Πολιτική Ασφάλειας Πληροφοριών

	Ονοματεπώνυμο	Τίτλος	Υπογραφή
Δημιουργός:	Γ. Τζάνος	IT Compliance & Security Officer	
Εγκρίθηκε:	Σπ. Πασχάλης	CEO	

Ιστορικό Αναθεωρήσεων

Ημερομηνία Αναθεώρησης	Έκδοση	Κατάσταση	Αναθεώρηση από	Περίληψη Αλλαγών
29/11/2017	1	Final	IT&T	Management Approval
4/11/2019	2	Final	CSO	Yearly Review, no changes
10/11/2020	2	Final	CSO	Yearly Review, no changes
25/10/2021	3	Final	CSO	Yearly Review, New chapter for Summary of relevant legislation

Εισαγωγή

Ο όμιλος «Attica» χρησιμοποιεί σύγχρονα μέσα πληροφορικής και τηλεπικοινωνιών για τις επιχειρηματικές του δραστηριότητες. Αυτό το επιχειρηματικό περιβάλλον βασίζεται στη χρήση της τεχνολογίας, προκειμένου να συλλέγει, ανταλλάσσει, επεξεργάζεται, αναλύει και αποθηκεύει όγκους δεδομένων που θα παράγουν πολύτιμες πληροφορίες για τον Όμιλο.

Οι επενδύσεις στην τεχνολογία παράγουν το ανταγωνιστικό πλεονέκτημα, το οποίο είναι απαραίτητο για τις επιχειρηματικές δραστηριότητες, αλλά δημιουργούν επίσης νέα πεδία έκθεσης σε κινδύνους. Τα δεδομένα που συλλέγονται, αποθηκεύονται και διαβιβάζονται, περιέχουν σημαντικές πληροφορίες για τον Όμιλο, τους πελάτες του, τους τρίτους συνεργάτες του και το προσωπικό του.

Ο Όμιλος «Attica» αναγνωρίζει την αξία των πληροφοριών για την εκτέλεση των καθημερινών εργασιών, καθώς και την ανάγκη διαχείρισης των κινδύνων όσον αφορά στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα αυτών των πληροφοριών. Το παρόν έγγραφο, που περιγράφει την Πολιτική για την Ασφάλεια των Πληροφοριών του Ομίλου, αποτελεί την άποψη της Διοίκησης για τα θέματα ασφάλειας των πληροφοριών. Παρέχει την απαραίτητη κατεύθυνση, υποστήριξη και δέσμευση από τη Διοίκηση σε θέματα ασφάλειας πληροφοριών σύμφωνα με τις επιχειρηματικές απαιτήσεις και τους σχετικούς νόμους και κανονισμούς.

Η εν λόγω Πολιτική έχει αναπτυχθεί για να προστατεύει όλα τα συστήματα του Ομίλου «Attica» σε επαρκές επίπεδο από γεγονότα που μπορεί να θέσουν σε κίνδυνο την επιχειρηματική δραστηριότητα. Τα γεγονότα αυτά περιλαμβάνουν ατυχήματα καθώς και συμπεριφορές που έχουν σχεδιαστεί σκόπιμα για να προκαλέσουν δυσκολίες.

Η εν λόγω πολιτική έχει βασιστεί στις βέλτιστες διεθνείς πρακτικές και πρότυπα για την ασφάλεια των πληροφοριών (ISO/IEC 27001:2013). Σκοπός της παρούσας πολιτικής είναι να υποστηρίξει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ-ISMS), το οποίο θα διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών και των πληροφοριακών συστημάτων του Ομίλου.

Δήλωση Πολιτικής

Ο Όμιλος «Attica» επιδιώκει να διασφαλίσει ότι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών της διατηρούνται με την εφαρμογή βέλτιστων πρακτικών για την ελαχιστοποίηση του κινδύνου.

