

# Information Security Policy

## Information Security Policy

ΔΕΚ.ΘΑΟΝ

Monday, September 1, 2025

Version 01.02

## Πίνακας περιεχομένων

<b>1. ΕΙΣΑΓΩΓΗ</b>	<b>4</b>
ΑΝΤΙΚΕΙΜΕΝΙΚΟΣ ΣΚΟΠΟΣ	4
ΣΚΟΠΟΣ	4
ΕΜΒΕΛΕΙΑ	4
ΕΠΙΒΟΛΗ	4
<b>2. ΤΑΞΙΝΟΜΗΣΗ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ ΚΑΙ ΈΛΕΓΧΟΣ</b>	<b>5</b>
ΛΟΓΟΔΟΣΙΑ ΓΙΑ ΠΕΡΙΟΥΣΙΑΚΑ ΣΤΟΙΧΕΙΑ	5
ΤΑΞΙΝΟΜΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ	5
ΑΠΟΔΕΚΤΗ ΧΡΗΣΗ	6
<b>3. ΕΤΑΙΡΙΚΕΣ ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ &amp; ΕΠΙΣΚΕΠΤΩΝ</b>	<b>6</b>
ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΟΡΙΣΜΟ ΤΩΝ ΘΕΣΕΩΝ ΕΡΓΑΣΙΑΣ ΚΑΙ ΤΗΝ ΣΤΕΛΕΧΩΣΗ	7
ΠΡΟΣΒΑΣΗ ΓΙΑ ΤΟΥΣ ΕΠΙΣΚΕΠΤΕΣ	7
ΕΚΠΑΙΔΕΥΣΗ	7
ΑΝΤΑΠΟΚΡΙΣΗ ΣΕ ΠΕΡΙΣΤΑΤΙΚΑ	7
<b>4. ΔΙΑΧΕΙΡΙΣΗ 3ΟΥ ΜΕΡΟΥΣ</b>	<b>8</b>
<b>5. ΑΣΦΑΛΕΙΑ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΧΩΡΟΥ</b>	<b>9</b>
ΑΣΦΑΛΕΙΣ ΠΕΡΙΟΧΕΣ	9
ΑΣΦΑΛΕΙΑ ΕΞΟΠΛΙΣΜΟΥ	9
<b>6. ΛΕΙΤΟΥΡΓΙΑ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ Η/Υ ΚΑΙ ΔΙΚΤΥΟΥ</b>	<b>10</b>
ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ	10
ΠΡΟΣΤΑΣΙΑ ΛΟΓΙΣΜΙΚΟΥ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ	11
ΧΕΙΡΙΣΜΟΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΟΡΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ	11
ΠΡΟΣΤΑΣΙΑ ΥΠΗΡΕΣΙΩΝ ΔΙΚΤΥΟΥ	11
ΑΝΤΑΛΛΑΓΗ ΔΕΔΟΜΕΝΩΝ	12
<b>7. ΠΟΛΙΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ</b>	<b>12</b>
ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ	13
ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΟΤΥΠΑ ΚΑΙ ΑΛΓΟΡΙΘΜΟΙ	13
ΙΣΧΥΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΚΑΙ ΜΗΚΟΣ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΚΛΕΙΔΙΟΥ	13
<b>8. ΈΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ</b>	<b>13</b>
ΈΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΣΕ ΕΦΑΡΜΟΓΕΣ/ΣΥΣΤΗΜΑΤΑ/ΥΠΟΛΟΓΙΣΤΕΣ	14
ΠΟΛΙΤΙΚΗ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ	14
ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΠΡΟΣΒΑΣΗ	15
<b>9. ΚΑΤΑΓΡΑΦΗ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗ</b>	<b>15</b>
<b>10. ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ</b>	<b>16</b>
ΜΟΝΤΕΛΑ ΑΝΑΠΤΥΞΗΣ CLOUD COMPUTING	16
ΜΟΝΤΕΛΑ ΥΠΗΡΕΣΙΩΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ	17
ΠΑΡΟΧΟΙ CLOUD	18
<b>11. ΣΥΝΕΧΗΣ ΒΕΛΤΙΩΣΗ</b>	<b>18</b>
ΕΙΣΕΡΧΟΜΕΝΑ ΓΙΑ ΤΗΝ ΣΥΝΕΧΗ ΒΕΛΤΙΩΣΗ	18
ΔΙΑΧΕΙΡΙΣΗ ΒΕΛΤΙΩΣΕΩΝ	19

ΣΧΕΔΙΟ ΣΥΝΕΧΟΥΣ ΒΕΛΤΙΩΣΗΣ.....	19
ΕΞΕΡΧΟΜΕΝΑ.....	19
ΑΝΑΣΚΟΠΗΣΗ ΑΠΟ ΤΗΝ ΔΙΟΙΚΗΣΗ.....	20
ΣΥΧΝΟΤΗΤΑ ΕΝΕΡΓΕΙΩΝ ΣΥΝΕΧΟΥΣ ΒΕΛΤΙΩΣΗΣ.....	20
<b>12. ΑΝΑΠΤΥΞΗ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΑΛΛΑΓΩΝ .....</b>	<b>20</b>
SECURITY REQUIREMENTS OF SYSTEMS .....	21
ΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΔΟΚΙΜΩΝ .....	21
<b>13. ΔΙΑΧΕΙΡΙΣΗ ΔΙΑΜΟΡΦΩΣΗΣ .....</b>	<b>21</b>
ΒΑΣΙΚΗ ΔΙΑΜΟΡΦΩΣΗ .....	21
<b>14. ΔΙΑΡΡΟΗ ΔΕΔΟΜΕΝΩΝ .....</b>	<b>22</b>
<b>15. ΚΑΛΥΨΗ / ΨΕΥΔΩΝΥΜΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ .....</b>	<b>23</b>
ΓΕΝΙΚΕΣ ΑΡΧΕΣ.....	23
ΜΕΘΟΔΟΙ ΑΠΟΡΡΙΨΗΣ ΔΕΔΟΜΕΝΩΝ .....	23
ΔΙΑΓΡΑΦΗ ΔΕΔΟΜΕΝΩΝ ΟΠΟΥ ΕΜΠΛΕΚΟΝΤΑΙ ΕΞΩΤΕΡΙΚΟΙ ΠΑΡΟΧΟΙ .....	24
ΔΙΑΓΡΑΦΗ ΔΕΔΟΜΕΝΩΝ ΣΕ MOBILE DEVICES .....	24
<b>16. WEB FILTERING.....</b>	<b>24</b>
<b>17. THREAT INTELLIGENCE .....</b>	<b>25</b>
<b>18. ΔΙΑΧΕΙΡΙΣΗ ΓΙΑ ΤΗΝ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ .....</b>	<b>25</b>
<b>19. ΤΗΛΕΡΓΑΣΙΑ.....</b>	<b>26</b>

# 1. Εισαγωγή

## Αντικειμενικός Σκοπός

Η διοίκηση της ΕΤΑΙΡΙΑΣ δεσμεύεται να αναπτύξει και να επιβάλει τη διακυβέρνηση της ασφάλειας πληροφοριών με βάση μια συστηματική προσέγγιση επιχειρηματικού κινδύνου, προκειμένου να καθιερώσει, να εφαρμόσει, να λειτουργήσει, να παρακολουθήσει, να αναθεωρήσει, να διατηρήσει και να βελτιώνει συνεχώς ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) που καλύπτει όλες τις λειτουργίες και δραστηριότητες σε αυτό σύμφωνα με το ISO 27001:2022.

## Σκοπός

Αυτή η Πολιτική Ασφάλειας Πληροφοριών παρέχει κατεύθυνση διαχείρισης και υποστήριξη για την ασφάλεια των πληροφοριών σύμφωνα με τις επιχειρηματικές απαιτήσεις και τους σχετικούς νόμους και κανονισμούς. Όλα τα εμπλεκόμενα πρόσωπα ανεξάρτητα από την ιδιότητά τους (π.χ. εργαζόμενοι της ΕΤΑΙΡΙΑΣ, εργολάβοι, σύμβουλοι, πωλητές, πάροχοι υπηρεσιών κ.λπ.) ή θέση εργασίας απαιτείται να συμμορφώνονται με τις διατάξεις της Πολιτικής Ασφάλειας Πληροφοριών που αναφέρονται στο παρόν έγγραφο και μελλοντικά έγγραφα σχετικά με την ασφάλεια των πληροφοριών.

## Εμβέλεια

Η παρούσα πολιτική ισχύει για όλες τις δραστηριότητες της ΕΤΑΙΡΙΑΣ.

Αυτή η πολιτική ισχύει για όλα τα πληροφοριακά στοιχεία της ΕΤΑΙΡΙΑΣ. Ωστόσο, οι απειλές, οι κίνδυνοι και οι ανάγκες ασφάλειας θα διαφέρουν ανάλογα με τους τύπους πληροφοριών και τα συστήματα. Κατά συνέπεια, οι πρακτικές ασφαλείας πρέπει να προσαρμόζονται σε κάθε μεμονωμένη περίπτωση.

Η πληροφοριακή και υποστηρικτική τεχνική υποδομή της ΕΤΑΙΡΙΑΣ αποτελεί βασικό περιουσιακό στοιχείο της επιχείρησης. Επομένως, είναι απαραίτητο να προστατευθούν αυτά τα περιουσιακά στοιχεία από απειλές που μπορεί να προκύψουν από διάφορες πηγές (απάτη μέσω υπολογιστή, ιοί, χάκερ, τρίτα μέρη κ.λπ.).

Η Πολιτική Ασφάλειας Πληροφοριών εφαρμόζεται σε τρεις διακριτούς τομείς πληροφοριών:

- Το φυσικό υλικό που αναφέρεται σε έντυπη ή υλική πληροφορία, αποθηκευμένη κάπου (π.χ. ντουλάπι ή χρηματοκιβώτιο),
- Το λογισμικό, το οποίο αναφέρεται σε πληροφορίες που αποθηκεύονται σε υπολογιστές αλλά έχουν πρόσβαση είτε τοπικά (πρόσβαση κονσόλας) είτε μέσω δικτύων,
- Τα ζητήματα που σχετίζονται με το απόρρητο των δεδομένων. Το απόρρητο των δεδομένων αφορά την επεξεργασία προσωπικών δεδομένων αποκλειστικά για τον σκοπό για τον οποίο συλλέχθηκαν και για να διασφαλιστεί ότι τα άτομα είναι απαλλαγμένα από την αποκάλυψη απορρήτου που προκαλείται από μη εξουσιοδοτημένη πρόσβαση ή έκθεση των προσωπικών τους πληροφοριών.

## Επιβολή

Κάθε εργαζόμενος που διαπιστώνεται ότι έχει παραβιάσει την παρούσα πολιτική μπορεί να υπόκειται σε πειθαρχικές κυρώσεις από την ΕΤΑΙΡΙΑ, μέχρι και τον τερματισμό της απασχόλησής του.

## 2. Ταξινόμηση περιουσιακών στοιχείων και Έλεγχος

### Assets Classification and Control

Τα πληροφοριακά στοιχεία είναι πολύτιμα, όπως και το λογισμικό και το υλικό που χρησιμοποιούνται για την επεξεργασία και αποθήκευση πληροφοριών. Για την προστασία των πληροφοριών, είναι απαραίτητο να προσδιοριστεί καθένα από αυτά τα περιουσιακά στοιχεία και να καθοριστεί το επίπεδο και το είδος της προστασίας που απαιτούν.

#### Λογοδοσία για περιουσιακά στοιχεία

Τα πληροφοριακά περιουσιακά στοιχεία προσδιορίζονται, λογιστικοποιούνται και αποδίδονται στους καθορισμένους ιδιοκτήτες. Ανάλογα με τον τύπο του στοιχείου πληροφοριών, ο κάτοχος μπορεί να είναι κάτοχος μιας εφαρμογής, ενός συστήματος ή απλά δεδομένων. Εάν ένας ιδιοκτήτης δεν έχει οριστεί επίσημα (π.χ. σε μητρώο περιουσιακών στοιχείων εταιρείας) για ένα πληροφοριακό περιουσιακό στοιχείο, τότε το πρόσωπο που έχει τη διαχειριστική ευθύνη επί αυτού του περιουσιακού στοιχείου θεωρείται ιδιοκτήτης.

