ΕΛΛΗΝΟΑΜΕΡΙΚΑΝΙΚΗ ΕΝΩΣΗ

Σωματείο Κοινωφελές, Εκπαιδευτικό και Πολιτιστικό

Πολιτική Ασφάλειας Πληροφοριών

ΔΙΑΒΑΘΜΙΣΗ ΕΓΓΡΑΦΟΥ	Εμπιστευτικό
ΑΝΑΦΟΡΑ ΕΓΓΡΑΦΟΥ	ISMS-DOC-05-4
ΕΚΔΟΣΗ	1
ΗΜΕΡΟΜΗΝΙΑ	[Insert date]
ΣΥΝΤΑΚΤΗΣ ΕΓΓΡΑΦΟΥ	[Insert name]
ΚΑΤΟΧΟΣ ΕΓΓΡΑΦΟΥ	[Insert name/role]

Ιστορικό Αναθεωρήσεων

ΕΚΔΟΣΗ	ΗΜΕΡΟΜΗΝΙΑ	ΣΥΝΤΑΚΤΗΣ ΑΝΑΘΕΩΡΗΣΗΣ	ΠΕΡΙΛΗΨΗ ΑΛΛΑΓΩΝ

Διακίνηση

ΟΝΟΜΑ	ΤΙΤΛΟΣ

Έγκριση

ΟΝΟΜΑ	ΘΕΣΗ	ΥΠΟΓΡΑΦΗ	ΗΜΕΡΟΜΗΝΙΑ

Περιεχόμενα

Πίνακες

1 Εισαγωγή

Αυτό το έγγραφο καθορίζει την πολιτική ασφάλειας πληροφοριών της Ελληνοαμερικανικής Ένωσης.

Ως ένα σύγχρονο, στραμμένο προς το μέλλον σωματείο, η Ελληνοαμερικανική Ένωση αναγνωρίζει σε ανώτερα επίπεδα διοίκησης την ανάγκη να διασφαλίσει ότι το σωματείο της λειτουργεί ομαλά και χωρίς διακοπές προς όφελος των πελατών, των μετόχων και των άλλων ενδιαφερόμενων μερών.

Προκειμένου να παρέχει ένα τέτοιο επίπεδο συνεχούς λειτουργίας, η Ελληνοαμερικανική Ένωση έχει εφαρμόσει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) σύμφωνα με το Διεθνές Πρότυπο για την Ασφάλεια Πληροφοριών, ISO/IEC 27001 με την επέκτασή του ISO/IEC 27701 για την Ιδιωτικότητα. Αυτά τα πρότυπα καθορίζουν τις απαιτήσεις για ένα ISMS που βασίζεται σε διεθνώς αναγνωρισμένες βέλτιστες πρακτικές (best practices).

Η λειτουργία του ISMS έχει πολλά οφέλη για το σωματείο, όπως:

- Προστασία των ροών εσόδων και της κερδοφορίας του σωματείου
- Διασφάλιση της προμήθειας αγαθών και υπηρεσιών στους πελάτες
- Διατήρηση και ενίσχυση της μετοχικής αξίας
- Συμμόρφωση με νομικές και κανονιστικές απαιτήσεις

Η Ελληνοαμερικανική Ένωση αποφάσισε να προβεί και να διατηρήσει πλήρη πιστοποίηση κατά ISO/IEC 27001, προκειμένου η αποτελεσματική υιοθέτηση της βέλτιστης πρακτικής ασφάλειας πληροφοριών να μπορεί να επικυρωθεί από ανεξάρτητο τρίτο μέρος, έναν Εγγεγραμμένο Έγκυρο Φορέα Πιστοποίησης (RegisteredCertification Body). Επιπλέον, έχουν υιοθετηθεί πλήρως οι οδηγίες που περιέχονται στους κώδικες πρακτικής ISO/IEC 27017 και ISO/IEC 27018.

Αυτή η πολιτική ισχύει για όλα τα συστήματα, τα άτομα και τις διαδικασίες που αποτελούν τα πληροφοριακά συστήματα του σωματείου, συμπεριλαμβανομένων των μελών του διοικητικού συμβουλίου, των διευθυντών, των εργαζομένων, των προμηθευτών και άλλων τρίτων μερών που έχουν πρόσβαση στα συστήματα της Ελληνοαμερικανικής Ένωσης.

