

Π02 Πολιτική Ασφάλειας Πληροφοριών

Εισαγωγή

Αυτή η πολιτική ισχύει για την Krypto Security (Cyprus) Ltd και συγκεκριμένα για το προσωπικό, τον εξοπλισμό και εφαρμογές πληροφορικής της εταιρίας, με σκοπό την εξασφάλιση της αποτελεσματικής ασφάλειας των πληροφοριών που η εταιρεία επεξεργάζεται, λαμβάνοντας Οργανωτικά και Τεχνικά μέτρα για την διασφάλιση της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας των πληροφοριών αυτών.

Το πεδίο εφαρμογής της Πολιτικής περιλαμβάνει όλα τα Τμήματα της εταιρείας και κατά συνέπεια όλες τις δραστηριότητες της.

Ως αρχικό μέσο μείωσης και μετριασμού κινδύνων κυβερνοαπειλών στην εταιρεία, είναι η χρήση της ασφαλούς υποδομής τεχνολογίας πληροφοριών που παρέχεται για την επίτευξη της καθημερινής εργασίας του προσωπικού.

Στόχοι

Η εταιρεία έθεσε τους παρακάτω σκοπούς ασφάλειας πληροφοριών · οι μετρήσιμοι στόχοι και οι δείκτες τους καθορίζονται ετησίως και παρακολουθούνται σύμφωνα με τη Δ15

- Να παρέχεται στο προσωπικό, κατεύθυνση και υποστήριξη στην ασφάλεια πληροφοριών σύμφωνα με τις επιχειρησιακές απαιτήσεις και τους σχετικούς νόμους και τους κανονισμούς.
- Να θεσπίσει το κατάλληλο διοικητικό πλαίσιο που θα δύναται να ελέγξει την εφαρμογή και τη λειτουργία της ασφαλείας πληροφοριών μέσα στην εταιρεία.
- Να εξασφαλίζει ότι το προσωπικό και οι συνεργάτες της εταιρείας γνωρίζουν, καταλαβαίνουν και εκπληρώνουν τις ευθύνες τους στην ασφάλεια πληροφοριών.
- Να προσδιορίζει και να προστατεύει τα περιουσιακά στοιχεία της εταιρείας με τον καθορισμό των κατάλληλων οργανωτικών και τεχνικών μέτρων ασφάλειας.
- Να εξασφαλίζει ότι οι πληροφορίες προστατεύονται ανάλογα με τη σημασία που έχουν για την εταιρεία.
- Να εξασφαλίζει μέτρα ασφάλειας στις υποδομές των δικτύων και επεξεργασίας πληροφοριών.
- Να εξασφαλίζει την προστασία των περιουσιακών στοιχείων και των πληροφοριών της εταιρείας, στις οποίες έχουν πρόσβαση συνεργάτες.
- Να εξασφαλίζει τη διαθεσιμότητα των υποδομών επεξεργασίας πληροφοριών.
- Να συμμορφώνεται με νομικές, κανονιστικές και συμβατικές απαιτήσεις και τις απαιτήσεις των ενδιαφερόμενων μερών που αφορούν την ασφάλεια πληροφοριών.

Για την επίτευξη των παραπάνω στόχων που η εταιρεία έχει θέσει, η Διεύθυνση θα παρέχει τους απαραίτητους πόρους για την εφαρμογή τεχνικών και οργανωτικών μέτρων. Ενδεικτικά και όχι περιοριστικά αναφέρονται:

Π02 Πολιτική Ασφάλειας Πληροφοριών

- Τεχνικά μέτρα για την ασφάλεια των διακομιστών (firewall και κωδικοί ασφάλειας, domain, Microsoft)
- Τεχνικά μέτρα για την ασφάλεια των συστημάτων (firewall, έλεγχος ταυτότητας πολλαπλών παραγόντων – MFA)
- Οργάνωση ρόλων και αρμοδιοτήτων (συμφωνία εμπιστευτικότητας και μη δημοσίευσης με το προσωπικό και τους συνεργάτες)
- Καθορισμό Υπεύθυνου Προστασίας Δεδομένων (εξωτερικός συνεργάτης)
- Διεξαγωγή Σεμιναρίων για ενημέρωση αλλά και καλλιέργεια κουλτούρας στο προσωπικό
- Διενέργεια περιοδικών ελέγχων για την επισκόπηση της καταλληλότητας και αποτελεσματικότητας των μέτρων ασφάλειας (ISO 9001 & ISO 27001)
- Διαμερισματοποίηση του Δικτύου
- Φυσική Ασφάλεια διακομιστών
- Διενέργεια Εκτίμησης Επικινδυνότητας και Εκτίμησης Αντικτύπου όπου επιβάλλεται
- Υπογραφή Συμφωνίας Ανάθεσης Επεξεργασίας, με εξωτερικούς Συνεργάτες εκεί που γίνεται Επεξεργασία Δεδομένων
- Πολιτική Ασφάλειας Κωδικών
- Πολιτική Καθαρού Γραφείου
- Πολιτική Αντιγράφων Ασφαλείας
- Πολιτική Προστασίας Δεδομένων
- Πολιτική Ασφάλειας Εξοπλισμού εκτός Κτιρίου
- Πολιτική Επιχειρησιακής Συνέχειας
- Πολιτική Αποδεκτής Χρήσης
- Πολιτική Επαφής με Ομάδες Ειδικού Ενδιαφέροντος
- Πολιτική Ασφάλειας Cloud
- Πολιτική Threat Intelligence
- Πολιτική Διαχείρισης Έργων
- Πολιτική Μεταφοράς Πληροφορίας
- Πολιτική Διαχείρισης Πνευματικών Δικαιωμάτων
- Πολιτική Αποθήκευσης, Διαχείρισης, Φύλαξης και Καταστροφής Ηλεκτρονικών Αρχείων
- Πολιτική Προστασίας από Ιούς και Κακόβουλο Λογισμικό
- Πολιτική Δοκιμών Ευπάθειας και Διείσδυσης
- Πολιτική Καταγραφής (Logging)
- Πολιτική Κρυπτογράφησης Δεδομένων
- Πολιτική Patching