Οι ιδιοκτήτες πληροφοριών/συστημάτων έχουν την ευθύνη για την εφαρμογή και τη διατήρηση των κατάλληλων μέτρων ασφαλείας που απαιτούνται για την προστασία των αντίστοιχων περιουσιακών στοιχείων.

Παραδείγματα στοιχείων περιλαμβάνουν τα εξής:

- Πληροφοριακά στοιχεία, συμπεριλαμβανομένων των πληροφοριών των εργαζομένων, χρηματοοικονομικών ή επιχειρησιακών πληροφοριών που σχετίζονται με τρίτους,
- Λογικά περιουσιακά στοιχεία , συμπεριλαμβανομένου λογισμικού συστήματος και εφαρμογών, εργαλείων ανάπτυξης και βοηθητικών προγραμμάτων,
- Υλικά περιουσιακά στοιχεία, συμπεριλαμβανομένου εξοπλισμού πληροφορικής (που βρίσκεται σε γραφεία και πλοία), κλειδιών/καρτών εισόδου, κινητών τηλεφώνων, μέσων κάθε είδους κ.λπ..

#### Ταξινόμηση πληροφοριών

Τα περιουσιακά στοιχεία πρέπει να ταξινομούνται σύμφωνα με τις πιο πολύτιμες ή/και ευαίσθητες λεπτομέρειες που περιέχουν και σύμφωνα με τις αρχές της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Τα επίπεδα ταξινόμησης που χρησιμοποιούνται για την επισήμανση των στοιχείων ενεργητικού είναι τα ακόλουθα:

Περιγραφή	Παραδείγματα
<b>Public</b>	Δημόσια εκτεθειμένες πληροφορίες, π.χ. πληροφορίες που περιλαμβάνονται στην ιστοσελίδα της ΕΤΑΙΡΙΑΣ ελεύθερα διαθέσιμες (χωρίς εγγραφή ή συνδρομή).
<b>Internal Use</b>	Εσωτερικές πληροφορίες της εταιρείας, π.χ. εσωτερικές επικοινωνίες αλληλογραφίας.

<b>Restricted Use</b>	Πληροφορίες στρατηγικής σημασίας όπως οικονομικές συμφωνίες με τρίτους, σχεδιασμός νέων υπηρεσιών κ.λπ.
<b>Confidential</b>	Πληροφορίες που δεν πρέπει να αποκαλυφθούν, π.χ. προσωπικά δεδομένα τρίτων και εργαζομένων και ευαίσθητα προσωπικά δεδομένα, πληροφορίες πελατών, εκθέσεις εσωτερικού ελέγχου, αναφορές περιστατικών κ.λπ.

Σε περίπτωση αμφιβολίας, οι κάτοχοι πληροφοριών πρέπει να χρησιμοποιούν τον μεγαλύτερο βαθμό διαβάθμισης.

#### Αποδεκτή χρήση

Οι πόροι πληροφορικής μπορούν να χρησιμοποιηθούν μόνο για επιχειρηματικές ανάγκες με σκοπό την εκτέλεση εργασιών που σχετίζονται με τον οργανισμό.

Απαγορεύεται η χρήση πόρων πληροφορικής κατά τρόπο που καταλαμβάνει άσκοπα χωρητικότητα, αποδυναμώνει τις επιδόσεις του συστήματος πληροφοριών ή συνιστά απειλή για την ασφάλεια. Απαγορεύεται επίσης:

- να κατεβάσετε αρχεία εικόνας ή βίντεο που δεν έχουν επιχειρηματικό σκοπό, να στείλετε αλυσιδωτές επιστολές ηλεκτρονικού ταχυδρομείου (e-mail chain letters), να παίξετε παιχνίδια κ.λπ..
- εγκαταστήσετε λογισμικό χωρίς άδεια χρήσης ή άλλο πιθανώς κακόβουλο λογισμικό σε έναν τοπικό υπολογιστή.
- να κάνετε λήψη κώδικα προγράμματος από εξωτερικά μέσα.
- να κάνετε εγκατάσταση ή χρήση περιφερειακών συσκευών, όπως μόντεμ, κάρτες μνήμης ή άλλες συσκευές για την αποθήκευση και την ανάγνωση δεδομένων (π.χ. μονάδες flash USB), οι οποίες δεν χρησιμοποιούνται για επιχειρηματικές ανάγκες και μπορεί να μολυνθούν από κακόβουλο λογισμικό.

Οποιαδήποτε παραβίαση αυτής της πολιτικής μπορεί να οδηγήσει σε πειθαρχικά μέτρα και ακόμη και τερματισμό της απασχόλησης. Παράνομες δραστηριότητες μπορούν επίσης να αναφέρονται στις αρμόδιες αρχές.

## 3. Εταιρικές Πολιτικές Ασφάλειας Δεδομένων Προσωπικού & Επισκεπτών

### Corporate Data Security Policies for Personnel & Visitors

Οι πληροφορίες είναι ευάλωτες στον κίνδυνο ανθρώπινου λάθους, κλοπής, απάτης και κακής χρήσης. Οι πτυχές ασφάλειας κάθε θέσης εργασίας θα προσδιοριστούν κατά την ανάλυση της θέσης εργασίας και θα αντιμετωπιστούν κατά τη διαδικασία πρόσληψης. Η πρόσβαση σε πληροφορίες ή/και συστήματα πληροφοριών χορηγείται ή αφαιρείται με βάση την αρχή «ανάγκη να γνωρίζει – need to know». Το προσωπικό θα ενημερωθεί για τις απαιτήσεις ασφαλείας της εταιρείας, θα λάβει επαρκή εκπαίδευση για να τις ανταποκριθεί και θα του παρασχεθούν κανάλια για την επίσημη αναφορά ζητημάτων ασφαλείας, περιστατικών και απειλών.

Ασφάλεια στον ορισμό των θέσεων εργασίας και την στελέχωση

Ζητήματα ασφάλειας αντιμετωπίζονται όταν το προσωπικό αναλαμβάνει ή αποχωρεί από θέσεις εργασίας και περιλαμβάνεται σε περιγραφές καθηκόντων και συμβάσεις.

- Οι αιτήσεις για απασχόληση σε θέσεις εργασίας που περιλαμβάνουν πρόσβαση σε απόρρητες ή εμπιστευτικές πληροφορίες ή σε συστήματα που χειρίζονται τέτοιες πληροφορίες ελέγχονται προκειμένου να προσδιοριστεί πόσο αξιόπιστος είναι ο αιτών.
- Οι περιγραφές θέσεων εργασίας πρέπει να αναφέρουν ρόλους και ευθύνες ασφαλείας.
- Κατά την πρόσληψη ο νέος υπάλληλος υπογράφει συμφωνία εμπιστευτικότητας.
- Η πρόσβαση στα πληροφοριακά συστήματα καταργείται όταν οι εργαζόμενοι αποχωρούν από την εταιρεία και τα δικαιώματα πρόσβασης επανεξετάζονται κάθε φορά που αλλάζουν θέση εργασίας εντός της εταιρείας.

Πρόσβαση για τους επισκέπτες

Ελέγχεται η πρόσβαση των εξωτερικών επισκεπτών στα πληροφοριακά συστήματα. Οι έλεγχοι που εμφανίζονται παρακάτω θεωρούνται ελάχιστες απαιτήσεις:

- Οι επισκέπτες δεν πρέπει να έχουν μη εξουσιοδοτημένη πρόσβαση σε χώρους εργασίας, πληροφορίες ή πληροφοριακά συστήματα. Η διοίκηση της ΕΤΑΙΡΙΑΣ εγκρίνει την είσοδο των επισκεπτών στις εγκαταστάσεις της εταιρείας και την πρόσβαση στα σχετικά συστήματα.
- Θα πρέπει να εξετάζονται συμφωνίες εμπιστευτικότητας για τους επισκέπτες που απαιτείται να έχουν πρόσβαση σε εμπιστευτικές ή κρίσιμες πληροφορίες ή συστήματα που χειρίζονται τέτοιες πληροφορίες. Οι συμφωνίες αυτές θα πρέπει να αποτελούν μέρος σύμβασης που θα υπογραφεί μεταξύ της ΕΤΑΙΡΙΑΣ και του συνδεδεμένου τρίτου.

Εκπαίδευση

Όλο το προσωπικό πρέπει να ενημερώνεται για τις απαιτήσεις ασφαλείας της ΕΤΑΙΡΙΑΣ και να εκπαιδεύεται στην ορθή και ασφαλή χρήση των πληροφοριών και των συναφών συστημάτων και εγκαταστάσεων.

- Όλο το προσωπικό θα ενημερωθεί για την Πολιτική Ασφάλειας Πληροφοριών της ΕΤΑΙΡΙΑΣ, μέσω εταιρικών παρουσιάσεων που θα πραγματοποιούνται περιοδικά (τουλάχιστον ετησίως) με σκοπό την εξοικείωση με τις έννοιες και τις πρακτικές της ασφαλείας πληροφοριών.
- Τα διευθυντικά στελέχη διασφαλίζουν ότι όλο το προσωπικό έχει επίγνωση των ευθυνών του όσον αφορά την πολιτική ασφαλείας πληροφοριών της εταιρείας και ότι το προσωπικό που δεν παρακολουθεί τις εκπαιδευτικές παρουσιάσεις εισάγεται στις απαιτήσεις της πολιτικής που ισχύει για αυτούς.
- Πρέπει να παρέχεται κατάρτιση στην ορθή χρήση των μέσων πληροφορικής πριν χορηγηθεί πρόσβαση χωρίς επίβλεψη στα συστήματα και εφαρμογές πληροφορικής της εταιρείας.

Ανταπόκριση σε περιστατικά

Καθιερώνονται δίαυλοι αναφοράς και διαχείρισης απειλών, συμβάντων ή δυσλειτουργιών για την ασφάλεια.

Σε περίπτωση συμβάντος, συγκροτείται ομάδα για τη λήψη των κατάλληλων μέτρων για την αποκατάσταση των συστημάτων ΤΠ, ώστε να καταστεί δυνατή η αποκατάσταση της κανονικής επιχειρηματικής λειτουργίας. Η ομάδα εκτελεί τουλάχιστον τα ακόλουθα βήματα:

1. Αρχική αξιολόγηση. Για να εξασφαλιστεί η κατάλληλη αντίδραση, η ομάδα αντιμετώπισης ανακαλύπτει:
  - πώς συνέβη το περιστατικό,
  - ποια συστήματα επηρεάστηκαν και πώς,
  - ο βαθμός στον οποίο επηρεάζονται τα εμπορικά ή/και λειτουργικά δεδομένα,
  - σε ποιο βαθμό εξακολουθεί να υφίσταται οποιαδήποτε απειλή.
2. Ανάκτηση συστημάτων και δεδομένων. Μετά από μια αρχική αξιολόγηση του συμβάντος που αφορά την ασφάλεια των πληροφοριών, τα συστήματα και τα δεδομένα πρέπει να καθαρίζονται, να ανακτώνται και να αποκαθίστανται, στο μέτρο του δυνατού, σε λειτουργική κατάσταση με την αφαίρεση των απειλών από το σύστημα και την αποκατάσταση του λογισμικού.
3. Διερεύνηση του περιστατικού. Για την κατανόηση των αιτίων και των συνεπειών ενός συμβάντος που θέτει σε κίνδυνο την ασφάλεια των πληροφοριών, διεξάγεται έρευνα από την ομάδα ΤΠ, όπως απαιτείται. Οι πληροφορίες από μια έρευνα θα διαδραματίσουν σημαντικό ρόλο στην πρόληψη πιθανής επανεμφάνισης.
4. Αποτρέψτε την επανεμφάνιση. Λαμβάνοντας υπόψη το αποτέλεσμα της έρευνας που αναφέρεται ανωτέρω, εξετάζονται ενέργειες για την αντιμετώπιση τυχόν ανεπαρκειών στα τεχνικά και/ή οργανωτικά μέτρα προστασίας, σύμφωνα με τις διαδικασίες της εταιρείας για την εφαρμογή διορθωτικών ενεργειών.