Τα ακόλουθα υποστηρικτικά έγγραφα είναι σχετικά με αυτήν την πολιτική ασφάλειας πληροφοριών και παρέχουν πρόσθετες πληροφορίες σχετικά με τον τρόπο εφαρμογής της:

- Διαδικασία Εκτίμησης και Αντιμετώπισης Κινδύνων
- Δήλωση Εφαρμοσιμότητας
- Διαδικασία αξιολόγησης ασφάλειας πληροφοριών προμηθευτή
- Πολιτική Αποδεκτής Χρήσης Διαδικτύου

- Πολιτική Cloud Computing
- Πολιτική φορητών συσκευών
- Πολιτική Τηλεργασίας
- Πολιτική ελέγχου πρόσβασης
- Διαδικασία διαχείρισης πρόσβασης χρήστη
- Πολιτική Κρυπτογράφησης
- Πολιτική Φυσικής Ασφάλειας
- Πολιτική κατά του κακόβουλου λογισμικού
- Πολιτική δημιουργίας αντιγράφων ασφαλείας
- Πολιτική καταγραφής και παρακολούθησης συστημάτων
- Πολιτική λογισμικού
- Πολιτική διαχείρισης τεχνικών αδυναμιών-ευπαθειών
- Πολιτική Ασφάλειας Δικτύου
- Πολιτική Ηλεκτρονικών Μηνυμάτων
- Πολιτική Ασφαλούς Ανάπτυξης Λογισμικού
- Πολιτική Ασφάλειας Πληροφοριών για Σχέσεις Προμηθευτών
- Πολιτική διαχείρισης Διαθεσιμότητας
- Πολιτική συμμόρφωσης πνευματικής ιδιοκτησίας και πνευματικών δικαιωμάτων
- Πολιτική διατήρησης και προστασίας αρχείων
- Πολιτική Απορρήτου και Προστασίας Προσωπικών Δεδομένων
- Πολιτική εκκαθάρισης γραφείου και εκκαθάρισης οθόνης
- Πολιτική μέσων κοινωνικής δικτύωσης
- Πολιτική Ασφάλειας Ανθρώπινου Δυναμικού

2 Πολιτική Ασφάλειας Πληροφοριών

2.1 Απαιτήσεις Ασφάλειας Πληροφοριών

Ένας σαφής ορισμός των απαιτήσεων για την ασφάλεια των πληροφοριών εντός της Ελληνοαμερικανικής Ένωσης θα συμφωνηθεί και θα διατηρηθεί με τα εσωτερικά τμήματα και διευθύνσεις καθώς και τους πελάτες υπηρεσιών cloud, έτσι ώστε όλη η δραστηριότητα του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) να επικεντρώνεται στην εκπλήρωση αυτών των απαιτήσεων. Επιπλέον, οι νομικές, κανονιστικές και συμβατικές απαιτήσεις θα τεκμηριωθούν και θα εισαχθούν στη διαδικασία σχεδιασμού. Συγκεκριμένες απαιτήσεις σχετικά με την ασφάλεια νέων ή αλλαγμένων συστημάτων ή υπηρεσιών θα ληφθούν υπόψη ως μέρος του σταδίου σχεδιασμού κάθε έργου.

Είναι θεμελιώδης αρχή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών της Ελληνοαμερικανικής Ένωσης ότι οι έλεγχοι που εφαρμόζονται καθοδηγούνται από επιχειρησιακές ανάγκες και αυτό θα κοινοποιείται τακτικά σε όλο το προσωπικό μέσω συναντήσεων και ενημερωτικών εγγράφων.

