Πολιτική Ασφάλειας
της Cosmos Business Systems AEBE

Πολιτική Ασφάλειας –
Cosmos Business Systems

ΕΙΣΑΓΩΓΗ

Η Πολιτική Ασφάλειας περιγράφει το σύνολο των κανόνων που καθορίζουν τον τρόπο με τον οποίο η Cosmos Business Systems πρέπει να διαχειρίζεται και να προστατεύει το Πληροφοριακό της Σύστημα, έτσι ώστε να επιτυγχάνει συγκεκριμένους στόχους ασφάλειας. Παρέχοντας καθοδήγηση στα στελέχη της Εταιρείας αναφορικά με τον τρόπο οργάνωσης και επεξεργασίας των πληροφοριών, η Πολιτική Ασφάλειας αποτελεί το πλέον αποτελεσματικό μμέσο για την προστασία των δεδομένων που διαχειρίζεται η Cosmos Business Systems.

Η Πολιτική Ασφάλειας δεν είναι απόλυτη ή στατική. Αντιθέτως, είναι ένα κείμενο με δυναμική που πρέπει να αντανακλά τις αλλαγές στις προτεραιότητες της Δδιοίκησης της Εταιρείας καθώς και τις αλλαγές στο περιβάλλον και τις τεχνολογικές εξελίξεις. Η δυναμική αυτή επιβάλλει την συνεχή αναθεώρησή της ώστε να είναι πάντα επίκαιρη, σύμφωνα με τις εκάστοτε συνθήκες.
Η Πολιτική Ασφάλειας βασίστηκε στις απαιτήσεις των στρατηγικών κατευθύνσεων της Εταιρείας, σε σχέση με την αξιοποίηση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) και την ασφάλειά τους.

ΑΡΧΕΣ ΔΙΑΜΟΡΦΩΣΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Η Πολιτική Ασφάλειας του Πληροφοριακού Συστήματος της Εταιρείας Cosmos Business Systems δείχνει την πρόθεση της διοίκησης της Εταιρείας να προστατέψει το Πληροφοριακό Σύστημα. Με τη βοήθεια της Πολιτικής Ασφάλειας, η Εταιρεία Cosmos Business Systems καλείται να επιτύχει τους ακόλουθους στόχους:

- Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων και τη διασφάλιση του απορρήτου των επικοινωνιών
- Διασφάλιση της επιχειρησιακής της ικανότητας, στο βαθμό που εξαρτάται από την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα πληροφοριών και επικοινωνιών.

Λαμβάνοντας υπόψη τους στόχους προς επίτευξη, κατά την ανάπτυξη και σύνταξη της Πολιτικής Ασφάλειας που αφορά το Πληροφοριακό Σύστημα της Cosmos Business Systems, η Πολιτική Ασφάλειας έχει τα ακόλουθα χαρακτηριστικά:

- Είναι επίκαιρη σε σχέση με τις τρέχουσες τεχνολογικές εξελίξεις.
- Είναι γενικεύσιμή, ώστε η εφαρμογή της να είναι επεκτάσιμή σε μμελλοντικές νέες δραστηριότητες της Cosmos Business Systems
- Είναι σαφής, ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της.
- Αποτελεί πολιτική απαλλαγμένη από μη απαραίτητους τεχνικούς όρους, που θα την καθιστούσαν δύσκολη στην εφαρμογή και εξαρτημένη από τεχνολογικές επιλογές.

Η Πολιτική Ασφάλειας συντάχθηκε με γνώμονα ορισμένες βασικές αρχές, οι οποίες είναι οι ακόλουθες:

- Αποφυγή συγκεκριμένων ή εξειδικευμένων αναφορών έτσι ώστε να μην τροποποιείται συχνά, αλλά μόνον όταν συμβαίνουν σημαντικές αλλαγές στην διαχείριση της ασφάλειας του ΠΕΣ.
- Να είναι κατανοητή, αποτελεσματική και εφαρμόσιμή από άποψη κόστους.
- Να μην έχει τεχνικό μόνο χαρακτήρα.
- Να περιλαμβάνει ένα οργανωτικό πλαίσιο ρόλων και αρμοδιοτήτων για την ορθή εφαρμογή της.Για την πληρέστερη αξιοποίηση της Πολιτικής Ασφάλειας, το περιεχόμενό της θα πρέπει να γίνει γνωστό σε κάθε εργαζόμενο που εμπλέκεται στη χρήση του Πληροφοριακού Συστήματος. Αυτό απαιτεί την εκπαίδευση των εργαζομένων στη εφαρμογή της Πολιτικής Ασφάλειας.