Όταν ένα συμβάν που αφορά την ασφάλεια των πληροφοριών είναι περίπλοκο, για παράδειγμα εάν τα συστήματα δεν μπορούν να επανέλθουν σε κανονική λειτουργία, μπορεί να χρειαστεί να δρομολογηθεί σχέδιο αποκατάστασης, το οποίο λαμβάνει υπόψη τα ακόλουθα:

1. Εάν τα συστήματα πρέπει να τερματιστούν ή να συνεχίσουν να λειτουργούν για την προστασία των δεδομένων.
2. Η κατάλληλη χρήση τυχόν προηγμένων εργαλείων που παρέχονται σε προεγκατεστημένο λογισμικό ασφαλείας.
3. Ο βαθμός στον οποίο το συμβάν έχει θέσει σε κίνδυνο συστήματα πέραν των δυνατοτήτων των υφιστάμενων σχεδίων αποκατάστασης.

## 4. Διαχείριση 3ου Μέρους

### Third Party Management

Η ΕΤΑΙΡΙΑ αξιολογεί και ενσωματώνει τις διαδικασίες διαχείρισης της φυσικής ασφαλείας και της ασφαλείας πληροφοριών των παρόχων υπηρεσιών και τρίτων μερών σε σχετικές συμφωνίες και συμβάσεις. Οι διαδικασίες που αξιολογούνται κατά τον έλεγχο των προμηθευτών και περιλαμβάνονται στις απαιτήσεις της σύμβασης πρέπει να περιλαμβάνουν:

- διαχείριση της ασφαλείας, συμπεριλαμβανομένης της διαχείρισης των υπερβολάβων,
- κατασκευαστική/επιχειρησιακή ασφάλεια,
- τεχνολογία λογισμικού και αρχιτεκτονική,
- διαχείριση συμβάντων ασφαλείας,
- ασφάλεια προσωπικού,
- προστασία δεδομένων και πληροφοριών.

Η αξιολόγηση τρίτων πρέπει να γίνεται σε περιοδική βάση, ιδίως για όσους έχουν πρόσβαση, επεξεργάζονται ή διαχειρίζονται εμπιστευτικές πληροφορίες της ΕΤΑΙΡΙΑΣ.

Η έλλειψη φυσικής ή/και πληροφοριακής ασφάλειας στα προϊόντα ή την υποδομή τρίτων μπορεί να οδηγήσει σε παραβίαση της ασφάλειας των πληροφοριών.

Η ΕΤΑΙΡΙΑ διαθέτει διαδικασία διαχείρισης και αξιολόγησης κινδύνων τόσο για τις νέες όσο και για τις υφιστάμενες συμβάσεις. Καθορίζεται ένα ελάχιστο σύνολο απαιτήσεων για τη διαχείριση των κινδύνων της αλυσίδας εφοδιασμού ή τρίτων. Ένα σύνολο απαιτήσεων ασφάλειας πληροφοριών που αντικατοπτρίζουν τις προσδοκίες της ΕΤΑΙΡΙΑΣ πρέπει να είναι σαφές και ξεκάθαρο στους προμηθευτές. Αυτό μπορεί επίσης να βοηθήσει τις πρακτικές προμηθειών στις συναλλαγές με πολλούς προμηθευτές.

## 5. Ασφάλεια περιβάλλοντος χώρου

### Physical and Environmental Security

Οι πληροφορίες φυσικές και άλλα υλικά περιουσιακά στοιχεία που χρησιμοποιούνται για την αποθήκευση, επεξεργασία ή μετάδοση πληροφοριών, π.χ. υλισμικό, μαγνητικά μέσα, καλωδίωση κ.λπ., είναι ευάλωτα σε φυσικές βλάβες και παρεμβολές, συμπεριλαμβανομένων ζημιών από περιβαλλοντικούς παράγοντες όπως η φωτιά και το νερό. Αν και είναι αδύνατο να εξαλειφθούν πλήρως αυτοί οι κίνδυνοι, πρέπει να εντοπιστούν και να μειωθούν σε αποδεκτά επίπεδα με την τοποθέτηση περιουσιακών στοιχείων σε κατάλληλα περιβάλλοντα και τη φυσική προστασία τους από απειλές για την ασφάλεια και περιβαλλοντικούς κινδύνους.

#### Ασφαλείς Περιοχές

Οι εγκαταστάσεις τεχνολογίας πληροφοριών που υποστηρίζουν κρίσιμες ή ευαίσθητες επιχειρηματικές δραστηριότητες στεγάζονται σε ασφαλείς χώρους.

- σε ασφαλείς περιοχές που περιέχουν πληροφοριακά περιουσιακά στοιχεία των οποίων η ταξινόμηση απαιτεί υψηλό επίπεδο ασφάλειας (π.χ. Data Centers) πρέπει να εφαρμόζονται μέτρα περιμετρικής φυσικής ασφάλειας.
- οι ασφαλείς περιοχές πρέπει να προστατεύονται με κατάλληλους ελέγχους διαχείρισης / περιορισμού / ελέγχου της πρόσβασης.
- τα δικαιώματα πρόσβασης σε ασφαλείς περιοχές πρέπει να ελέγχονται αυστηρά.
- οι ασφαλείς περιοχές δεν πρέπει να περιλαμβάνουν εξοπλισμό γενικής χρήσης.

#### Ασφάλεια εξοπλισμού

Ο εξοπλισμός που υποστηρίζει κρίσιμες ή ευαίσθητες επιχειρηματικές διαδικασίες (συμπεριλαμβανομένου του εφεδρικού εξοπλισμού και μέσα αποθήκευσης) προστατεύεται φυσικά από απειλές για την ασφάλεια και περιβαλλοντικούς κινδύνους, ανάλογα με την περίπτωση.

- Ο εξοπλισμός έχει τοποθετηθεί σε επιλεγμένο σημείο ώστε να μειώνονται οι κίνδυνοι βλάβης από πυρκαγιά ή νερό, από παρεμβολές και η πρόσβαση ελέγχεται με κλειδαριά ώστε να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση.

- Ο εξοπλισμός που υποστηρίζει κρίσιμες επιχειρηματικές διαδικασίες προστατεύεται από διακοπές ρεύματος ή άλλες ηλεκτρικές ανωμαλίες.
- Τα περιβάλλοντα υπολογιστών και εξοπλισμού παρακολουθούνται, όπου απαιτείται, ώστε να εξασφαλίζεται ότι δεν σημειώνεται υπέρβαση περιβαλλοντικών περιορισμών, όπως η θερμοκρασία και η υγρασία.
- Οι τηλεπικοινωνίες και τα καλώδια τροφοδοσίας προστατεύονται από υποκλοπή ή διακοπή.
- Ο εξοπλισμός συντηρείται σύμφωνα με τις συστάσεις του κατασκευαστή.
- Οι διαδικασίες και οι έλεγχοι ασφαλείας διασφαλίζουν την ασφάλεια του εξοπλισμού όταν χρησιμοποιείται εκτός των εγκαταστάσεων της εταιρείας.
- Τα δεδομένα απαλείφονται από τον εξοπλισμό, συμπεριλαμβανομένων των μέσων αποθήκευσης, πριν από την απόρριψή τους.

## 6. Λειτουργία και Διαχείριση Η/Υ και Δικτύου

### Computer and Network Operation and Management

Οι περισσότερες πληροφορίες που ανήκουν ή χρησιμοποιούνται από την ΕΤΑΙΡΙΑ υποβάλλονται σε επεξεργασία και αποθηκεύονται σε υπολογιστές. Προκειμένου να προστατευθούν αυτές οι πληροφορίες, οι υπολογιστές αυτοί πρέπει να διαχειρίζονται και να λειτουργούν με ασφαλή και ελεγχόμενο τρόπο και να διαθέτουν επαρκείς πόρους.

Όπως και με τα συστήματα πληροφορικής, η διαχείριση των δικτύων πρέπει να γίνεται με ελεγχόμενο και ασφαλή τρόπο. Πρέπει να προστατεύεται η πρόσβαση στα συστήματα πληροφορικής του δικτύου, καθώς και η ακεραιότητα και η διαθεσιμότητα του λογισμικού, των δεδομένων και των υπηρεσιών δικτύου. Οι πληροφορίες που διαβιβάζονται μέσω δικτύων, ιδίως όταν ανταλλάσσονται μεταξύ οργανισμών, πρέπει να τηρούνται εμπιστευτικές.

#### Επιχειρησιακές διαδικασίες και Αρμοδιότητες

Καθορίζονται αρμοδιότητες και διαδικασίες για τη διαχείριση και τη λειτουργία όλων των υπολογιστών, συστημάτων και δικτύων. Προετοιμάζονται και να διατηρούνται (up to date) σαφείς και περιεκτικές διαδικασίες λειτουργίας για όλες τις πτυχές των συστημάτων πληροφορικής και των δικτύων, ώστε να βοηθηθεί η ορθή και ασφαλή λειτουργία και να καθοριστούν επακριβώς οι αντίστοιχοι ρόλοι και ευθύνες. Οι διαδικασίες αυτές περιλαμβάνουν:

- Προγραμματισμένες δραστηριότητες παροχής υπηρεσιών για λειτουργίες που παρέχονται σε επιχειρήσεις ή τρίτους.
- Χειρισμός αρχείων και δεδομένων με επαλήθευση των δεδομένων που μεταδίδονται μέσω δικτύων.
- Διαδικασίες διαχείρισης αλλαγών για όλες τις προγραμματισμένες εργασίες ανάπτυξης, συντήρησης και δοκιμών του συστήματος.
- Χειρισμός σφαλμάτων και επεξεργασία κατ'έξαιρεση που εξυπηρετεί απροσδόκητα συμβάντα.
- Διαδικασίες διαχείρισης προβλημάτων, συμπεριλαμβανομένης της καταγραφής όλων των προβλημάτων δικτύου και της επίλυσής τους (όπου να προσδιορίζεται το πώς και το ποιος).
- Διαδικασίες διαχείρισης συμβάντων.
- Διαδικασίες δοκιμής/αξιολόγησης για όλο το νέο ή τροποποιημένο υλισμικό ή λογισμικό, συμπεριλαμβανομένων των επιδόσεων, της διαθεσιμότητας, της αξιοπιστίας, της δυνατότητας ελέγχου, της ανθεκτικότητας και της ικανότητας χειρισμού σφαλμάτων.

- Δραστηριότητες τακτοποίησης και διευθέτησης θεμάτων όπως διαδικασίες εκκίνησης και τερματισμού λειτουργίας, δημιουργία αντιγράφων ασφαλείας δεδομένων, συντήρηση εξοπλισμού, διαχείριση υπολογιστών και δικτύων, μέτρα ή απαιτήσεις ασφαλείας.
- Συμβάσεις υποστήριξης σε περίπτωση απρόβλεπτων λειτουργικών ή τεχνικών δυσκολιών.
- Για να ελαχιστοποιηθεί ο κίνδυνος αμελούς ή εκούσιας κατάχρησης υπολογιστών, συστημάτων ή δικτύων από το σύστημα, τα καθήκοντα διαχωρίζονται, όπου είναι δυνατόν.
- Τα συστήματα development και testing διαχωρίζονται / απομονώνονται από τα live συστήματα όπου αυτό είναι εφικτό.
- Οι προβλέψεις για τη χρήση τρίτων για τη διαχείριση πληροφοριών πρέπει να προσδιορίζουν τυχόν επιπτώσεις στην ασφάλεια και σχετικούς ελέγχους ασφαλείας.
- Οι διαχειριστές (administrators) υπολογιστών και δικτύων τηρούν αρχείο καταγραφής όλων των εκτελούμενων εργασιών.
- Συχνά, μόνιμα ή ασυνήθιστα σφάλματα δικτύου πρέπει να αναφέρονται και να διερευνώνται.
- Τα αρχεία όλων των αδειών λογισμικού και των μηχανημάτων στα οποία εφαρμόζονται τηρούνται και ενημερώνονται.

#### Προστασία λογισμικού και υπολογιστών

Πρέπει να λαμβάνονται μέτρα για την πρόληψη και τον εντοπισμό μη εξουσιοδοτημένων αλλαγών στο λογισμικό ή/και τις πληροφορίες.