Ποιος επηρεάζεται από την Πολιτική;

Η Πολιτική ισχύει για όλους τους εργαζόμενους του Ομίλου «Attica». Κάθε εργαζόμενος έχει την ευθύνη να σέβεται, να τηρεί και να επιβάλλει την παρούσα πολιτική. Ισχύει επίσης για τους εργολάβους και τους επισκέπτες, που δεν απασχολούνται από τον Όμιλο, αλλά προσλαμβάνονται για να εργαστούν με πληροφορίες του Ομίλου ή έχουν πρόσβαση σε αυτές, π.χ. εργολάβοι συντήρησης υπολογιστών, σύμβουλοι, ελεγκτές κ.λπ.

Πεδίο Εφαρμογής της Πολιτικής

Η Πολιτική εφαρμόζεται σε όλες τα σημεία που διαθέτουν πρόσβαση στα συστήματα του Ομίλου «Attica» (συμπεριλαμβανομένης της οικιακής χρήσης). Όταν υπάρχουν σύνδεσμοι που επιτρέπουν σε οντότητες εκτός του Ομίλου να έχουν πρόσβαση σε πληροφορίες του Ομίλου «Attica», η οντότητα πρέπει να επιβεβαιώνει ότι οι πολιτικές ασφαλείας που εφαρμόζει πληρούν τις απαιτήσεις ασφαλείας μας ή ότι ο κίνδυνος είναι κατανοητός και περιορισμένος. Η πολιτική εφαρμόζεται σε όλα τα συστήματα και όλες τις πληροφορίες, είτε πρόκειται για διοικητικές είτε για άλλες.

Τα δεδομένα που είναι αποθηκευμένα σε χειροκίνητα και ηλεκτρονικά συστήματα που χρησιμοποιεί ο Όμιλος «Attica» αποτελούν ένα εξαιρετικά πολύτιμο περιουσιακό στοιχείο. Η αυξανόμενη εξάρτηση από την τεχνολογία των πληροφοριών για την παροχή υπηρεσιών καθιστά απαραίτητο να διασφαλιστεί ότι τα συστήματα αυτά αναπτύσσονται, λειτουργούν, χρησιμοποιούνται και συντηρούνται με ασφαλή τρόπο, συμπεριλαμβανομένων αρχείων που διατηρούνται σε έγχαρτη μορφή. Η αυξανόμενη ανάγκη μετάδοσης πληροφοριών μέσω δικτύων υπολογιστών, καθιστά τα δεδομένα πιο ευάλωτα σε τυχαία ή σκόπιμη μη εξουσιοδοτημένη τροποποίηση ή δημοσιοποίηση.

Επιπλέον, εφαρμόζεται σε όλα τα περιουσιακά στοιχεία που χρησιμοποιούνται για τη χρήση πληροφοριών, όπως συστήματα, εφαρμογές, εξοπλισμός γραφείου, τηλεπικοινωνιακός εξοπλισμός κ.λπ.

Στόχοι Πολιτικής

- Να εξασφαλίσει ότι κάθε μέλος του προσωπικού έχει την κατάλληλη επίγνωση και μέριμνα για την ασφάλεια των συστημάτων πληροφορικής και επαρκή εκτίμηση της ευθύνης του για την ασφάλεια των πληροφοριών.
- Να διασφαλίσει ότι όλοι οι συνεργάτες και οι υπάλληλοί τους έχουν την κατάλληλη επίγνωση και μέριμνα για την ασφάλεια των πληροφοριών του Ομίλου «Attica».
- Να παρέχει ένα πλαίσιο, για τη θέσπιση προτύπων, διαδικασιών για την εφαρμογή της ασφάλειας επί των υπολογιστικών συστημάτων.
- Να καθορίσει τις αρμοδιότητες του Ομίλου «Attica».
- Να διασφαλίσει ότι όλο το προσωπικό έχει επίγνωση της ευθύνης του και ότι γνωρίζει ότι η μη συμμόρφωση με την Πολιτική για την Ασφάλεια των Πληροφοριών αποτελεί πειθαρχικό αδίκημα που μπορεί να περιλαμβάνει μέτρα έως και απόλυση με συνοπτικές διαδικασίες. Κάθε ενέργεια που πραγματοποιείται είναι σύμφωνη με τις κατάλληλες πολιτικές ανθρώπινου δυναμικού του Ομίλου «Attica».