Πολιτική Ασφάλειας –
Cosmos Business Systems

Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο

- Η Cosmos Business Systems δεσμεύεται για την τήρηση της νομοθεσίας που αφορά την προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά τη νομοθεσία που αφορά τη χρήση ΠΕΣ, καθώς και για την εφαρμογή των σχετικών αποφάσεων της Αρχής Προστασίας Προσωπικών Δεδομένων και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών.
- Η Εταιρεία καταρτίζει και εφαρμόζει διαδικασίες που διασφαλίζουν τη διατήρηση των δεδομένων των επικοινωνιών για το χρονικό διάστημα που ορίζει η νομοθεσία.
- Η Εταιρεία προβαίνει σε όλες τις ενέργειες που απαιτούνται, ώστε να παρέχει στις Αρχές διευκολύνσεις και πληροφορίες, όπως προβλέπει η σχετική νομοθεσία. Η Εταιρεία διασφαλίζει ότι οι σχετικές διευκολύνσεις και πληροφορίες παρέχονται μόνο στις περιπτώσεις που προβλέπονται από τη νομοθεσία, ακολουθώντας νόμιμες διαδικασίες.
- Η Διοίκηση της Εταιρείας και ειδικότερα τα στελέχη της Διαχείρισης Ανθρώπινου Δυναμικού μμεριμνούν ώστε όλα τα μέλη του προσωπικού να γνωρίζουν τις υποχρεώσεις τους που απορρέουν από τη νομοθεσία σχετικά με την επεξεργασία προσωπικών πληροφοριών και τη διασφάλιση του απορρήτου των επικοινωνιών.
- Η Διοίκηση μεριμνά για την ανάπτυξη οργανωτικών δομών και διαδικασιών με στόχο την προστασία της Εταιρείας από νομικές ενέργειες που στρέφονται εναντίον της.
- Η Εταιρεία μεριμνά για την προστασία του προσωπικού από νομικές συνέπειες που μπορεί να προκύψουν από ενέργειές τους στα πλαίσια της άσκησης των καθηκόντων τους και εφόσον τηρούν πιστά τις πολιτικές και τους κανονισμούς της Εταιρείας.

Οργανωτική υποδομή

- Η Εταιρεία αναπτύσσει κατάλληλες οργανωτικές και διοικητικές δομές για την αποτελεσματική διαχείριση της ασφάλειας ΠΕΣ. Η ευθύνη για τη διαχείριση της ασφάλειας ΠΕΣ ανατίθεται σε ανεξάρτητη Διεύθυνση. Ο επικεφαλής της Διεύθυνσης αναλαμβάνει το ρόλο του Υπεύθυνου Ασφάλειας ΠΕΣ
- Η Εταιρεία μεριμνά για την επαρκή στελέχωση των διευθύνσεων που έχουν ενεργό ρόλο στην ασφάλεια των ΠΕΣ
- Στο οργανόγραμμά της Εταιρείας εντάσσεται ο ρόλος του Υπεύθυνου Ασφάλειας ΠΕΣ.
- Όλες οι διαδικασίες που αφορούν την ασφάλεια ΠΕΣ. είναι καταγεγραμμένες. Για κάθε διαδικασία πρέπει να ορίζεται ένας υπεύθυνος για την καταγραφή, τον έλεγχο της αποτελεσματικότητας, την επικαιροποίηση και τη διάθεσή της στα
- μέλη του προσωπικού που έχουν ανάγκη γνώσης ("need-to-know").