- Εφαρμόζονται μέτρα ανίχνευσης και πρόληψης ιών και κατάλληλες διαδικασίες ευαισθητοποίησης των χρηστών.
- Οι διαδικασίες ελέγχου αλλαγών χρησιμοποιούνται για τη ρύθμιση των αλλαγών στο λογισμικό παραγωγής και στα δεδομένα.

#### Χειρισμός και προστασία πόρων πληροφορικής

Οι πόροι πληροφορικής ελέγχονται και, εφόσον απαιτείται, προστατεύονται φυσικά.

- Τα αφαιρούμενα μέσα υπολογιστών ελέγχονται.
- Θεσπίζονται και ακολουθούνται διαδικασίες χειρισμού μέσω πληροφορικής που περιέχουν εμπιστευτικά ή κρίσιμα δεδομένα.
- Τα μέσα πληροφορικής πρέπει να απορρίπτονται καταλλήλως όταν δεν χρειάζονται πλέον.

#### Προστασία υπηρεσιών δικτύου

Οι συνδέσεις με τις υπηρεσίες δικτύου ελέγχονται.

- Ο έλεγχος πρόσβασης δικτύου πρέπει να περιλαμβάνει έλεγχο ταυτότητας και αυθεντικοποίηση χρήστη.
- Η εξουσιοδότηση των χρηστών να συνδέονται σε ένα δίκτυο ελέγχεται σύμφωνα με τις απαιτήσεις της πολιτικής πρόσβασης.
- Η χρήση εξοπλισμού παρακολούθησης δικτύου πρέπει να είναι περιορισμένη και να επιτρέπεται σε συγκεκριμένους χρήστες με επίσημη εξουσιοδότηση. Επιπλέον, πρέπει να χρησιμοποιούνται εργαλεία λογισμικού για την ενεργοποίηση συναγερμών, ειδοποιώντας την ομάδα πληροφορικής της ΕΤΑΙΡΙΑΣ για οποιαδήποτε ύποπτη δραστηριότητα.
- Οι κίνδυνοι που συνδέονται με τη χρήση υπηρεσιών εξωτερικού δικτύου θα πρέπει να αξιολογούνται και να αντιμετωπίζονται.

- Οι συνδέσεις απομακρυσμένων χρηστών μέσω δημόσιων δικτύων ή απομακρυσμένων δικτύων ή υπολογιστών πρέπει να επιτρέπεται μετά από αυθεντικοποίηση των χρηστών και πρέπει να εφαρμόζονται μέθοδοι κρυπτογράφησης δεδομένων (π.χ. VPN) για την ασφαλή ανταλλαγή πληροφοριών.
- Όλες οι συνδέσεις από εξωτερικά δίκτυα σε εσωτερικά εταιρικά δίκτυα (π.χ. LAN ή LAN VPN) πρέπει να προστατεύονται.
- Η αρχιτεκτονική Flat network (δηλαδή δίκτυα χωρίς ιεράρχηση ή διαχωρισμό σε layers) πρέπει να αποφεύγεται. Αυτό μπορεί να επιτευχθεί, για παράδειγμα, διαιρώντας το δίκτυο σε ξεχωριστά λογικά network domain με βάση κοινούς βαθμούς εμπιστοσύνης (π.χ. Production, test, pre-production, κλπ.). Επιτρέπεται μόνο εξουσιοδοτημένη κυκλοφορία / ανταλλαγή δεδομένων / πρόσβαση μεταξύ των network domains.
- Χρησιμοποιούνται κατάλληλα μέτρα για την εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών (π.χ. Χρήση virtual private networks, κρυπτογράφηση).
- Σε περίπτωση απώλειας σύνδεσης ή απροσδόκητου σφάλματος στο δίκτυο, οι διαχειριστές πρέπει να είναι σε θέση να διαχειρίζονται τα στοιχεία δικτύου μέσω συστημάτων διαχείρισης δικτύου.
- Τηρούνται αρχεία / ίχνη των δραστηριοτήτων του δικτύου (audit trails, logs) ώστε να εξασφαλίζεται ότι μπορεί να συγκεντρωθεί επαρκής ποσότητα πληροφοριών που θα βοηθήσει στις έρευνες για τον εντοπισμό τυχόν καταχρήσεων του δικτύου.
- Μόνο εγκεκριμένος εξοπλισμός συνδέεται με το εταιρικό δίκτυο.
- Μόνο δοκιμασμένο και εγκεκριμένο λογισμικό εγκαθίσταται στο δίκτυο.
- Ο σχεδιασμός και η διαμόρφωση του δικτύου πρέπει να τεκμηριώνονται και να συντηρούνται.
- Η ομάδα IT έχει την ευθύνη να βεβαιώνεται πως οι υπολογιστές (e.g. workstations) που συνδέονται στο δίκτυο της ΕΤΑΙΡΙΑΣ έχουν περασμένα όλα τα λογισμικά ασφαλείας (eg. antivirus). Επιπροσθέτως, η ομάδα IT βεβαιώνεται πως τα διάφορα λογισμικά που είναι εγκατεστημένα στους υπολογιστές είναι εγκεκριμένα από την ΕΤΑΙΡΙΑ και έχουν αποκτηθεί (και ανανεωθεί) οι κατάλληλες άδειες.

#### Ανταλλαγή δεδομένων

Η ανταλλαγή δεδομένων και λογισμικών εντός του γραφείου ή μεταξύ εξωτερικών συνεργατών offices, πρέπει να ελέγχεται.

- Οι συμφωνίες ανταλλαγής δεδομένων και λογισμικού προσδιορίζουν τους ελέγχους ασφαλείας που θα χρησιμοποιούνται.
- Έχουν υιοθετηθεί τα συνιστώμενα πρωτόκολλα ασφαλείας για τη μεταφορά δεδομένων.
- Τα μέσα υπολογιστών προστατεύονται από απώλεια ή κατάχρηση κατά τη μεταφορά τους.
- Εξετάζονται τακτικά έλεγχοι για τη μείωση των επιχειρηματικών και ασφαλείας κινδύνων που συνδέονται με το ηλεκτρονικό ταχυδρομείο σε αποδεκτά επίπεδα.
- Συντάσσονται και να εφαρμόζονται σαφείς πολιτικές και κατευθυντήριες γραμμές για τον έλεγχο των επιχειρηματικών και ασφαλείας κινδύνων που συνδέονται με τα ηλεκτρονικά συστήματα γραφείου.

## 7. Πολιτική Κρυπτογράφησης

### Cryptography Policy

Η χρήση κρυπτογραφικών αλγορίθμων είναι απαραίτητη προκειμένου ο οργανισμός να διασφαλίσει την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών που δημιουργούνται και διατηρούνται στο πληροφοριακό σύστημα. Η κρυπτογραφία μπορεί να προσθέσει ένα επιπλέον επίπεδο ασφάλειας κατά την αποθήκευση και τη μετάδοση ευαίσθητων πληροφοριών.

#### Χρήση κρυπτογραφίας

Η χρήση ιδιόκτητων αλγορίθμων κρυπτογράφησης δεν επιτρέπεται για κανένα σκοπό, εκτός εάν αναθεωρηθεί και εγκριθεί.

- Κατά τη διαβίβαση εμπιστευτικών δεδομένων, αυτά κρυπτογραφούνται.
- Τα εμπιστευτικά δεδομένα κρυπτογραφούνται όταν αποθηκεύονται σε θέσεις εργασίας του προσωπικού της ΕΤΑΙΡΙΑΣ.
- Το σχήμα κρυπτογραφίας που χρησιμοποιεί η ΕΤΑΙΡΙΑ πρέπει να είναι ευέλικτο και κεντρικά ελεγχόμενο, ώστε να είναι εύκολη η αλλαγή του κρυπτογραφικού αλγορίθμου που χρησιμοποιείται, σε περιπτώσεις παραβίασης ενός αλγορίθμου.
- Όλα τα συστήματα που χρησιμοποιούν κρυπτογραφία πρέπει να υποστηρίζουν την ανάκτηση δεδομένων σε περίπτωση που το κλειδί που χρησιμοποιείται για την κρυπτογράφηση τους δεν είναι διαθέσιμο.

#### Κρυπτογραφικά πρότυπα και αλγόριθμοι

Τα συστήματα κρυπτογράφησης που χρησιμοποιούνται πρέπει να βασίζονται σε κοινώς αποδεκτούς αλγορίθμους, όπως απαιτείται από νομικές και συμβατικές απαιτήσεις.

#### Ισχύς κρυπτογραφίας και μήκος κρυπτογραφικού κλειδιού

Η ισχύς ενός κρυπτογραφικού συστήματος εξαρτάται από τους αλγόριθμους που χρησιμοποιούνται και τη μοναδικότητα του κλειδιού που χρησιμοποιείται. Τα κλειδιά που χρησιμοποιούνται για κρυπτογράφηση από την ΕΤΑΙΡΙΑ πρέπει να έχουν μήκος τουλάχιστον 128 bit. Προκειμένου να διατηρηθεί η αποτελεσματικότητα και η ασφάλεια των κρυπτογραφικών λειτουργιών, θα πρέπει να εφαρμόζονται οι ακόλουθοι κανόνες:

- Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται για κρυπτογράφηση από την ΕΤΑΙΡΙΑ ταξινομούνται ως εμπιστευτικές πληροφορίες και προστατεύονται.
- Η δημιουργία και διαχείριση όλων των κρυπτογραφικών κλειδιών που χρησιμοποιούνται από τους υπαλλήλους της ΕΤΑΙΡΙΑΣ γίνεται κεντρικά από τον Chief Information Security Officer.

## 8. Έλεγχος Πρόσβασης

### Access Control

Για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, χειραγώγησης ή καταστροφής πληροφοριών, είναι απαραίτητος ο έλεγχος της πρόσβασης σε πληροφοριακά συστήματα και δεδομένα που βρίσκονται στα γραφεία της ΕΤΑΙΡΙΑΣ. Ο έλεγχος της πρόσβασης στα συστήματα πληροφορικής περιλαμβάνει την καθιέρωση και τη χρήση διαδικασιών για την έγκριση της πρόσβασης, την κατανομή δικαιωμάτων και την εκπαίδευση του προσωπικού στην ασφαλή χρήση των συστημάτων. Τα

συστήματα πρέπει να παρακολουθούνται για να εξασφαλίζεται η συμμόρφωσή τους με τις καθιερωμένες διαδικασίες. Ο διαχειριστής του συστήματος (administrator) έχει την ευθύνη να καθορίσει και να εκχωρήσει δικαιώματα πρόσβασης χρήστη. Πρέπει να υπάρχει διαδικασία εγγραφής/διαγραφής χρήστη.

Έλεγχος Πρόσβασης σε εφαρμογές/συστήματα/υπολογιστές

Η πρόσβαση σε εφαρμογές/συστήματα/υπολογιστές και δεδομένα ελέγχεται.

- Καθορίζονται και τεκμηριώνονται απαιτήσεις λειτουργίας για τον έλεγχο πρόσβασης.
- Η πρόσβαση στα πληροφοριακά συστήματα πρέπει να εξουσιοδοτείται από καθορισμένο υπεύθυνο στέλεχος (π.χ. τον επικεφαλής ενός τμήματος, τον ιδιοκτήτη της επιχείρησης).
- Η πρόσβαση στα δεδομένα και στα συστήματα πληροφορικής παρέχεται σύμφωνα με τις καθορισμένες απαιτήσεις λειτουργίας.
- Η πρόσβαση στις υπηρεσίες κοινής ωφέλειας του δικτύου (system utilities) περιορίζεται και ελέγχεται.
- Πρέπει να λαμβάνονται υπόψη περιορισμοί στους χρόνους σύνδεσης για συστήματα υψηλού κινδύνου.
- Οι ομαδικοί ή κοινόχρηστοι λογαριασμοί δεν πρέπει να επιτρέπονται.
- Τα προεπιλεγμένα ονόματα χρήστη (default usernames) που υπάρχουν στα συστήματα μετά τη φάση εγκατάστασης πρέπει να διαγραφούν ή να γίνουν ασφαλή αλλάζοντας τον κωδικό πρόσβασης.
- Πρέπει να εφαρμοστεί μια ασφαλής διαδικασία για την παράδοση των αρχικών διαπιστευτηρίων ελέγχου ταυτότητας λογαριασμού χρήστη (user account authentication credentials) και την επαναφορά ξεχασμένων διαπιστευτηρίων (π.χ. κωδικών πρόσβασης).
- Η κατανομή των δικαιωμάτων των χρηστών πρέπει να βασίζεται στις αρχές ασφαλείας «separation of duties» και «need to know».
- Κάθε πρόσβαση πρέπει να καταγράφεται (logs) και πρέπει να συλλέγεται επαρκής ποσότητα πληροφοριών για να είναι διαθέσιμη για έρευνες.