2.2 Πλαίσιο για τον Καθορισμό Στόχων

Θα χρησιμοποιηθεί ένας τακτικός κύκλος για τον καθορισμό στόχων για την ασφάλεια των πληροφοριών, ώστε να συμπίπτει με τον κύκλο προγραμματισμού του προϋπολογισμού. Αυτό θα διασφαλίσει ότι θα υπάρξει επαρκής χρηματοδότηση για τις δραστηριότητες βελτίωσης που εντοπίστηκαν. Αυτοί οι στόχοι θα βασίζονται σε μια σαφή κατανόηση των επιχειρηματικών/επιχειρησιακών απαιτήσεων, που θα αλλάζουν μέσω της διαδικασίας αναθεώρησης της διοίκησης (management review), κατά τη διάρκεια της οποίας μπορούν να ληφθούν οι απόψεις όλων των σχετικών ενδιαφερομένων.

Οι στόχοι ασφάλειας πληροφοριών θα τεκμηριωθούν για μια συμφωνημένη χρονική περίοδο, μαζί με λεπτομέρειες για τον τρόπο επίτευξής τους. Αυτά θα αξιολογηθούν και θα παρακολουθούνται ως μέρος των επισκοπήσεων της διοίκησης για να διασφαλιστεί ότι παραμένουν έγκυρα. Σε περίπτωση που απαιτούνται τροποποιήσεις, η διαχείριση τους θα γίνεται μέσω της διαδικασίας διαχείρισης αλλαγών.

Σύμφωνα με το ISO/IEC 27001, οι έλεγχοι (controls) που περιγράφονται λεπτομερώς στο Παράρτημα Α του προτύπου (Annex A) θα υιοθετηθούν κατά περίπτωση από την Ελληνοαμερικανική Ένωση. Αυτά θα επανεξετάζονται σε τακτική βάση σε σχέση με τα αποτελέσματα από την αξιολόγηση κινδύνων και σύμφωνα με το σχέδιο αντιμετώπισης κινδύνων για την ασφάλεια των πληροφοριών. Για λεπτομέρειες σχετικά με το ποιοι έλεγχοι του Παραρτήματος Α έχουν εφαρμοστεί και ποιοι έχουν εξαιρεθεί, μπορείτε να ανατρέξετε στη Δήλωση Εφαρμοσιμότητας του Προτύπου.

2.3 Συνεχής Βελτίωση του ISMS

Η πολιτική της Ελληνοαμερικανικής Ένωσης σχετικά με τη συνεχή βελτίωση είναι:

- Συνεχής βελτίωση της αποτελεσματικότητας του ISMS
- Βελτίωση των διαδικασιών ώστε να ευθυγραμμιστούν με την καλή πρακτική (best practice) όπως ορίζεται στο ISO/IEC 27001 και τα σχετικά πρότυπα
- Απόκτηση πιστοποίησης ISO/IEC 27001 και διατήρησή της σε συνεχή βάση
- Αύξηση του επιπέδου προληπτικής δράσης (και της αντίληψης των ενδιαφερομένων για προληπτική δράση) όσον αφορά την ασφάλεια των πληροφοριών
- Προσπάθεια να γίνουν οι διαδικασίες και οι έλεγχοι ασφάλειας πληροφοριών πιο μετρήσιμοι, προκειμένου να παρέχουν μια σωστή βάση για τεκμηριωμένες αποφάσεις
- Επανεξέταση των σχετικών μετρήσεων σε ετήσια βάση για να αξιολογηθεί εάν είναι σκόπιμο να αλλαχθούν, με βάση τα συλλεγόμενα ιστορικά δεδομένα
- Ιδέες για βελτίωση μέσω τακτικών συναντήσεων και άλλων μορφών επικοινωνίας με ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των πελατών υπηρεσιών cloud
- Επανεξέταση ιδεών για βελτίωση σε τακτικές συναντήσεις της διοίκησης, προκειμένου να ιεραρχηθούν και να αξιολογηθούν τα χρονοδιαγράμματα και τα οφέλη

Ιδέες για βελτιώσεις μπορούν να ληφθούν από οποιαδήποτε πηγή, συμπεριλαμβανομένων των εργαζομένων, των πελατών, των προμηθευτών, του προσωπικού πληροφορικής, των αξιολογήσεων κινδύνου και των αναφορών των υπηρεσιών. Μόλις εντοπιστούν, θα καταγράφονται και θα αξιολογούνται ως μέρος των ελέγχων της διοίκησης.