Πολιτική Ασφάλειας –
Cosmos Business Systems

1. ΠΟΛΙΤΙΚΗ ΑΠΟΔΕΚΤΗΣ ΧΡΗΣΗΣ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Εισαγωγή

Η Πολιτική Αποδεκτής Χρήσης ρυθμίζει τα θέματα που αφορούν στη χρήση του Πληροφοριακού Συστήματος που υποστηρίζει τις δραστηριότητες της Εταιρείας. Η πολιτική αυτή συμβάλει στο να γνωρίζουν οι χρήστες ποιες ενέργειές τους θεωρούνται επιτρεπτές και ποιες μη επιτρεπτές.

Η αποτελεσματική ασφάλεια είναι μια συλλογική προσπάθεια που στηρίζεται στη συμμετοχή και την υποστήριξη του κάθε μέλους του προσωπικού που χειρίζεται πληροφορίες ή/και πληροφοριακά συστήματα.

Πεδίο Εφαρμογής

Η πολιτική αυτή απευθύνεται στα μέλη του προσωπικού της Εταιρείας και στους συνεργάτες της Εταιρείας που χρησιμοποιούν και υποστηρίζουν δραστηριότητες της Cosmos Business Systems.

Η Διεύθυνση Ανθρώπινου Δυναμικού στις ενέργειες πρόσληψης προσωπικού ή συνεργατών τούς κοινοποιεί την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας και εξασφαλίζει με τη "Δήλωση Εργαζομένου" ότι έχουν λάβει γνώσει και αποδεχτεί την Πολιτική αυτή.

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας.

Πολιτική

1. Τα Πληροφοριακά Συστήματα συγκαταλέγονται στους πολυτιμότερους πόρους της Εταιρείας και κάθε μέλος του προσωπικού έχει την υποχρέωση να τα χρησιμοποιεί με σύνεση.
2. Τα Πληροφοριακά Συστήματα που προσφέρονται στο προσωπικό της Εταιρείας αποτελούν περιουσιακό της στοιχείο και η χρήση τους πρέπει να γίνεται αποκλειστικά για τους σκοπούς της Εταιρείας.
3. Η χρήση των Πληροφοριακών Συστημάτων συνεπάγεται την ανάληψη ευθυνών και υποχρεώσεων που περιγράφονται στην Πολιτική Αποδεκτής Χρήσης.

Δικαιώματα και Υποχρεώσεις Χρηστών

Οι παρακάτω δραστηριότητες παρέχουν ένα πλαίσιο με τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις του Πληροφοριακού Συστήματος.

Χρήση συστημάτων και δικτύων

1. Το προσωπικό πρέπει να χρησιμοποιεί το ΠΕΣ της Εταιρείας σύμφωνα με τα όσα προβλέπονται στην παρούσα Πολιτική Αποδεκτής Χρήσης.
2. Οι χρήστες οφείλουν να λαμβάνουν όλα τα μέτρα που υποδεικνύουν οι υπεύθυνοι της Εταιρείας για τη διασφάλιση του απορρήτου των επικοινωνιών τους.

   Η εταιρεία οφείλει να ενημερώνει τους χρήστες των παρεχόμενων υπηρεσιών τουλάχιστον κατά την σύναψη της μεταξύ τους σύβασης αλλά και σε τακτά χρονικά διαστήματα σχετικά με τα μέτρα που ενδείκνυται να λαμβάνουν για την προστασία του απορρήτου των επικοινωνιών τους , ιδίως σχετικά με κανόνες ορθής χρήσης των παρεχόμενων υπηρεσιών αλλά και τους τρόπους χρήσης τεχνολογιών και πόρων σχετικών με την ασφάλεια των πληροφοριών που σχετίζονται με τη διασφάλιση του απορρήτου των επικοινωνιών.
4. Τα εφεδρικά αντίγραφα πρέπει να τυγχάνουν μεταχείρισης του ιδίου επιπέδου κρισιμότητας και ευαισθησίας με τα δεδομένα και τις εφαρμογές που αποθηκεύονται σ' αυτά.
5. Τα εφεδρικά αντίγραφα μεταφέρονται σε μια ασφαλή, περιβαλλοντικά-ελεγχόμενη τοποθεσία εκτός του κτηρίου που φιλοξενεί το Μηχανογραφικό Κέντρο της Εταιρείας.
6. Κάθε σύστημα έχει ένα καθορισμένο πρόγραμμα διατήρησης εφεδρικών αντιγράφων που θα συμμορφώνεται με τις πολιτικές διατήρησης δεδομένων της Εταιρείας.

