Εταιρική Πολιτική 7
Παγκόσμια Ασφάλεια Πληροφοριών και Συστημάτων

Σκοπός

Σκοπός της παρούσας Πολιτικής είναι να εκφράσει τη δέσμευση της Stryker στη διατήρηση κατάλληλων ελέγχων ασφαλείας για τις πληροφορίες, τα συστήματα και τις λειτουργίες της, πάντα σύμφωνα με την ισχύουσα νομοθεσία.

Πεδίο εφαρμογής

Η παρούσα Πολιτική ισχύει για όλους τους εργαζομένους της Stryker και τα τρίτα μέρη (π.χ. παρόχους, αναδόχους, αντιπροσώπους) που ενεργούν εκ μέρους της Stryker ανεξάρτητα από την τοποθεσία. Αν οποιαδήποτε διάταξη αυτής της Πολιτικής δεν συμμορφώνεται με την τοπική ή περιφερειακή νομοθεσία που ισχύει για κάποια συγκεκριμένη νομική οντότητα της Stryker, η εκάστοτε οντότητα θα πρέπει, στον βαθμό που απαιτείται, να προσθέσει ένα παράρτημα στην παρούσα Πολιτική, με το οποίο θα συμμορφώνεται με την τοπική ή περιφερειακή νομοθεσία, δεδομένου ότι η αναθεωρημένη πολιτική θα συνάδει στον μέγιστο δυνατό βαθμό με τις αρχές που περιέχονται σε αυτήν την Πολιτική. Αυτού του είδους τα παραρτήματα πρέπει να εγκρίνονται από το CISO. Στις περιπτώσεις στις οποίες δεν προστίθεται τοπικό ή περιφερειακό παράρτημα, θα συνεχίσουν να ισχύουν όλες οι διατάξεις της παρούσας Πολιτικής στον βαθμό που υπαγορεύει η ισχύουσα νομοθεσία.

Βασικές πολιτικές

Η Stryker θα συμμορφώνεται με όλους τους νόμους που διέπουν την ασφάλεια των προϊόντων και των συστημάτων της. Επιπλέον, η Stryker δεσμεύεται να τηρεί τα πρότυπα που ορίζονται παρακάτω.

1. **Διορισμός ανώτερου στελέχους ασφάλειας πληροφοριών (CISO):** Το CISO είναι υπεύθυνο για τον προσδιορισμό και την επιβολή της αποτελεσματικής λειτουργίας του παγκόσμιου προγράμματος ασφάλειας πληροφοριών της Stryker και για την ευθυγράμμιση των πρωτοβουλιών ασφαλείας με τα εταιρικά προγράμματα και τους επιχειρηματικούς στόχους για την προστασία στοιχείων πληροφοριών, προϊόντων, συστημάτων και τεχνολογιών.

2. **Εφαρμογή πολιτικών ασφαλείας και διαχειριστικών και διοικητικών δομών:** Η Stryker, μέσω των ισχυόντων Συστημάτων Διαχείρισης Ποιότητας, Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών, προτύπων Διακυβέρνησης Πληροφοριών, προτύπων Αποδεκτής Χρήσης, του Προγράμματος Απόκρισης σε Συμβάντα, καθώς και των σχετικών προτύπων και διαδικασιών, θα εφαρμόσει κατάλληλους διαχειριστικούς, τεχνικούς και πραγματικούς ελέγχους ασφαλείας.

3. **Αξιολόγηση τρίτων μερών:** Πριν την απασχόληση οποιουδήποτε τρίτου μέρους που έχει πρόσβαση στα δίκτυα ή τα ευαίσθητα ηλεκτρονικά δεδομένα της Stryker ή που παρέχει ηλεκτρονικές λύσεις ή λογισμικό για εσωτερική χρήση ή χρήση ενός προϊόντος ή υπηρεσίας που προσφέρει η Stryker, πρέπει να ολοκληρώνεται η παγκόσμια διαδικασία αξιολόγησης ασφάλειας.

4. **Χρήση του εξοπλισμού και των συστημάτων της Stryker:** Οποιοσδήποτε εργαζόμενος της Stryker ή τρίτο μέρος που έχει πρόσβαση στον εξοπλισμό ή τα συστήματα της Stryker θα χρησιμοποιεί τέτοιο εξοπλισμό και συστήματα σύμφωνα με τις ισχύουσες απαιτήσεις αποδεκτής χρήσης.

Ευθύνες

Αποτελεί ευθύνη όλων των εργαζομένων της Stryker και των τρίτων μερών να συμμορφώνονται με την παρούσα Πολιτική και κάθε ισχύον πρότυπο και διαδικασία εφαρμογής. Το CISO, σε συνεργασία με άλλες κατάλληλες λειτουργίες και επιχειρηματικές μονάδες, πρέπει να εντοπίζει τυχόν επιπλέον πρότυπα και πολιτικές που απαιτούνται για συμμόρφωση με αυτήν την Πολιτική και πρέπει να προετοιμάζει και να εφαρμόζει αυτά τα πρότυπα και τις πολιτικές.

Συμμόρφωση

Η Stryker απαιτεί από όλους του εργαζομένους και τα τρίτα μέρη να συμμορφώνονται με την παρούσα Πολιτική. Αν έχετε ερωτήσεις σχετικά με αυτήν την Πολιτική ή τις σχετικές διαδικασίες ή αν έχετε κάποια ανησυχία σχετικά με το πρόγραμμα ασφάλειας της Stryker, επικοινωνήστε με τον τοπικό εκπρόσωπο Ανθρώπινου Δυναμικού της Stryker, ένα στέλεχος συμμόρφωσης, έναν νομικό σύμβουλο ή τη Γραμμή Βοήθειας για Θέματα Δεοντολογίας. Η Stryker θα διατηρήσει τέτοιου είδους αναφορές εμπιστευτικές, σύμφωνα με τις πολιτικές και τις διαδικασίες της Γραμμής Βοήθειας.