2.4 Τομείς Πολιτικής Ασφάλειας Πληροφοριών

Η Ελληνοαμερικανική Ένωση ορίζει την πολιτική της για την ασφάλεια σε μια ευρεία ποικιλία τομέων που σχετίζονται με την ασφάλεια των πληροφοριών, οι οποίοι περιγράφονται λεπτομερώς σε ένα ολοκληρωμένο σύνολο τεκμηρίωσης των πολιτικών που συνοδεύει αυτήν την γενική πολιτική ασφάλειας πληροφοριών. Αυτό το σύνολο εγγράφων έχει δημιουργηθεί με σκοπό τη διατήρηση των τριών πτυχών της Ασφάλειας Πληροφοριών, δηλαδή της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας των Πληροφοριών.

Κάθε μία από αυτές τις πολιτικές ορίζεται και συμφωνείται από ένα ή περισσότερα άτομα με αρμοδιότητα στον σχετικό τομέα και, μόλις εγκριθεί επίσημα, κοινοποιείται στο κατάλληλο κοινό, τόσο εντός όσο και εκτός του οργανισμού.

Ο παρακάτω πίνακας δείχνει τις επιμέρους πολιτικές του συνόλου τεκμηρίωσης και συνοψίζει το περιεχόμενο κάθε πολιτικής καθώς και το κοινό των ενδιαφερομένων μερών στο οποίο απευθύνεται.

Τίτλος Πολιτικής	Περιοχές Εφαρμογής	Απευθυνόμενο Κοινό
Πολιτική Προστασίας Δεδομένων	PII όπως ορίζεται στο ISO/IEC 27701:2019	Όλοι οι ενδιαφερόμενοι
Πολιτική Αποδεκτής Χρήσης Διαδικτύου	Επιχειρησιακή χρήση του Διαδικτύου, προσωπική χρήση του Διαδικτύου, διαχείριση λογαριασμών Διαδικτύου, ασφάλεια και παρακολούθηση και απαγορευμένες χρήσεις της υπηρεσίας Διαδικτύου	Χρήστες της Υπηρεσίας Διαδικτύου
Πολιτική Cloud Computing	Η δέουσα επιμέλεια, η εγγραφή, η εγκατάσταση, η διαχείριση και η κατάργηση των υπηρεσιών υπολογιστικού νέφους.	Εργαζόμενοι που ασχολούνται με την προμήθεια και διαχείριση υπηρεσιών cloud
Πολιτική Φορητών Συσκευών	Φροντίδα και ασφάλεια κινητών συσκευών όπως φορητοί υπολογιστές, tablet και smartphone, είτε παρέχονται από τον οργανισμό είτε από το άτομο για επαγγελματική χρήση.	Χρήστες κινητών συσκευών που παρέχονται από το σωματείου και BYOD (Bring Your Own Device).
Πολιτική Τηλεργασίας	Θέματα ασφάλειας πληροφοριών κατά τη δημιουργία και τη λειτουργία μιας τοποθεσίας τηλεργασίας και διευθέτησης π.χ. Φυσική ασφάλεια, ασφάλιση και εξοπλισμός	Διοίκηση και εργαζόμενοι που εμπλέκονται στη δημιουργία και τη συντήρηση μιας τοποθεσίας τηλεργασίας
Πολιτική Ελέγχου Πρόσβασης	Εγγραφή και διαγραφή χρήστη, παροχή δικαιωμάτων πρόσβασης, εξωτερική πρόσβαση, έλεγχοι πρόσβασης, πολιτική κωδικού πρόσβασης, ευθύνες χρήστη και έλεγχος πρόσβασης συστημάτων και εφαρμογών.	Εργαζόμενοι που συμμετέχουν στη ρύθμιση και τη διαχείριση του ελέγχου πρόσβασης
Πολιτική Κρυπτογράφησης	Εκτίμηση κινδύνου, επιλογή τεχνικής, ανάπτυξη, δοκιμή και αναθεώρηση κρυπτογραφίας και διαχείριση κλειδιών	Εργαζόμενοι που εμπλέκονται στη δημιουργία και τη διαχείριση της χρήσης τεχνολογίας και τεχνικών κρυπτογράφησης
Πολιτική Φυσικής Ασφάλειας	Ασφαλείς περιοχές, ασφάλεια εντύπων και εξοπλισμού και διαχείριση κύκλου ζωής εξοπλισμού	Όλοι οι Εργαζόμενοι
Πολιτική κατά του κακόβουλου λογισμικού	Τείχη προστασίας, προστασία από ιούς, φιλτράρισμα ανεπιθύμητων μηνυμάτων, εγκατάσταση και σάρωση λογισμικού, διαχείριση ευπάθειας, εκπαίδευση ευαισθητοποίησης χρηστών, παρακολούθηση και	Εργαζόμενοι υπεύθυνοι για την προστασία της υποδομής του οργανισμού από κακόβουλο λογισμικό

