένης της διασφάλισης ότι οι επικοινωνίες δεν οδηγούν σε μη εξουσιοδοτημένη γνωστοποίηση.

11.1.2 P3 – Πολιτική Αποδεκτής Χρήσης: Ορίζει αποδεκτές συμπεριφορές για ψηφιακές πλατφόρμες και τεχνολογίες, οι οποίες διέπουν άμεσα την προσωπική και επαγγελματική χρήση κοινωνικών διαύλων.

11.1.3 P6 – Πολιτική Διαχείρισης Κινδύνων: Παρέχει το πλαίσιο κινδύνων για την αξιολόγηση απειλών που σχετίζονται με τη δημόσια επικοινωνία και την έκθεση σε ζημία φήμης.

11.1.4 P8 – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Επιβάλλει προγράμματα ευαισθητοποίησης που εκπαιδεύουν το προσωπικό σε πρακτικές ασφαλούς επικοινωνίας και απειλές κοινωνικής μηχανικής.

11.1.5 P13 – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθοδηγεί το προσωπικό σχετικά με το τι συνιστά περιορισμένες ή εμπιστευτικές πληροφορίες, οι οποίες δεν πρέπει να γνωστοποιούνται εξωτερικά.

11.1.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών: Ορίζει τον τρόπο χειρισμού περιστατικών που σχετίζονται με δημόσια επικοινωνία, συμπεριλαμβανομένων διαρροών δεδομένων, πλαστοπροσωπίας και κανονιστικής παράβασης.

11.1.7 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Διέπει τις ελεγκτικές διεργασίες που επικυρώνουν ελέγχους μέσων κοινωνικής δικτύωσης, συστήματα παρακολούθησης και τη συμμόρφωση με πολιτικές εξωτερικής επικοινωνίας.

12. Πρότυπα και πλαίσια αναφοράς

12.1 ISO/IEC 27001:

12.1.1 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί καθορισμένες διεργασίες και διακυβέρνηση βάσει ρόλων για τη διαχείριση δημόσιων επικοινωνιών, με διασφάλιση της ακρίβειας, ροές έγκρισης και κλιμάκωση περιστατικών που αφορούν δεδομένα ή κίνδυνο για τη φήμη.

12.2 ISO/IEC 27002:2022:

12.2.1 Έλεγχος 5.10 – Χρήση πληροφοριών: Διέπει την εξουσιοδοτημένη και δεοντολογική διάδοση εσωτερικών ή εξωτερικών επικοινωνιών.

12.2.2 Έλεγχος 5.11 – Αποδεκτή χρήση πληροφοριών και περιουσιακών στοιχείων: Ενισχύει τις αποδεκτές πρακτικές κοινοποίησης περιεχομένου με χρήση εταιρικών περιουσιακών στοιχείων ή προσωπικών λογαριασμών.

12.2.3 Έλεγχος 5.35 – Επικοινωνία με αρχές: Απαιτεί δομημένη και εξουσιοδοτημένη εξωτερική επικοινωνία με ρυθμιστικούς φορείς και δημόσιες αρχές.

12.2.4 Έλεγχος 5.36 – Συμμόρφωση με πολιτικές και πρότυπα: Απαιτεί συνεπή εφαρμογή των εσωτερικών πολιτικών σε όλα τα σενάρια επικοινωνίας.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Κανόνες συμπεριφοράς: Απαιτεί επίσημους κανόνες για τη χρήση συστημάτων και επικοινωνιών, συμπεριλαμβανομένων προτύπων δημόσιας γνωστοποίησης.

12.3.2 AC-8 – Ειδοποίηση χρήσης συστήματος: Υποστηρίζει υποχρεωτικές αποποιήσεις ευθύνης και προειδοποιήσεις περιεχομένου σε πλατφόρμες με εξωτερική έκθεση.

12.3.3 AU-12 – Διατήρηση αρχείων ελέγχου: Εφαρμόζεται στη διατήρηση αρχείων καταγραφής και ιστορικού επικοινωνιών για σκοπούς ανασκόπησης περιστατικών και ελέγχου.

12.4 ΓΚΠΔ της ΕΕ (2016/679):

12.4.1 Άρθρο 5 – Αρχές επεξεργασίας δεδομένων: Απαγορεύει τη μη εξουσιοδοτημένη κοινοποίηση δεδομένων προσωπικού χαρακτήρα μέσω δημόσιας επικοινωνίας.

12.4.2 Άρθρο 25 – Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού: Απαιτεί δικλίδες ιδιωτικότητας σε εργαλεία επικοινωνίας και ροές περιεχομένου.

12.4.3 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Εφαρμόζεται σε κρυπτογράφηση, έλεγχο πρόσβασης και διεργασίες έγκρισης περιεχομένου.

12.4.4 Άρθρο 33 – Γνωστοποίηση παραβίασης: Επιβάλλει έγκαιρη γνωστοποίηση διαρροών δεδομένων προσωπικού χαρακτήρα μέσω δημόσιων διαύλων.

12.5 Οδηγία NIS2 της ΕΕ (2022/2555):

12.5.1 Άρθρο 21 – Μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας: Περιλαμβάνει πρωτόκολλα επικοινωνίας και υποχρεώσεις κατά τη διάρκεια περιστατικών και στη δημόσια επικοινωνία σχετικά με κινδύνους.

12.6 Κανονισμός DORA της ΕΕ (2022/2554):

12.6.1 Άρθρο 9 – Διαχείριση κινδύνων ΤΠΕ: Εφαρμόζεται σε κινδύνους επικοινωνίας που εκδηλώνονται εξωτερικά, όπως πλαστοπροσωπία, παραπληροφόρηση και διατάραξη της φήμης.

12.6.2 Άρθρο 16 – Στρατηγική επικοινωνίας: Απαιτεί από κρίσιμους χρηματοοικονομικούς φορείς ή παρόχους υπηρεσιών να διαχειρίζονται κινδύνους επικοινωνίας και αποκρίσεις σε σενάρια κρίσης.

12.7 COBIT 2019:

12.7.1 APO09 – Διαχειριζόμενες συμφωνίες υπηρεσιών και επικοινωνία: Απαιτεί δομημένη διακυβέρνηση επί των εσωτερικών και εξωτερικών επικοινωνιών.

12.7.2 DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Διασφαλίζει ότι οι δραστηριότητες επικοινωνίας δεν εισάγουν πρόσθετο κίνδυνο ούτε υπονομεύουν τις διεργασίες χειρισμού περιστατικών.