7. Περιοδικά εξετάζονται οι διαδικασίες λήψης εφεδρικών αντιγράφων και ανάκτησης δεδομένων από εφεδρικά αντίγραφα για να διασφαλιστεί ότι τα δεδομένα μπορούν να ανακτηθούν αποτελεσματικά από τα εφεδρικά αντίγραφα.

8. Η εταιρεία καταγράφει και εφαρμόζει λεπτομερείς διαδικασίες για τη διεξαγωγή της λήψης εφεδρικών αντιγράφων, την ανάκτηση δεδομένων, την διεξαγωγή εξέτασης των εφεδρικών αντιγράφων, τη μεταφορά των ταινιών από/προς τις εγκαταστάσεις αποθήκευσης και την ανακύκλωση ή εξουδετέρωση των εφεδρικών αντιγράφων με τη πάροδο της περιόδου διατήρησής τους. Σκοπός των ενεργειών αυτών είναι η αποτροπή αποκάλυψης δεδομένων επικοινωνίας των χρηστών των παρεχόμενων υπηρεσιών σε μη εξουσιοδοτημένα άτομα.

9. Οι χρήστες οφείλουν να ενημερώνουν άμεσα το Τμήμα Ασφάλειας αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας συστήματος που θέτει σε κίνδυνο το απόρρητο επικοινωνιών των ίδιων ή άλλων χρηστών.

10. Οι χρήστες υποχρεούνται να συμμορφώνονται με την νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας.

11. Οι χρήστες δεν επιτρέπεται να συμμετέχουν σε οποιαδήποτε παράνομή δραστηριότητα, βάσει εθνικού ή ευρωπαϊκού δικαίου, κάνοντας χρήση των πληροφοριακών πόρων της Εταιρείας.

12. Δεν επιτρέπεται η χρήση λογισμικού που δεν έχει αποκτηθεί με νόμιμο τρόπο.

13. Δεν επιτρέπεται η χρήση οποιουδήποτε υλικού ή λογισμικού που δεν είναι σε γνώση της Διεύθυνσης Πληροφορικής.

14. Η εγκατάσταση υλικού και λογισμικού στους Η/Υ των χρηστών γίνεται μόνο από το εξουσιοδοτημένο προσωπικό του Τμήματος Τεχνικής Υποστήριξης.

15. Οι χρήστες δεν πρέπει να παραβιάζουν τους ελέγχους πρόσβασης (access controls), ακόμα και αν αυτοί είναι ανεπαρκείς.

16. Δεν επιτρέπεται οποιαδήποτε ενέργεια μη εξουσιοδοτημένης χαρτογράφησης του δικτύου και η διεξαγωγή οποιασδήποτε μορφής παρακολούθησης του δικτύου της Εταιρείας.

17. Δεν επιτρέπεται η χρήση υπολογιστικών συστημάτων που δεν ανήκουν στην Εταιρεία για εργασίες της Εταιρείας.

18. Τα μέλη του προσωπικού που διαθέτουν φορητό υπολογιστή, ο οποίος παρέχεται από την Εταιρεία και χρησιμοποιείται για εργασιακούς σκοπούς, πρέπει να συμμορφώνονται με τις πολιτικές που ισχύουν για το σχετικό εξοπλισμό (Πολιτική Φορητών Υπολογιστών).