Σκοπός

Σκοπός του παρόντος εγγράφου είναι να αποτυπώσει τη δέσμευση της Διοίκησης και να θέσει τα θεμέλια για την εφαρμογή ενός εσωτερικού Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ - ISMS).

Η καθιέρωση του ΣΔΑΠ θα παρέχει εύλογη διασφάλιση του επιπέδου ασφάλειας των πληροφοριών του Ομίλου από όλες τις απειλές, εσωτερικές και εξωτερικές, σκόπιμες ή τυχαίες, οι οποίες στοχεύουν σε συγκεκριμένες πληροφορίες, φορείς πληροφοριών ή πηγές πληροφοριών.

Με τη χρήση του ΣΔΑΠ ο Όμιλος «Attica» στοχεύει σε:

- Παροχή της καλύτερης δυνατής προσπάθειας για τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας όλων των πληροφοριών ανάλογα με την αξία και την κρισιμότητά τους για τη λειτουργία της
- Δημιουργία, συντήρηση και δοκιμή ενός Σχεδίου Επιχειρησιακής Συνέχειας (ΣΕΣ-BCP)
- Συμμόρφωση με όλες τις κανονιστικές, νομικές και συμβατικές απαιτήσεις
- Εκπαίδευση, κατάρτιση και βελτίωση της ευαισθητοποίησης όλων των εργαζομένων του Ομίλου «Attica» σε θέματα ασφάλειας πληροφοριών
- Αναφορά, παρακολούθηση και διερεύνηση κάθε πραγματικού ή ύποπτου περιστατικού ασφαλείας και παραβίασης της παρούσας Πολιτικής.

Για τη διαχείριση του ΣΔΑΠ, ο Όμιλος έχει ορίσει έναν Υπεύθυνο Ασφάλειας των Πληροφοριών, ο οποίος εργάζεται υπό την εποπτεία του Διευθυντή της Τεχνολογίας της Πληροφορίας και των Επικοινωνιών (ΤΠΕ). Ο Υπεύθυνος Ασφάλειας των Πληροφοριών έχει την αρμοδιότητα να δημιουργεί και περιοδικά να τροποποιεί τα δικαιολογητικά έγγραφα για την Ασφάλεια Πληροφοριών (οδηγοί αναφοράς, διαδικασίες κ.λπ.), τα οποία είναι σύμφωνα με την εν λόγω πολιτική. Τα εν λόγω δικαιολογητικά έγγραφα έχουν το ίδιο πεδίο εφαρμογής και την ίδια αρμοδιότητα, σαν να περιλαμβάνονταν στο παρόν έγγραφο.

Η διαφύλαξη της ασφάλειας των πληροφοριών αποτελεί κύρια ευθύνη της Διοίκησης και ένα κρίσιμο καθήκον. Ωστόσο, η καθημερινή λειτουργία των ελέγχων που απορρέουν από την εν λόγω πολιτική και αφορούν στην ασφαλή λειτουργία του Ομίλου είναι ευθύνη και καθήκον όλων των εργαζομένων και των τρίτων που συνεργάζονται με τον Όμιλο.