Πολιτική κωδικού πρόσβασης

Οι ακόλουθοι κανόνες κωδικού πρόσβασης εφαρμόζονται σε κάθε τύπο χρηστών και διαχειριστών (users και administrators για DB, OS και εφαρμογές):

- Μοναδικό ID & password πρέπει να χρησιμοποιείται για την πρόσβαση στα συστήματα.
- Οι κωδικοί πρόσβασης δεν πρέπει να είναι οι ίδιοι με το user ID.
- Οι αρχικοί κωδικοί πρόσβασης πρέπει να είναι έγκυροι μόνο μέχρι την πρώτη προσπάθεια σύνδεσης του user, το σύστημα πρέπει στη συνέχεια να επιβάλει την αλλαγή του αρχικού κωδικού πρόσβασης.
- Οι κωδικοί πρόσβασης πρέπει να έχουν ελάχιστο μήκος 8 χαρακτήρων.
- Οι κωδικοί πρόσβασης παραμένουν σε ισχύ για μέγιστο διάστημα 30 ημερών από την τελευταία αλλαγή τους.
- Οι χρήστες πρέπει να εμποδίζονται να επαναχρησιμοποιούν τους τελευταίους 3 κωδικούς πρόσβασής τους.
- Μετά από 3 αποτυχημένα logins ο λογαριασμός θα κλειδωθεί.
- Ο κωδικός πρόσβασης πρέπει να περιέχει τουλάχιστον 2 από τα ακόλουθα: κεφαλαία και πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες.

- Οι κωδικοί πρόσβασης δεν πρέπει να αποτελούνται από λέξεις από το λεξικό της αγγλικής γλώσσας.
- Οι κωδικοί πρόσβασης πρέπει να κρυπτογραφούνται ή να καλύπτονται κατά την αποθήκευσή τους.

#### Απομακρυσμένη πρόσβαση

- Η απομακρυσμένη πρόσβαση στα συστήματα πρέπει να ελέγχεται αυστηρά.
- Λογισμικό ανίχνευσης ιών εγκαθίσταται μονίμως σε όλους τους φορητούς προσωπικούς υπολογιστές.
- Για απομακρυσμένη πρόσβαση σε εμπιστευτικές πληροφορίες απαιτείται να διασφαλιστεί η αυστηρή ταυτοποίηση των απομακρυσμένων χρηστών και η ισχυρή κρυπτογράφηση των διαβιβαζόμενων δεδομένων.
- Η πρόσβαση στο δίκτυο και τα δεδομένα από προσωπικό υποστήριξης εξωτερικού παρόχου θα περιορίζεται μόνο στα συστήματα που υποστηρίζουν.
- Πρέπει να υπάρχει μια καθορισμένη διαδικασία για την έγκριση αιτημάτων και τη διαχείριση της παροχής απομακρυσμένης πρόσβασης.
- Όλη η απομακρυσμένη πρόσβαση πρέπει να καταγράφεται (logs) και πρέπει να συλλέγεται επαρκής ποσότητα πληροφοριών για να βοηθήσει στις έρευνες και να εντοπίσει κατάχρηση της υπηρεσίας απομακρυσμένης πρόσβασης.

## 9. Καταγραφή και Παρακολούθηση

### Logging and Monitoring

Τα ενεργά στοιχεία της υποδομής πληροφορικής παρέχουν αρχεία καταγραφής (Logs) με πληθώρα δεδομένων σχετικά με τη λειτουργία τους (από την κατάσταση του συστήματος, την πρόσβαση των χρηστών και τον φόρτο εργασίας έως τα σφάλματα και τις αποτυχίες). Η συλλογή αυτών των δεδομένων είναι απαραίτητη και πρέπει να συμμορφώνεται με τις ακόλουθες απαιτήσεις:

1. Τα αρχεία καταγραφής (Logs) πρέπει να είναι σε μορφή που μπορεί να χρησιμοποιηθεί απευθείας από το προσωπικό ασφαλείας χωρίς πρόσθετο λογισμικό. Τα Logs πρέπει επίσης να συμμορφώνεται με νομικές, κανονιστικές και συμβατικές υποχρεώσεις, συμπεριλαμβανομένης της εργατικής νομοθεσίας και της νομοθεσίας περί προστασίας δεδομένων προσωπικού χαρακτήρα που διέπουν την λειτουργία της εταιρείας.
2. Τα ρολόγια του συστήματος πρέπει να συγχρονίζονται για να είναι σε θέση να συσχετίσουν τα ίχνη ελέγχου (audit trails και logs) πολλών συστημάτων.
3. Τα ενεργά στοιχεία της υποδομής πληροφορικής που παρέχουν τη δυνατότητα πρέπει να παρακολουθούνται για: χρόνο λειτουργίας (uptime), διαθεσιμότητα (availability), κατάσταση (status) και εύρυθμη λειτουργία. Οι δραστηριότητες παρακολούθησης θα αξιοποιούν αυτοματοποιημένα εργαλεία, όπου είναι δυνατόν, για τον εντοπισμό ανωμαλιών εντός του περιβάλλοντος ΤΠΕ (ICT), συμπεριλαμβανομένων του υπολογιστικού νέφους (cloud). Η ενοποίηση δεδομένων σε πολλαπλά συστήματα θα παρέχει μια ολοκληρωμένη εικόνα της κατάστασης του περιβάλλοντος ΤΠΕ.
4. Τα παρακάτω στοιχεία δραστηριότητας πρέπει κατ' ελάχιστον να καταγράφονται σε audit logs:
  - User ID,

- Terminal identity,
- Log on και log off ώρα και ημέρα,
- Systems, data, applications, files, και networks στα οποία έχει γίνει πρόσβαση,
- Αποτυχημένες προσπάθειες πρόσβασης σε systems, data, applications, files, και δίκτυα,
- Αλλαγές σε system configurations και χρήση system utilities,
- Αλλαγές σε δικαιώματα πρόσβασης χρηστών (users access rights)
- Περιεχόμενο Network traffic, volume, και metadata (π.χ. προέλευση and προορισμός)
- Επίπεδα πρόσβασης και χρονοδιάγραμμα, με ιδιαίτερη έμφαση σε admin-level resources
- Χρήση πόρων ΤΠΕ, όπως επεξεργασία και αποθήκευση
- Logs και events από εφαρμογές και συσκευές

Η παρακολούθηση είναι συνεχής, εκτός εάν δικαιολογούνται εξαιρέσεις και εγκρίνονται από την ανώτατη διοίκηση. Οι ειδοποιήσεις διερευνώνται άμεσα και χρησιμοποιούνται αυτοματοποιημένες απαντήσεις όπου είναι εφικτό για την αποτελεσματική αντιμετώπιση των απειλών. Οι πληροφορίες απειλών (Threat intelligence), τόσο εσωτερικές όσο και εξωτερικές, ανατροφοδοτούν τις δραστηριότητες παρακολούθησης, διασφαλίζοντας επικαιροποιημένη αναγνώριση απειλών.

## 10. Υπολογιστικό Νέφος

### Cloud Computing

Η ΕΤΑΙΡΙΑ υιοθετεί βασικούς κανόνες και κατευθυντήριες γραμμές για την προστασία των κρίσιμων περιουσιακών στοιχείων της από τη χρήση του cloud.

Το Cloud computing είναι ένα μοντέλο που επιτρέπει την εύκολη, κατ' απαίτηση πρόσβαση του δικτύου σε μια κοινόχρηστη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων (π.χ., networks, servers, storage, applications, και services) που μπορούν να παρασχεθούν και να διατεθούν γρήγορα με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο υπηρεσιών cloud. Το Cloud computing επιτρέπει τη χρήση μιας υπολογιστικής υποδομής, ως υπηρεσία κατά παραγγελία (on-demand service) που διατίθεται μέσω του Διαδικτύου ή άλλου δικτύου υπολογιστών.

Από την χρήση υπηρεσιών Cloud computing προκύπτει όφελος από τις οικονομίες κλίμακας που επιτυγχάνονται μέσω της ευέλικτης χρήσης των πόρων, της εξειδίκευσης και άλλων πρακτικών δυνατοτήτων βελτίωσης της αποτελεσματικότητας. Ωστόσο, το cloud computing είναι μια αναδυόμενη μορφή distributed computing που εξακολουθεί να υφίσταται εξέλιξη και τυποποίηση. Ο ίδιος ο όρος χρησιμοποιείται συχνά σήμερα με μια σειρά εννοιών και ερμηνειών.

#### Μοντέλα ανάπτυξης Cloud Computing

Τα μοντέλα ανάπτυξης χαρακτηρίζουν ευρέως τη διαχείριση και τη διάθεση υπολογιστικών πόρων για την παροχή υπηρεσιών στους καταναλωτές, καθώς και τη διαφοροποίηση μεταξύ κατηγοριών

καταναλωτών. Ένα **δημόσιο υπολογιστικό νέφος** είναι εκείνο στο οποίο η υποδομή και οι υπολογιστικοί πόροι που περιλαμβάνει διατίθενται στο ευρύ κοινό μέσω του Διαδικτύου. Ανήκει και λειτουργεί από έναν πάροχο cloud που παρέχει υπηρεσίες cloud στους καταναλωτές και, εξ ορισμού, είναι εξωτερικό προς τις οργανώσεις των καταναλωτών.

Από την άλλη, ένα **ιδιωτικό cloud** είναι εκείνο στο οποίο το υπολογιστικό περιβάλλον λειτουργεί αποκλειστικά για έναν μόνο οργανισμό. Μπορεί να το διαχειρίζεται ο ίδιος ο οργανισμός ή τρίτος και μπορεί να φιλοξενηθεί εντός του Data Center του οργανισμού ή εκτός αυτού. Ένα ιδιωτικό cloud έχει τη δυνατότητα να δώσει στον οργανισμό μεγαλύτερο έλεγχο της υποδομής, των υπολογιστικών πόρων και των καταναλωτών cloud από ό, τι ένα δημόσιο cloud.