19. Δεν επιτρέπεται η εισαγωγή κακόβουλων προγραμμάτων στο δίκτυο ή τους κεντρικούς υπολογιστές (π.χ., ιοί, σκουλήκια, Δούρειοι Ίπποι, e-mail bombs, κ.λπ.).

20. Όλοι οι υπολογιστές που χρησιμοποιούνται από υπαλλήλους που συνδέονται με το Internet/Intranet/Extranet της Εταιρείας πρέπει να εκτελούν συνεχώς το εγκεκριμένο λογισμικό ανίχνευσης ιών με μια ενημερωμένη βάση δεδομένων ιών.

21. Όλοι οι υπολογιστές πρέπει να κάνουν χρήση της λειτουργία προφύλαξης οθόνης (screensaver) με προστασία κωδικού πρόσβασης ή να γίνεται κλείδωμά του ηλεκτρονικού υπολογιστή κατά την απομάκρυνση του χρήστη.

22. Οι χρήστες υποχρεούνται να συμμορφώνονται με την εκάστοτε ισχύουσα “Πολιτική Κωδικών Πρόσβασης“ για τη σωστή επιλογή και διαχείριση αυτών.

Χρήση Ηλεκτρονικού Ταχυδρομείου και Παγκοσμίου Ιστού

1. Η πρόσβαση στο Διαδίκτυο παρέχεται στο προσωπικό της Εταιρείας για να χρησιμοποιηθεί για τους σκοπούς της Εταιρείας και για τη βελτίωση των γνώσεων και δεξιοτήτων του ανθρώπινου δυναμικού της.

2. Η Εταιρεία διατηρεί το δικαίωμα να περιορίσει την πρόσβαση σε συγκεκριμένους Ισοτόπους (Web Sites) του Παγκόσμιου Ιστού (World Wide Web). Οι χρήστες που χρειάζονται πρόσβαση σε Ισοτόπους που η πρόσβαση έχει περιοριστεί έχουν το δικαίωμα να υποβάλλουν σχετικό αίτημα στο Τμήμα Τεχνικής Υποστήριξης.

2. ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΕΦΕΔΡΙΚΩΝ ΑΝΤΙΓΡΑΦΩΝ

Εισαγωγή

Υπάρχουν πολλές απειλές που θα μπορούσαν να προκαλέσουν απώλεια, φθορά ή προσωρινή μη-διαθεσιμότητα των δεδομένων. Αυτές περιλαμβάνουν, ενδεικτικά και όχι περιοριστικά, αστοχίες υλικού, τυχαία διαγραφή, λανθασμένη τροποποίηση, φθορά λογισμικού και κακόβουλες ενέργειες. Οι προαναφερόμενες απειλές είναι πολύ κοινές και αναπόφευκτα
μερικές από αυτές θα εμφανιστούν περιστασιακά στην Εταιρεία.
Είναι επομένως αναγκαίο η Εταιρεία να διατηρεί εφεδρικά αντίγραφα όλων των κρίσιμων δεδομένων και συστημάτων έτσι ώστε να μπορούν να χρησιμοποιηθούν για να παρέχουν συνεχή διαθεσιμότητα και βιωσιμότητα αυτών των πόρων όταν εμφανίζονται τέτοια περιστατικά.

Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους πληροφοριακούς πόρους της Εταιρείας.

3. ΠΟΛΙΤΙΚΗ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ (Physical and Environmental Security)

Εισαγωγή

Είναι κρίσιμο και αναγκαίο για την Εταιρεία να εφαρμόζει μέτρα προστασίας φυσικής ασφάλειας για την προστασία των πληροφοριακών της πόρων. Τα μέτρα αυτά πρέπει να εφαρμόζονται σε όλους τους διοικητικούς, φυσικούς, και τεχνικούς χώρους και περιλαμβάνουν τη χρήση κλειδαριών, διοικητικών ελέγχων και μέτρων για την προστασία από τη ζημία που προέρχεται από σκόπιμές πράξεις, ατυχήματα, πυρκαγιές και περιβαλλοντικούς κινδύνους.