Π02 Πολιτική Ασφάλειας Πληροφοριών

- Πολιτική Απόσυρσης ή Επαναχρησιμοποίησης Εξοπλισμού
- Πολιτική Web Filtering
- Πολιτική Αρχιτεκτονικής και Αρχών Μηχανικής Ασφαλών Συστημάτων
- Πολιτική Προστασίας Συστημάτων κατά τη Διάρκεια Audit
- Πολιτική Cookies
- Μια σειρά Πολιτικών και Διαδικασιών κάτω από το Διεθνές Πρότυπο 27001:2022

Επεξεργασία δεδομένων

Τα δεδομένα αποτελούν κρίσιμο περιουσιακό στοιχείο της εταιρείας και η προστασία τους σε όλα τα στάδια της επεξεργασίας τους είναι απαραίτητη. Για το λόγο αυτό πρέπει τα δεδομένα να :

- διαβαθμίζονται ανάλογα με τον βαθμό εμπιστευτικότητάς τους (Δημόσια Χρήση, Εσωτερική Χρήση, Εμπιστευτικό, Απόρρητο) και αντίστοιχα να τίθενται οι σχετικοί περιορισμοί χρήσης, κοινοποίησης και επεξεργασίας.
- αντιμετωπίζονται με εμπιστευτικότητα και να χρησιμοποιούνται αποκλειστικά για το σκοπό που επεξεργάζονται.
- αποθηκεύονται μόνο σε εγκεκριμένα εταιρικά συστήματα (διακομιστές της εταιρείας, Microsoft OneDrive / SharePoint).

Επιπρόσθετα

- Η χρήση αφαιρούμενων μέσων αποθήκευσης (USB, εξωτερικοί δίσκοι) επιτρέπεται μόνο με έγκριση του ΥΑΠ και κρυπτογράφηση
- Οι κωδικοί πρόσβασης πρέπει να προστατεύονται.
- Να αποφεύγεται η αχρείαστη εκτύπωση και αντιγραφή των πληροφοριών, μειώνοντας έτσι τον κίνδυνο να καταλήξουν σε μη εξουσιοδοτημένα άτομα.
- Ο κάθε χρήστης εκτυπώνει σε συγκεκριμένο προκαθορισμένο εκτυπωτή.
- Η κοινοποίηση των εμπιστευτικών πληροφοριών να γίνεται μόνο σε εξουσιοδοτημένα άτομα.
- Να χρησιμοποιούνται συσκευές κατατεμαχισμού (shreders) για την καταστροφή εμπιστευτικών πληροφοριών / εγγράφων με ανάλογες προδιαγραφές.
- Να εφαρμόζεται πολιτική καθαρού γραφείου.
- Η φύλαξη εμπιστευτικών εγγράφων είναι υποχρεωτική.

Δέσμευση



Κωδικός:	Π02
Έκδοση:	02
Ημερομηνία:	22/09/2026

Π02 Πολιτική Ασφάλειας Πληροφοριών

Η Διεύθυνση της εταιρείας είναι αρμόδια και δεσμεύεται ώστε να παρέχει όλους τους απαραίτητους πόρους για να ικανοποιήσει όλες τις απαιτήσεις της ασφαλείας πληροφοριών για την εταιρεία και να βελτιώνει συνεχώς το σύστημα διαχείρισης ασφαλείας πληροφοριών.

Μέσα στο πλαίσιο της γενικότερης πολιτικής εκπαίδευσης του προσωπικού, η εταιρεία θα παρέχει ευκαιρίες εκπαίδευσης και στους τομείς που καλύπτονται από τη συγκεκριμένη πολιτική, έτσι, ώστε να μεγιστοποιούνται τα οφέλη που παρέχει η τεχνολογία, μειώνοντας παράλληλα τους κινδύνους που μπορεί να προέρχονται από τη μη σωστή χρήση της. Το προσωπικό οφείλει να συμμετέχει στα σχετικά προγράμματα εκπαίδευσης.

Η πολιτική είναι διαθέσιμη σε όλα τα ενδιαφερόμενα μέρη, αρμόδιες αρχές και προσωπικό της εταιρείας.

Η πολιτική αυτή θα αναθεωρείται περιοδικά, τουλάχιστον ετησίως, στο πλαίσιο της Ανασκόπησης Διοίκησης, και αν κρίνεται αναγκαίο, θα τροποποιείται ανάλογα.

Διευθύνων Σύμβουλος

22/09/2026