Τίτλος Πολιτικής	Περιοχές Εφαρμογής	Απευθυνόμενο Κοινό
	ειδοποιήσεις απειλών, τεχνικές αναθεωρήσεις και διαχείριση περιστατικών κακόβουλου λογισμικού.	
Πολιτική δημιουργίας αντιγράφων ασφαλείας	Κύκλοι αντιγράφων ασφαλείας, δημιουργία αντιγράφων ασφαλείας στο cloud, αποθήκευση εκτός τοποθεσίας, τεκμηρίωση, δοκιμή ανάκτησης και προστασία μέσων αποθήκευσης	Υπάλληλοι υπεύθυνοι για το σχεδιασμό και την εφαρμογή πολιτικών δημιουργίας αντιγράφων ασφαλείας
Πολιτική καταγραφής και παρακολούθησης	Ρυθμίσεις για τη συλλογή συμβάντων, προστασία και αναθεώρηση τους	Εργαζόμενοι υπεύθυνοι για την προστασία της υποδομής του οργανισμού από επιθέσεις
Πολιτική λογισμικού	Αγορά λογισμικού, εγγραφή λογισμικού, εγκατάσταση και αφαίρεση, εσωτερική ανάπτυξη λογισμικού και χρήση λογισμικού στο cloud.	Όλοι οι υπάλληλοι
Πολιτική διαχείρισης τεχνικών αδυναμιών-ευπαθειών	Ορισμός ευπάθειας, πηγές πληροφοριών, ενημερώσεις κώδικα, αξιολόγηση ευπαθειών, προστασία Λειτουργικών Συστημάτων και εκπαίδευση ευαισθητοποίησης	Εργαζόμενοι υπεύθυνοι για την προστασία της υποδομής του οργανισμού από κακόβουλο λογισμικό
Πολιτική Ασφάλειας Δικτύου	Σχεδιασμός ασφάλειας δικτύου, συμπεριλαμβανομένου του διαχωρισμού δικτύου, της περιμετρικής ασφάλειας, των ασύρματων δικτύων και της απομακρυσμένης πρόσβασης, διαχείριση ασφάλειας δικτύου, συμπεριλαμβανομένων ρόλων και ευθυνών, καταγραφής και παρακολούθησης και αλλαγών.	Εργαζόμενοι υπεύθυνοι για το σχεδιασμό, την υλοποίηση και τη διαχείριση δικτύων
Πολιτική Ηλεκτρονικών Μηνυμάτων	Αποστολή και λήψη ηλεκτρονικών μηνυμάτων, παρακολούθηση εγκαταστάσεων ηλεκτρονικών μηνυμάτων και χρήση email.	Χρήστες ηλεκτρονικών μηνυμάτων
Πολιτική Ασφαλούς Ανάπτυξης Λογισμικού	Προδιαγραφές επιχειρηματικών απαιτήσεων, σχεδιασμός συστημάτων, ανάπτυξη και δοκιμή και ανάπτυξη λογισμικού από εξωτερικούς συνεργάτες.	Εργαζόμενοι υπεύθυνοι για το σχεδιασμό, τη διαχείριση και τη σύνταξη κώδικα
Πολιτική Ασφάλειας Σχέσεων Προμηθευτών	Δέουσα επιμέλεια, συμφωνίες προμηθευτών, παρακολούθηση και αναθεώρηση υπηρεσιών, αλλαγές, διαφορές και λήξη των συμβάσεων.	Εργαζόμενοι που συμμετέχουν στη δημιουργία και τη διαχείριση σχέσεων προμηθευτών
Πολιτική διαχείρισης Διαθεσιμότητας	Απαιτήσεις διαθεσιμότητας και σχεδιασμός, παρακολούθηση και αναφορά, μη διαθεσιμότητα, δοκιμή σχεδίων διαθεσιμότητας και διαχείριση αλλαγών.	Εργαζόμενοι υπεύθυνοι για το σχεδιασμό συστημάτων και τη διαχείριση της παροχής υπηρεσιών