Η πολιτική αυτή ορίζει τις διαδικασίες, τις οδηγίες και τα πρότυπα που αφορούν την εφαρμογή των φυσικών μέτρων ασφάλειας με σκοπό να προστατεύσουν τους πληροφοριακούς πόρους της Εταιρείας. Δεν αφορά την προστασία του προσωπικού, των εγκαταστάσεων και της περιουσίας που δεν συνδέεται άμεσα με τις τεχνολογίες πληροφορικής.

Πολιτική
Διαδικασίες & Οδηγίες

a) Η φυσική πρόσβαση στους πληροφοριακούς πόρους ελέγχεται ανάλογα της κατηγοριοποίησης του πόρου και το επίπεδο κινδύνου.

b) Οι χώροι που φιλοξενούν ευαίσθητους πληροφοριακούς πόρους απαιτούν ειδικά μέτρα προστασίας για να περιοριστεί η πρόσβαση σε αυτούς τους πόρους:

1) Η είσοδος σε αυτούς τους χώρους περιορίζεται στο προσωπικό που εργάζεται στο συγκεκριμένο χώρο και στα άτομα που τους έχει συγκεκριμένα χορηγηθεί η πρόσβαση στο χώρο.

2) Το προσωπικό που εργάζεται στο χώρο συνοδεύει το προσωπικό χωρίς κατάλληλη διαβάθμιση ασφάλειας.

3) Όταν προσωπικό χωρίς κατάλληλη διαβάθμιση ασφάλειας παρευρίσκεται σε αυτούς τους χώρους, οι ευαίσθητες πληροφορίες πρέπει να προστατεύονται από την παρατήρηση, αποκάλυψη ή απάλειψη (αφαίρεση). Αυτό περιλαμβάνει την αποθήκευση των εγγράφων σε μη εμφανή σημεία και την τοποθέτηση των οθονών Η/Υ έτσι ώστε να αποτραπεί η παρατήρησή τους από τα μη εξουσιοδοτημένα πρόσωπα.

c) Οι χώροι που φιλοξενούν κρίσιμους πληροφοριακούς πόρους τυγχάνουν ειδικών μέτρων προστασίας ώστε να διασφαλιστεί η διαθεσιμότητα αυτών των πόρων:

4. ΠΟΛΙΤΙΚΗ ΛΟΓΙΚΗΣ ΠΡΟΣΒΑΣΗΣ

Εισαγωγή

Οι χρήστες πρέπει να έχουν πρόσβαση στους πληροφοριακούς πόρους που απαιτούνται για να διεκπεραιώσουν τις εργασίες τους. Εντούτοις, η υπερβολική ή η ανεξέλεγκτη πρόσβαση μπορεί να οδηγήσει στη μη εξουσιοδοτημένη ή ακούσια αποκάλυψη, τροποποίηση ή καταστροφή των πόρων, καθώς και στον καταλογισμό ευθύνης για αμέλεια στην προστασία των πόρων. Επομένως, η πρόσβαση σε συγκεκριμένους πόρους χορηγείται μόνο στο εξουσιοδοτημένο προσωπικό που έχει μια εύλογη ανάγκη να χρησιμοποιήσει αυτούς τους πόρους. Τα προνόμια πρόσβασης σ' αυτούς τους πόρους περιορίζονται σ' εκείνα που απαιτούνται για την εκτέλεση των καθηκόντων του εξουσιοδοτημένου προσωπικού.

Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους χρήστες, ιδιοκτήτες και διαχειριστές πληροφοριών καθώς και για οποιαδήποτε πρόσβαση στους πληροφοριακούς πόρους της Εταιρείας. Στην παρούσα πολιτική γίνεται ιδιαίτερη αναφορά για τον έλεγχο πρόσβασης που αφορά τους χρήστες της υπηρεσίας ηλεκτρονικού ταχυδρομείου και τις λοιπές υπηρεσίες που παρέχονται μέσω της διαδικτυακής πύλης της εταιρείας (http://www.cbs.gr)