Μοντέλα υπηρεσιών υπολογιστικού νέφους

Το μοντέλο υπηρεσιών με το οποίο συμμορφώνεται ένα cloud υπαγορεύει το πεδίο εφαρμογής και τον έλεγχο ενός οργανισμού στο υπολογιστικό περιβάλλον και χαρακτηρίζει ένα επίπεδο αφαίρεσης για τη χρήση του. Ένα μοντέλο υπηρεσίας μπορεί να υλοποιηθεί ως δημόσιο cloud ή ως οποιοδήποτε από τα άλλα μοντέλα ανάπτυξης. Τρία γνωστά και συχνά χρησιμοποιούμενα μοντέλα υπηρεσιών είναι τα εξής::

- **Software-as-a-Service.** Software-as-a-Service (SaaS) είναι ένα μοντέλο παροχής υπηρεσιών σύμφωνα με το οποίο μία ή περισσότερες εφαρμογές και οι υπολογιστικοί πόροι για την εκτέλεσή τους παρέχονται για χρήση κατ' απαίτηση ως υπηρεσία «με το κλειδί στο χέρι». Ο κύριος σκοπός του είναι να μειώσει το συνολικό κόστος ανάπτυξης, συντήρησης και λειτουργίας υλικού και λογισμικού. Οι διατάξεις ασφαλείας εκτελούνται κυρίως από τον πάροχο cloud. Ο χρήστης του cloud δεν διαχειρίζεται ούτε ελέγχει την υποκείμενη υποδομή cloud ή μεμονωμένες εφαρμογές, εκτός από τις επιλογές προτιμήσεων και τις περιορισμένες ρυθμίσεις διαχειριστικών εφαρμογών.
- **Platform-as-a-Service.** Platform-as-a-Service (PaaS) είναι ένα μοντέλο παροχής υπηρεσιών στο πλαίσιο του οποίου η υπολογιστική πλατφόρμα παρέχεται ως υπηρεσία κατ' απαίτηση βάσει της οποίας μπορούν να αναπτυχθούν και να αναπτυχθούν εφαρμογές. Ο κύριος σκοπός του είναι να μειώσει το κόστος και την πολυπλοκότητα της αγοράς, της στέγασης και της διαχείρισης των υποκείμενων στοιχείων υλικού και λογισμικού της πλατφόρμας, συμπεριλαμβανομένων τυχόν απαραίτητων εργαλείων ανάπτυξης προγραμμάτων και βάσεων δεδομένων. Το περιβάλλον ανάπτυξης είναι συνήθως ειδικού σκοπού, καθορίζεται από τον πάροχο cloud και προσαρμόζεται στο σχεδιασμό και την αρχιτεκτονική της πλατφόρμας του. Ο χρήστης του cloud έχει τον έλεγχο των εφαρμογών και των ρυθμίσεων περιβάλλοντος εφαρμογών της πλατφόρμας. Οι προβλέψεις ασφαλείας κατανέμονται μεταξύ του παρόχου cloud και του χρήστη cloud.
- **Infrastructure-as-a-Service.** Infrastructure-as-a-Service (IaaS) είναι ένα μοντέλο παροχής υπηρεσιών όπου η βασική υπολογιστική υποδομή των servers, του λογισμικού και του εξοπλισμού δικτύου παρέχεται ως υπηρεσία κατ' απαίτηση πάνω στην οποία μπορεί να δημιουργηθεί μια πλατφόρμα για την ανάπτυξη και εκτέλεση εφαρμογών. Ο κύριος σκοπός του είναι να αποφευχθεί η αγορά, η στέγαση και η διαχείριση των βασικών στοιχείων υποδομής υλικού και λογισμικού και αντ' αυτού να αποκτήσει αυτούς τους πόρους ως εικονικά (virtual) αντικείμενα ελεγχόμενα μέσω ενός service interface. Ο χρήστης cloud έχει γενικά ευρεία ελευθερία να επιλέξει το λειτουργικό σύστημα και το περιβάλλον ανάπτυξης που θα φιλοξενηθεί. Οι διατάξεις ασφαλείας πέρα από τη βασική υποδομή πραγματοποιούνται κυρίως από τον χρήστη cloud.

## Πάροχοι cloud

Οι πάροχοι cloud προσφέρουν συνήθως τα προαναφερθέντα μοντέλα υπηρεσιών Cloud Computing με τη διαχείριση υποδομών, πλατφορμών ή εφαρμογών βάσει συγκεκριμένων συμβατικών απαιτήσεων και συμφωνιών επιπέδου υπηρεσιών (Service Level Agreements) με τους πελάτες τους. Καθώς οι πάροχοι cloud τείνουν να επεκτείνονται σε περισσότερες από μία περιοχές, πολιτείες ή περιοχές, πρέπει να διαχειριστούν την πολυπλοκότητα ενός ετερογενούς νομικού και κανονιστικού πλαισίου, εκτός από τις απειλές που σχετίζονται με την πληροφορική. Στο πλαίσιο της παροχής επαρκούς ασφάλειας πληροφοριών στους πελάτες τους, οι πάροχοι υπηρεσιών ενσωματώνουν πρότυπα ασφάλειας πληροφοριών ή/και επιτρέπουν στους πελάτες τους να διενεργούν ελέγχους στις εγκαταστάσεις.

## 11. Συνεχής Βελτίωση

### Continual Improvement

- 1) Ο Υπεύθυνος Ασφάλειας Πληροφοριών, σε συντονισμό με τα κατάλληλα ενδιαφερόμενα μέρη, συλλέγει και αναλύει δεδομένα (αναφορές συμβάντων ασφαλείας, αποτελέσματα επιθεωρήσεων και ελέγχων, εκτιμήσεις κινδύνου, αναλύσεις τάσεων) σε τακτική βάση για τον εντοπισμό πιθανών Ενεργειών για Βελτίωση.
- 2) Τυχόν περιπτώσεις μη συμμόρφωσης αντιμετωπίζονται. Είναι ευθύνη του Υπεύθυνου Ασφάλειας Πληροφοριών να διασφαλίζει ότι όλες οι διαπιστωμένες μη συμμορφώσεις αντιμετωπίζονται έγκαιρα και αποτελεσματικά.
- 3) Πρέπει να προσδιοριστεί η βασική αιτία (root cause) των μη συμμορφώσεων και να ληφθούν κατάλληλες Διορθωτικές Ενέργειες για την εξάλειψη της αιτίας, προκειμένου να αποφευχθεί η επανάληψή τους.
- 4) Οι Διορθωτικές Ενέργειες πρέπει να είναι κατάλληλες για τις μη συμμορφώσεις που σκοπεύουν να αντιμετωπίσουν.
- 5) Η συνεχής βελτίωση υποστηρίζεται από μετρήσιμες διαδικασίες και οργανωτική δομή που εξασφαλίζει υπευθυνότητα (accountability).
- 6) Οι διαδικασίες στο πλαίσιο της πολιτικής συνεχούς βελτίωσης αξιολογούνται για να διασφαλιστεί ότι η προσέγγιση παραμένει αποτελεσματική και αποδοτική για την παραγωγή των επιθυμητών αποτελεσμάτων.

### Εισερχόμενα για την Συνεχή Βελτίωση

Τα παρακάτω εισερχόμενα αξιοποιούνται για τον εντοπισμό (δυννητικών) μη συμμορφώσεων και δυννητικών βελτιώσεων:

- 1) Αξιολογήσεις κινδύνου για την ασφάλεια των πληροφοριών
- 2) Αξιολογήσεις επιδόσεων ασφαλείας πληροφοριών
- 3) Αποτελέσματα τεχνικών ελέγχων (Technical Assessment όπως VA, PenTest)
- 4) Επιθεωρήσεις και ανασκοπήσεις του ISMS
- 5) Συμβάντα ασφαλείας πληροφοριών
- 6) Αδυναμίες ασφαλείας πληροφοριών που παρατηρήθηκαν και αναφέρθηκαν από το προσωπικό.

## Διαχείριση βελτιώσεων

Ο υπεύθυνος ασφάλειας πληροφοριών διασφαλίζει ότι λαμβάνονται τα ακόλουθα μέτρα:

- 1) Ιεράρχηση ευκαιριών βελτίωσης με βάση τα αποτελέσματα των κριτηρίων αξιολόγησης
- 2) Σχεδιασμός της εφαρμογής των βελτιώσεων, συμπεριλαμβανομένου χρονοδιαγράμματος και αρμοδιοτήτων
- 3) Εφαρμογή των βελτιώσεων
- 4) Ενημέρωση τεκμηρίωσης όπως απαιτείται κατά τη διάρκεια/μετά την εφαρμογή των βελτιώσεων
- 5) Παρακολούθηση όλων των εγκεκριμένων Ενεργειών Βελτίωσης που αντιμετωπίζονται
- 6) Επαλήθευση της εφαρμογής προληπτικών και διορθωτικών ενεργειών σύμφωνα με το σχέδιο δράσης
- 7) Μέτρηση της επιτυχίας των βελτιώσεων ελέγχοντας τα αποτελέσματα ΚΡΙ πριν και μετά
- 8) Κατάλληλη αντίδραση σε μη επιτυχημένες βελτιώσεις
- 9) Ενημέρωση όλων των ενδιαφερόμενων μερών σχετικά με τις σχετικές βελτιώσεις.

## Σχέδιο Συνεχούς Βελτίωσης

Μόλις εντοπιστεί δυνητική βελτίωση ή προσδιοριστούν Διορθωτικές Ενέργειες, ο υπεύθυνος ασφάλειας πληροφοριών:

- 1) Αναπτύσσει ή επικαιροποιεί το σχέδιο για την εφαρμογή της βελτίωσης. Το σχέδιο περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα στοιχεία:
  - a. Τρέχουσα κατάσταση / δήλωση προβλήματος
  - b. Ανάλυση της βασικής αιτίας (root cause)
  - c. Σχέδια δράσης, συμπεριλαμβανομένων δραστηριοτήτων, χρονοδιαγραμμάτων, ευθύνης και εκτίμησης προϋπολογισμού
  - d. Αξιολόγηση του πώς η ΕΤΑΙΡΙΑ θα καθορίσει ότι η ενέργεια Βελτίωσης έχει επιτύχει τους επιδιωκόμενους στόχους της.
- 2) Υποβολή του σχεδίου συνεχούς βελτίωσης στην Διοίκηση για έγκριση πριν από την εφαρμογή.

## Εξερχόμενα

Επιπλέον, ενδέχεται να χρειαστεί να ενημερωθούν και άλλα στοιχεία του ISMS, όπως:

- 1) Πολιτικές, Διεργασίες & Διαδικασίες
- 2) Επιχειρησιακή τεκμηρίωση
- 3) Εκτίμηση Κινδύνου & Σχέδιο
- 4) Πρόγραμμα εσωτερικών επιθεωρήσεων
- 5) Πλαίσιο μέτρησης αποτελεσματικότητας

Ανασκόπηση από την Διοίκηση

Κατά τη διενέργεια της Ανασκόπησης από την Διοίκηση, η Διοίκηση:

- 1) Καθορίζει τυχόν νέους ή αναθεωρημένους στόχους ISMS που απαιτούν πρόσθετες ή τροποποιημένες ενέργειες βελτίωσης
- 2) Εξετάζει τις μη συμμορφώσεις και τις διορθωτικές ενέργειες που υπάρχουν σε εξέλιξη για να διασφαλίσει την καταλληλότητα
- 3) Εξετάζει την πρόοδο / αποτελεσματικότητα της συνολικής Πολιτικής Συνεχούς Βελτίωσης.
- 4) Διατυπώνει τυχόν πρόσθετες Ενέργειες Βελτίωσης ως αποτέλεσμα της Ανασκόπησης από τη Διοίκηση.
- 5) Η συχνότητα και η μορφή της Ανασκόπησης από τη Διοίκηση περιγράφεται στην σχετική Διαδικασία και τα πρακτικά Ανασκόπησης Διοίκησης.

Συχνότητα Ενεργειών Συνεχούς Βελτίωσης

Δραστηριότητες	Συχνότητα
Επανεξέταση και επικαιροποίηση των στόχων του ISMS.	Ετησίως
Επανεξέταση πολιτικής ασφάλειας πληροφοριών.	Ετησίως
Επανεξέταση όλων των Πολιτικών και των Διαδικασιών του ISMS.	Ετησίως
Διεξαγωγή εκπαιδευτικού προγράμματος ευαισθητοποίησης σχετικά με την ασφάλεια πληροφοριών για τους υπαλλήλους και τήρηση αρχείων.	Ετησίως
Επανεξέταση αξιολογήσεων κινδύνου ασφάλειας πληροφοριών.	Ετησίως ή όποτε υπάρχει αλλαγή στις υποδομές
Διεξαγωγή τεχνικών αξιολογήσεων (όπως Vulnerability Assessment, Penetration test, Configuration review κ.λπ.).	Ανά διετία ή όποτε υπάρχει αλλαγή στις υποδομές
Διεξαγωγή εσωτερικής επιθεώρησης, ανασκόπηση τεκμηρίωσης και αναφορά ευρημάτων.	Ετησίως
Διορθωτικές ενέργειες που προκύπτουν από περιστατικά / παρ' ολίγον περιστατικά.	Όποτε υπάρχουν περιστατικά / παρ' ολίγον περιστατικά.
Συναντήσεις Ανασκόπησης Συστήματος (ISMS) από την Διοίκηση	Ετησίως

## 12. Ανάπτυξη Συστήματος και Διαχείριση Αλλαγών

### System Development and Change Management

Τα χαρακτηριστικά ασφαλείας είναι αποτελεσματικότερα και οικονομικότερα εάν καθιερώνονται κατά τη φάση της σύλληψης της ιδέας και καθ' όλη τη διάρκεια της προμήθειας και της ανάπτυξης συστημάτων πληροφοριών. Με αυτόν τον τρόπο, μπορούν να σχεδιαστούν κατάλληλοι έλεγχοι σε αυτά. Ειδικότερα, ελέγχεται η πρόσβαση σε αρχεία του συστήματος, στο source code / object code shall be controlled as well as access to project and support environments και αντικειμενικό κώδικα, καθώς και η πρόσβαση σε περιβάλλοντα έργων και υποστήριξης.