Η Διοίκηση δεσμεύεται να:

- Διασφαλίσει ότι οι στόχοι ασφάλειας των πληροφοριών προσδιορίζονται και ανταποκρίνονται στις απαιτήσεις του Ομίλου
- Διαμορφώσει την αξιολόγηση και την έγκριση της πολιτικής για την ασφάλεια των πληροφοριών
- Αξιολογήσει την αποτελεσματικότητα υλοποίησης της πολιτικής για την ασφάλεια των πληροφοριών
- Παρέχει σαφή κατεύθυνση και εμφανή διοικητική υποστήριξης για τις πρωτοβουλίες ασφαλείας
- Παρέχει τους αναγκαίους πόρους για την ασφάλεια των πληροφοριών
- Εγκρίνει την ανάθεση συγκεκριμένων ρόλων και αρμοδιοτήτων για την ασφάλεια των πληροφοριών σε ολόκληρο τον Όμιλο
- Σχεδιάσει και να οργανώσει πρόγραμμα ευαισθητοποίησης σχετικά με την ασφάλεια των πληροφοριών

Σχετική Νομοθεσία

Ευρωπαϊκό Κοινοβούλιο - ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 - Προστασία φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Οργανισμός της Ευρωπαϊκής Ένωσης για τα Θεμελιώδη Δικαιώματα - Εγχειρίδιο σχετικά με την προστασία των ιδιωτικών δεδομένων.

Ο νόμος 4624/2019 βασίζεται στις διατάξεις του Κανονισμού (ΕΕ) 2016/679 («ΓΚΠΔ») και ενσωματώνει τις διατάξεις της Οδηγίας (ΕΕ) 2016/680 στην Ελληνική νομοθεσία.

Ευρωπαϊκό Κοινοβούλιο / Ελληνική Αρχή για την Ασφάλεια και το Απόρρητο των Επικοινωνιών - Οδηγία 2002/58/ΕΚ - ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για το απόρρητο και τις ηλεκτρονικές επικοινωνίες).

Πηγές που μπορούν να χρησιμοποιηθούν για την ανάκτηση πληροφοριών σχετικά με την ισχύουσα Ελληνική και Ευρωπαϊκή νομοθεσία είναι οι παρακάτω ιστότοποι:

- https://eur-lex.europa.eu/
- http://www.et.gr/
- http://www.dpa.gr/
- http://www.adae.gr/
- https://www.hellenicparliament.gr/
- https://diavgeia.gov.gr

Συμμόρφωση

Η συμμόρφωση όλου του προσωπικού με την Πολιτική Ασφάλειας είναι ο πιο κρίσιμος έλεγχος για τη διασφάλιση των πληροφοριών του Ομίλου. Τα συστήματα, οι εφαρμογές, ο εξοπλισμός και τα δεδομένα της Τεχνολογίας των Πληροφοριών και Επικοινωνιών (ΤΠΕ) πρέπει να προστατεύονται. Προκειμένου να διασφαλιστεί ότι το επίπεδο έκθεσης στους σχετικούς κινδύνους είναι αποδεκτό, πρέπει να ενεργοποιούνται σε τακτά χρονικά διαστήματα ανεξάρτητες αξιολογήσεις της ασφάλειας των πληροφοριών. Οι εν λόγω αξιολογήσεις πρέπει να διενεργούνται από άτομα ανεξάρτητα από τον υπό εξέταση τομέα, δηλαδή από το τμήμα Εσωτερικού Ελέγχου, από εξωτερικούς ελεγκτές ή από τρίτο οργανισμό που ειδικεύεται σε τέτοιου είδους αξιολογήσεις.

Αναμένεται ότι όλοι οι εργαζόμενοι του Ομίλου «Attica», οι συνεργάτες ή τα τρίτα μέρη θα συμμορφώνονται με τις απαιτήσεις που παρατίθενται στο πλαίσιο του ΣΔΑΠ.

Η μη συμμόρφωση με τις πολιτικές ασφαλείας θα διερευνάται και μπορεί να οδηγήσει σε πειθαρχικά μέτρα ανάλογα με την παράβαση.

Η μη εφαρμογή τυχόν απαίτησης της πολιτικής δεν σημαίνει και έγκριση από τον Όμιλο.