Τίτλος Πολιτικής	Περιοχές Εφαρμογής	Απευθυνόμενο Κοινό
Πολιτική συμμόρφωσης IP και πνευματικών δικαιωμάτων	Προστασία της πνευματικής ιδιοκτησίας, του νόμου, των κυρώσεων και της συμμόρφωσης με την άδεια χρήσης λογισμικού.	Όλοι οι υπάλληλοι
Πολιτική διατήρησης και προστασίας αρχείων	Περίοδος διατήρησης για συγκεκριμένους τύπους εγγραφών, χρήση κρυπτογράφησης, επιλογή μέσων, ανάκτηση αρχείων, καταστροφή και επανεξέταση.	Υπάλληλοι υπεύθυνοι για τη δημιουργία και διαχείριση αρχείων
Πολιτική Απορρήτου και Προστασίας Προσωπικών Δεδομένων	Ισχύουσα νομοθεσία περί προστασίας δεδομένων, ορισμοί και απαιτήσεις.	Εργαζόμενοι υπεύθυνοι για το σχεδιασμό και τη διαχείριση συστημάτων που χρησιμοποιούν προσωπικά δεδομένα
Πολιτική εκκαθάρισης γραφείου και εκκαθάρισης οθόνης	Ασφάλεια πληροφοριών που εμφανίζονται σε οθόνες, εκτυπώνονται και διατηρούνται σε αφαιρούμενα μέσα.	Όλοι οι υπάλληλοι
Πολιτική μέσων κοινωνικής δικτύωσης	Οδηγίες για το πώς πρέπει να χρησιμοποιούνται τα μέσα κοινωνικής δικτύωσης κατά την εκπροσώπηση του οργανισμού και κατά τη συζήτηση θεμάτων που σχετίζονται με τον οργανισμό.	Όλοι οι υπάλληλοι
Πολιτική Ασφαλείας Ανθρώπινου Δυναμικού	Προσλήψεις, συμβάσεις εργασίας, συμμόρφωση με την πολιτική, πειθαρχική διαδικασία, καταγγελία	Όλοι οι υπάλληλοι
Πολιτική Αποδεκτής Χρήσης	Δέσμευση των εργαζομένων στις πολιτικές ασφάλειας πληροφοριών του οργανισμού	Όλοι οι υπάλληλοι
Πολιτική διαχείρισης περιουσιακών στοιχείων	Αυτό το έγγραφο καθορίζει τους κανόνες για τον τρόπο διαχείρισης των περιουσιακών στοιχείων από την άποψη της ασφάλειας των πληροφοριών.	Όλοι οι υπάλληλοι

Πίνακας 1: Σύνολο Εγγράφων Πολιτικών

2.5 Εφαρμογή Πολιτικής Ασφάλειας Πληροφοριών

Οι δηλώσεις σχετικά με την πολιτική Ασφάλειας Πληροφοριών που γίνονται σε αυτό το έγγραφο και στο σύνολο των υποστηρικτικών πολιτικών που αναφέρονται στον Πίνακα 1 έχουν ελεγχθεί και εγκριθεί από την ανώτατη διοίκηση της Ελληνοαμερικανικής Ένωσης και πρέπει να τηρούνται. Εάν ένας υπάλληλος δεν συμμορφωθεί με αυτές τις πολιτικές, ενδέχεται να ληφθούν πειθαρχικά μέτρα σύμφωνα με την πειθαρχική διαδικασία των εργαζομένων του οργανισμού.

Ερωτήσεις σχετικά με οποιαδήποτε πολιτική της Ελληνοαμερικανικής Ένωσης θα πρέπει να απευθύνονται σε πρώτο βαθμό στον άμεσο διευθυντή του εργαζομένου.