### Αιτήσεις ασφάλειας συστημάτων

- Οι απαιτήσεις ασφάλειας πρέπει να προσδιορίζονται και να συμφωνούνται πριν από την ανάπτυξη ή την προμήθεια συστημάτων πληροφοριών.
- Τα ζητήματα ασφάλειας των πληροφοριών πρέπει να αντιμετωπίζονται στο στάδιο της ανάλυσης των απαιτήσεων σε κάθε έργο ανάπτυξης ή προμήθειας.
- Ένα έγγραφο που περιγράφει και εξηγεί τις ελάχιστες απαιτήσεις ασφάλειας πρέπει να αποτελεί υποχρεωτικό μέρος της διαδικασίας RFI (Request for Information) για νέα συστήματα, υπηρεσίες και προϊόντα που ενέχουν κινδύνους ασφάλειας.

### Ασφάλεια σε περιβάλλοντα ανάπτυξης και δοκιμών

Τα περιβάλλοντα έργου και υποστήριξης ελέγχονται αυστηρά.

- Πρέπει να υπάρχουν επίσημες διαδικασίες ελέγχου αλλαγών για το λογισμικό και τα δεδομένα του συστήματος πληροφοριών.
- Οι εφαρμογές επανεξετάζονται όταν πραγματοποιούνται αλλαγές στο λειτουργικό σύστημα για να διαπιστωθεί τυχόν επακόλουθες επιπτώσεις στην ασφάλεια και τη λειτουργικότητα.
- Τροποποιήσεις στα πακέτα λογισμικού θα γίνονται μόνο εάν είναι απαραίτητες και θα ελέγχονται και θα εγκρίνονται αυστηρά.
- Όποτε είναι δυνατόν, οι δοκιμές λογισμικού δεν θα πραγματοποιούνται σε live δεδομένα ή συστήματα.
- Τα Test data πρέπει να προστατεύονται και να ελέγχονται.
- Απαγορεύεται η μη εξουσιοδοτημένη πρόσβαση σε αρχεία συστήματος.
- Η εγκατάσταση λογισμικού σε live συστήματα ελέγχεται αυστηρά.

## 13. Διαχείριση Διαμόρφωσης

### Configuration Management

Όλοι οι εργαζόμενοι και τρίτα μέρη πρέπει να διαβάσουν, να κατανοήσουν και να συμμορφωθούν με αυτήν την πολιτική.

Το Τμήμα Πληροφορικής είναι υπεύθυνο για την εφαρμογή αυτής της πολιτικής σε όλα τα συστήματα και τις εφαρμογές πληροφορικής.

#### Βασική Διαμόρφωση

Οι εφαρμογές πρέπει να επιβάλλουν τους ακόλουθους ελέγχους ασφαλείας:

- a. Κρυπτογράφηση – Διασφάλιση εμπιστευτικότητας και ακεραιότητας δεδομένων κατά την αποθήκευση και τη μετάδοση.
- b. Έλεγχος ταυτότητας – Επαλήθευση της ταυτότητας των χρηστών και των συστημάτων που έχουν πρόσβαση σε πόρους πληροφορικής.
- c. Εξουσιοδότηση – Διασφάλιση ότι η πρόσβαση σε πόρους πληροφορικής εκχωρείται βάσει καθορισμένων ρόλων και δικαιωμάτων.

d. Καταγραφή – Καταγραφή συμβάντων και ενεργειών για παρακολούθηση, έλεγχο και αντιμετώπιση περιστατικών

## 14. Διαρροή Δεδομένων

### Data Leakage

Η ΕΤΑΙΡΙΑ παρακολουθεί συστήματα, δίκτυα και τερματικές συσκευές για τον εντοπισμό και την αποτροπή μη εξουσιοδοτημένης εξαγωγής ευαίσθητων πληροφοριών. Η παρακολούθηση πραγματοποιείται σύμφωνα με την ισχύουσα νομοθεσία και αποκλειστικά για την προστασία των ευαίσθητων δεδομένων του οργανισμού.

Κατηγορίες ευαίσθητων πληροφοριών. Τα ακόλουθα ταξινομούνται ως ευαίσθητα:

- Προσωπικά δεδομένα πελατών
- Αρχεία εργαζομένων
- Σχέδια / προδιαγραφές / χαρακτηριστικά προϊόντων και υπηρεσιών και στοιχεία πνευματικής ιδιοκτησίας
- Εμπιστευτικά οικονομικά στοιχεία
- Απαιτήσεις και χαρακτηριστικά πρακτικών για την αποτροπή της διαρροής δεδομένων

Ταυτοποίηση και ταξινόμηση

Ο οργανισμός εντοπίζει ευαίσθητες πληροφορίες και εφαρμόζει κατάλληλα επίπεδα διαβάθμισης για την προστασία από διαρροή δεδομένων, τηρώντας τις νομοθετικές απαιτήσεις.

#### **Η παρακολούθηση διαρροής δεδομένων καλύπτει:**

- Email services
- File transfers
- Αφαιρούμενα storage media

#### **Technical Controls:**

Εφαρμογή εργαλείων όπως Data Leakage Prevention (DLP) για τον εντοπισμό και την παρακολούθηση πιθανών παραβιάσεων δεδομένων. Περιορισμός της μη εξουσιοδοτημένης εξαγωγής δεδομένων μέσω μέτρων όπως:

- Αποκλεισμού copy-paste ή file transfers.
- Αποκλεισμού χρήσης αφαιρούμενων μέσων.

#### **Αντιμετώπιση περιστατικών:**

Λαμβάνονται άμεσα μέτρα σε περίπτωση μη εξουσιοδοτημένης εξαγωγής δεδομένων, όπως αποκλεισμός ενεργειών χρήστη ή διακοπή network transmissions.

#### **Ευαισθητοποίηση και ευθύνη χρήστη:**

Οι χρήστες εκπαιδεύονται τακτικά σχετικά με τους κινδύνους απώλειας δεδομένων και την πρόληψη. Οι εργαζόμενοι υποχρεούνται να αναφέρουν μη εξουσιοδοτημένες δραστηριότητες, συμπεριλαμβανομένων ενεργειών, όπως λήψη screenshots ή φωτογραφιών ευαίσθητων δεδομένων.

## Εργαλεία λογισμικού:

Όπου είναι δυνατόν, DLP software θα εντοπίσει και θα αποτρέψει αποκαλύψεις ευαίσθητων δεδομένων, όπως μη εξουσιοδοτημένη αποστολή email ή αντιγραφή αρχείων. Η μη εξουσιοδοτημένη εξαγωγή περιλαμβάνει οποιαδήποτε αντιγραφή, μετακίνηση ή εξαγωγή ευαίσθητων δεδομένων χωρίς την κατάλληλη άδεια σε εξωτερικές τοποθεσίες, όπως υπηρεσίες cloud, προσωπικούς λογαριασμούς email ή αφαιρούμενες συσκευές.

## 15. Κάλυψη / Ψευδωνυμοποίηση δεδομένων

### Data masking

Η χρήση τεχνικών data masking πρέπει πάντα να λαμβάνουν υπόψη τις υποχρεώσεις συμμόρφωσης της ΕΤΑΙΡΙΑΣ με την νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα (ΔΠΧ).

Αυτή η πολιτική ισχύει σε δύο κύριες κατηγορίες περιπτώσεων:

1. Όπου ΔΠΧ που τηρείται εσωτερικά, απαιτεί την εφαρμογή τεχνικών data masking προκειμένου να μειωθεί ο κίνδυνος.
2. Όταν πρόκειται να παρασχεθούν ΔΠΧ σε τρίτους, είναι σκόπιμο να εφαρμόζονται τεχνικές data masking για τη μείωση της έκτασης των ΔΠΧ ώστε να ανταποκρίνεται στον επιδιωκόμενο σκοπό της διαβίβασης.

Για λόγους συμμόρφωσης με τις αρχές του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), τα αρχεία που περιέχουν προσωπικά δεδομένα:

- αποθηκεύονται κατάλληλα, λαμβάνοντας υπόψη την ευαισθησία και την εμπιστευτικότητα του καταγεγραμμένου υλικού
- εξασφαλίζεται ότι είναι ανακτήσιμα και εύκολα ανιχνεύσιμα
- διατηρούνται μόνο για όσο διάστημα είναι απαραίτητο
- καταστρέφονται κατάλληλα για να διασφαλιστεί ότι τα πνευματικά δικαιώματα δεν παραβιάζονται και να αποφευχθεί η αποκάλυψη τους σε μη εξουσιοδοτημένα πρόσωπα

### Γενικές αρχές

- Η απόρριψη διασφαλίζει την εμπιστευτικότητα και τη συμμόρφωση με το GDPR και τις υποχρεώσεις εμπιστευτικότητας.
- Οι Information Asset Owners τηρεί μητρώο κατεστραμμένων αρχείων.
- Τα αρχεία απορρίπτονται χρησιμοποιώντας μεθόδους που εμποδίζουν τη μελλοντική ανάκτηση ή ανακατασκευή τους on-site ή off-site.
- Συμβάσεις με τρίτους περιλαμβάνουν όρους για ασφαλή διαγραφή δεδομένων κατά τη διάρκεια και μετά την περίοδο ισχύος της συμφωνίας.

### Μέθοδοι απόρριψης δεδομένων

1. Ηλεκτρονικά αρχεία:
  - Τα δεδομένα πρέπει να καθίστανται μη ανακτήσιμα (συμπεριλαμβανομένων των αντιγράφων ασφαλείας).
  - Ο Υπεύθυνος Ασφάλειας Πληροφοριών επιβλέπει την ασφαλή διαγραφή δεδομένων από όλα τα μέσα.

- Το εγκεκριμένο λογισμικό απόρριψης δεδομένων χρησιμοποιείται για τη μόνιμη καταστροφή δεδομένων, αποτρέποντας την ανάκτηση.
  - Αντίμετρα όπως degaussers εφαρμόζονται για μαγνητικά ή hardware-based μέσα αποθήκευσης.
2. Έντυπα αρχεία:
- Τα εμπιστευτικά αρχεία τεμαχίζονται ή απορρίπτονται σε ασφαλείς κάδους ή διαχείριση των οποίων γίνεται με ευθύνη του Υπεύθυνου Ασφάλειας Πληροφοριών.
3. System Configuration:
- Τα συστήματα και οι εγκαταστάσεις αποθήκευσης έχουν ρυθμιστεί για διαγραφή δεδομένων με βάση τις περιόδους διατήρησης που ορίζονται για κάθε κατηγορία δεδομένων ή τα αιτήματα πρόσβασης των υποκειμένων των ΔΠΧ.
  - Παλιά, περιττά ή προσωρινά αρχεία αφαιρούνται από παραγωγικά (live) συστήματα.

Διαγραφή δεδομένων όπου εμπλέκονται εξωτερικοί πάροχοι

- Οι πάροχοι cloud πρέπει να προσφέρουν δυνατότητες αυτόματης διαγραφής που ευθυγραμμίζονται με τις πολιτικές της ΕΤΑΙΡΙΑΣ και τον GDPR.
- Για το Hardware που εξέρχεται από τις εγκαταστάσεις (π.χ. για επισκευές) πρέπει πρώτα να αφαιρούνται οι μονάδες αποθήκευσης για να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα.

Διαγραφή δεδομένων σε Mobile Devices

- Εφαρμόζεται επαναφορά εργοστασιακών ρυθμίσεων για να σαρωθεί και αδειάσει πλήρως από δεδομένα (wipe) ο εσωτερικός χώρος αποθήκευσης και να επανέλθει το λειτουργικό σύστημα στην αρχική του κατάσταση.
- Οι μέθοδοι διαγραφής εξαρτώνται από το επίπεδο ταξινόμησης των αποθηκευμένων δεδομένων.

## 16. Web Filtering

- 1) Η πρόσβαση στο διαδίκτυο από συσκευές που παρέχονται από την ΕΤΑΙΡΙΑ παρακολουθείται ώστε να ελαχιστοποιείται η έκθεση σε κακόβουλο περιεχόμενο.
- 2) Όπου είναι δυνατόν, αυτό θα περιλαμβάνει πρόσβαση μέσω δικτύων εκτός του ελέγχου της ΕΤΑΙΡΙΑΣ, όπως ευρυζωνικές συνδέσεις ή κατά την εργασία απομακρυσμένα ή εν κινήσει.
- 3) Η παρακολούθηση συμμορφώνεται πάντα με τη σχετική νομοθεσία περί προστασίας ΔΠΧ.
- 4) Η πρόσβαση σε ιστότοπους που είναι ακατάλληλοι θα αποκλειστεί για τον χρήστη. (συγκεκριμένα αιτήματα πρόσβασης σε αποκλεισμένους ιστότοπους, αιτιολογημένα λόγω της δραστηριότητας ενδέχεται να επιτρέπονται από τη διοίκηση κατ' εξαίρεση).
- 5) Ο Υπ. Ασφάλειας Πληροφοριών διατηρεί κατάλογο με τις κατηγορίες ιστότοπων που έχουν αποκλειστεί, αυτές περιλαμβάνουν ιστότοπους οι οποίοι:
  - Φιλοξενούν κακόβουλο λογισμικό ή εμπλέκονται σε δραστηριότητες ηλεκτρονικού ψαρέματος (phishing),
  - Προκαλούν ανησυχία / υποψία για παράνομο περιεχόμενο (π.χ. file sharing),

- Παριέχουν ακατάλληλο περιεχόμενο, όπως σεξουαλικό, παράνομες ουσίες, αναφορές σε μισαλλοδοξία, βία και όπλα,
  - Φιλοξενούν downloads συγκεκριμένων τύπων αρχείων, όπως executables.
- 6) Η πρόσβαση σε ηλεκτρονικό ταχυδρομείο μέσω διαδικτύου επιτρέπεται, αλλά πρέπει να χρησιμοποιείται με προσοχή. Επιτρέπονται οι λήψεις μόνο αρχείων επιτρεπόμενου τύπου.
  - 7) Uploads αρχείων επιτρέπονται, αλλά υπόκεινται στην Πολιτική Πρόληψης Διαρροής Δεδομένων.
  - 8) Η πρόσβαση σε ιστότοπους social networking γενικά δεν επιτρέπεται, εκτός για διαχείριση του εταιρικού λογαριασμού (αν υπάρχει).
  - 9) Όλοι οι χρήστες ενημερώνονται ότι η πρόσβασή τους στο Διαδίκτυο παρακολουθείται σύμφωνα με την παρούσα πολιτική, και παρέχεται εκπαίδευση ευαισθητοποίησης σχετικά με τις κύριες απειλές που ενέχονται.
  - 10) Οι προσπάθειες πρόσβασης σε αποκλεισμένους ιστότοπους θα καταγράφονται και θα αναφέρονται στην διοίκηση (μπορούν να χρησιμοποιηθούν ως βάση πειθαρχικών μέτρων για περίπτωση επαναλαμβανόμενων προσπαθειών).
  - 11) Τροποποιήσεις στην πολιτική web filtering που υλοποιείται με το λογισμικό παρακολούθησης, γίνονται ελεγχόμενα από τον Υπ. Ασφάλειας Πληροφοριών ή άλλα εξουσιοδοτημένα στελέχη.

## 17. Threat Intelligence

Η ΕΤΑΙΡΙΑΣ συλλέγει και αναλύει πληροφορίες απειλών που διατίθενται από τρίτους (π.χ. από τους παρόχους λύσεων κυβερνοασφάλειας, τις ανακοινώσεις από αρμόδιες αρχές όπως η Αρχή Δίωξης Ηλεκτρονικού Εγκλήματος, η Αρχή Προστασίας ΔΠΧ) και σχετίζονται με την εταιρεία όσον αφορά τους κλάδους, τις αγορές και τις τοποθεσίες στις οποίες δραστηριοποιείται, την τεχνολογία που χρησιμοποιεί για την παροχή υπηρεσιών στους υπαλλήλους, τους συνεργάτες και τους πελάτες και τους κινδύνους που αντιμετωπίζει.

Η διαδικασία συλλογής και ανάλυσης πληροφοριών απειλών και οι ίδιες οι πληροφορίες απειλών που συλλέγονται, πρέπει να είναι όσο το δυνατόν ακριβέστερες και λεπτομερέστερες και να παρέχουν σαφή εφαρμόσιμη καθοδήγηση που μπορεί να χρησιμοποιηθεί για την κατάλληλη και έγκαιρη αντίδραση στο μεταβαλλόμενο τοπίο απειλών.

Για την επίτευξη αυτών των στόχων, τίθενται σαφείς στόχοι για την παραγωγή πληροφοριών σχετικά με απειλές, έτσι ώστε οι διαθέσιμοι πόροι να χρησιμοποιούνται αποτελεσματικά για να επικεντρωθούν σε θέματα που σχετίζονται με την τρέχουσα κατάσταση.

Ακολουθούνται καθορισμένες και τεκμηριωμένες διαδικασίες και διαδικασίες για να διασφαλιστεί ότι οι δραστηριότητες συλλογής πληροφοριών για απειλές είναι δομημένες και μετρήσιμες και ότι τα παραδοτέα που παράγονται πληρούν τα απαιτούμενα πρότυπα.

## 18. Διαχείριση για την Επιχειρησιακή Συνέχεια

Business continuity management

Η διαχείριση της επιχειρησιακής συνέχειας αποτελεί ουσιαστικό μέρος της διαδικασίας διαχείρισης κινδύνων, διασφαλίζοντας ότι οι κρίσιμες επιχειρηματικές δραστηριότητες αποκαθίστανται σύμφωνα με προκαθορισμένα χρονοδιαγράμματα μετά από οποιαδήποτε μεγάλη καταστροφή ή αποτυχία. Το Σχέδιο Επιχειρησιακής Συνέχειας της ΕΤΑΙΡΙΑΣ, έχει ως στόχο την με κάθε τρόπο ελαχιστοποίηση των επιπτώσεων καταστροφών. Αυτό περιλαμβάνει ελέγχους, μέτρα και προφυλάξεις για την αποφυγή καταστροφών, διαδικασίες και οδηγίες αποκατάστασης.

- Πρέπει να υπάρχουν τεκμηριωμένες διαδικασίες για την διατήρηση της επιχειρησιακής συνέχειας και σχέδια ανάκαμψης σε ολόκληρη την εταιρεία, σύμφωνα με τις επιχειρηματικές απαιτήσεις και προτεραιότητες.
- Το Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan) βασίζεται σε κατάλληλη εκτίμηση κινδύνου.
- Το Σχέδιο Επιχειρησιακής Συνέχειας περιέχει προβλέψεις για τη διατήρηση ή την αποκατάσταση των επιχειρηματικών δραστηριοτήτων εγκαίρως μετά από διακοπή ή αποτυχία κρίσιμων επιχειρηματικών διαδικασιών.
- Το Σχέδιο Επιχειρησιακής Συνέχειας υποβάλλεται σε τακτικές (τουλάχιστον ετησίως) δοκιμές και επικαιροποιείται με τακτικές επανεξετάσεις, ώστε να διασφαλίζεται ότι είναι εν ισχύ και αποτελεσματικό.

## 19. Τηλεργασία

### Teleworking

Η τηλεργασία δεν αποτελεί εναλλακτικό τρόπο εργασίας, αλλά μπορεί να εφαρμοστεί σε εξαιρετικές περιστάσεις, όπως καιρικά φαινόμενα ή άλλες καταστάσεις έκτακτης ανάγκης. Σε τέτοιες περιπτώσεις, μπορεί να επιτραπεί στους εργαζόμενους να εργάζονται εξ αποστάσεως προσωρινά.

Οι εργαζόμενοι πρέπει να λαμβάνουν προηγούμενη έγκριση από τον προϊστάμενο τους για τηλεργασία. Ο προϊστάμενος αξιολογεί το αίτημα με βάση τις επιχειρησιακές ανάγκες και σε συντονισμό με άλλο σχετικό διοικητικό προσωπικό. Η άδεια για τηλεργασία χορηγείται με βάση την επιλεξιμότητα του εργαζομένου και τις ειδικές συνθήκες της έκτακτης ανάγκης. Ο προϊστάμενος έχει πλήρη διακριτική ευχέρεια να εγκρίνει ή να απορρίψει αιτήματα τηλεργασίας.

Εάν απαιτείται τηλεργασία κατά τη διάρκεια καταστάσεων έκτακτης ανάγκης (π.χ. καιρικά φαινόμενα, πανδημίες), μπορεί να επιβληθεί προσωρινά σε ολόκληρο τον οργανισμό. Ο Γενικός Διευθυντής θα εφαρμόσει τηλεργασία με βάση την κατάσταση και θα κοινοποιήσει αυτή την απόφαση σε όλους τους υπαλλήλους.

Κατά τη διάρκεια της τηλεργασίας, οι εργαζόμενοι αναμένεται να διαχειρίζονται τον χρόνο τους σύμφωνα με τις ίδιες πολιτικές σαν να ήταν στο γραφείο. Οι εργαζόμενοι πρέπει να τηρούν τις ώρες εργασίας του οργανισμού, συμπεριλαμβανομένης της ανάγκης έγκρισης υπερωριών.

Οι τηλεεργαζόμενοι διαθέτουν καθορισμένο χώρο εργασίας απαλλαγμένο από περισπασμούς, με επαρκή φωτισμό και σταθερή σύνδεση στο διαδίκτυο. Εκτός από τον ειδικό εξοπλισμό που παρέχεται από την εταιρεία (π.χ. υπολογιστές, τηλέφωνα), οι εργαζόμενοι είναι υπεύθυνοι για την παροχή των δικών τους επίπλων και άλλου απαραίτητου εξοπλισμού.

Ο χειρισμός των εμπιστευτικών δεδομένων γίνεται με ασφάλεια και οι εργαζόμενοι ακολουθούν όλα τα πρωτόκολλα ασφαλείας για την προστασία των δεδομένων της εταιρείας. Αυτό περιλαμβάνει τη χρήση ασφαλών συστημάτων, τη διατήρηση προστασίας με κωδικό πρόσβασης σε συσκευές και τη διασφάλιση ενημερωμένης προστασίας από ιούς. Οποιαδήποτε παραβίαση της ασφαλείας των δεδομένων μπορεί να έχει ως αποτέλεσμα την άμεση αναστολή της άδειας για τηλεργασία.

Η απομακρυσμένη πρόσβαση στο δίκτυο της εταιρείας απαιτεί έγκριση διαχειριστή και πρέπει να γίνεται μέσω ασφαλών δικτύων (π.χ. VPN). Επιβάλλονται ισχυροί έλεγχοι αναγνώρισης, ελέγχου ταυτότητας και κρυπτογράφησης. Οι εργαζόμενοι διασφαλίζουν ότι οι συσκευές τους είναι ασφαλείς και ότι διατηρούνται αρχεία καταγραφής απομακρυσμένης πρόσβασης. Όταν χρησιμοποιούν κινητές συσκευές, οι εργαζόμενοι ακολουθούν αυστηρά πρωτόκολλα ασφαλείας, (όπως κωδικού πρόσβασης ή βιομετρικού ελέγχου ταυτότητας).

Οι εργαζόμενοι που εργάζονται εξ αποστάσεως διασφαλίζουν ότι χρησιμοποιούν ασφαλή, προστατευμένα με κωδικό πρόσβασης δίκτυα Wi-Fi και να αποφεύγουν τη χρήση δημόσιων Wi-Fi για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στα συστήματα της εταιρείας.