Πολιτική

Διαδικασίες & Οδηγίες

- Στους χρήστες πρέπει να χορηγούνται συγκεκριμένα δικαιώματα πρόσβασης σε κάθε σύστημα, τα οποία πρέπει να περιορίζονται σε εκείνα που απαιτούνται για να εκτελέσουν τις εργασίες τους.
- Οι χρήστες πρέπει να έχουν την έγκριση του ιδιοκτήτη των πληροφοριών πριν από τη χορήγηση της πρόσβασης σε έναν επιμέρους πόρο.
- Οι χρήστες πρέπει να προσπελαύνουν μόνο τους πόρους για τους οποίους έχουν εξουσιοδότηση, ανεξάρτητα από τα πραγματικά δικαιώματα συστήματος.
- Οι χρήστες δεν πρέπει να παρακάμπτουν τα δικαιώματα που χορηγούνται στους λογαριασμούς τους προκειμένου να αποκτήσουν πρόσβαση σε μη εξουσιοδοτημένους πληροφοριακούς πόρους.
- Οι χρήστες πρέπει να προστατεύουν τους λογαριασμούς τους:
    - Δεν πρέπει να επιτρέπουν σε τρίτους να χρησιμοποιούν τον λογαριασμό τους ή να χρησιμοποιούν τους υπολογιστές τους όταν είναι συνδεδεμένοι με το λογαριασμό τους, εκτός εάν απαιτείται για τη διαχείριση του συστήματος.
    - Οι χρήστες φέρουν την ευθύνη για οποιαδήποτε δραστηριότητα λαμβάνει μέρος στο ΠΕΣ με τη χρήση του δικούς τους αναγνωριστικού ταυτότητας «user ID» (δεδομένου ότι μόνο αυτοί πρέπει να έχουν πρόσβαση στο userID τους).
    - Όταν ο υπολογιστής τους είναι αφύλακτος, οι χρήστες είτε αποσυνδέονται είτε θέτουν σε λειτουργία την προστασία του συστήματος τους (όπως προφύλαξη οθόνης «screensaver» με κωδικό πρόσβασης).
- Το επίπεδο ελέγχου πρόσβασης εξαρτάται από την κατηγοριοποίηση του πόρου και το επίπεδο κινδύνου που συνδέεται με τον πόρο.
- Η εταιρεία ακολουθεί διαδικασία διαχείρισης χρηστών στην οποία περιγράφονται τα παρακάτω:
    - ο τρόπος προσθήκης νέων χρηστών, η διαγραφή χρηστών καθώς και η αναμονή και μεταβολή δικαιωμάτων ή επιπέδων πρόσβασης
    - να προβλέπεται η υποχρέωση τήρησης αρχείου των αιτήσεων που αφορούν σε κάθε μεταβολή στην κατάσταση πρόσβασης των χρηστών
    - να προβλέπεται η υποχρέωση τήρησης αρχείου με το ιστορικό όλων των δικαιωμάτων ή επιπέδων πρόσβασης των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα ΠΕΣ της εταιρείας

5. ΠΟΛΙΤΙΚΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

Εισαγωγή

Οι κωδικοί πρόσβασης (passwords) είναι μια από τις πιο σημαντικές συνιστώσες της ασφάλειας υπολογιστών. Αποτελούν την πρώτη γραμμή προστασίας για τους λογαριασμούς χρηστών (user accounts). Ένας κακώς επιλεγμένος κωδικός πρόσβασης εκθέτει την Εταιρεία στον κίνδυνο της πρόσβασης των Συστημάτων της από μη εξουσιοδοτημένα άτομα, με αποτέλεσμα να υπάρχει το ενδεχόμενο να παραβιαστούν και να τροποποιηθούν αυθαίρετα τα δεδομένα του συστήματος και να απειλείται η ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των πληροφοριών της.

Πεδίο εφαρμογής

Το πεδίο εφαρμογής αυτής της πολιτικής περιλαμβάνει όλα τα μέλη του προσωπικού που έχουν ή είναι υπεύθυνοι για κάποιο λογαριασμό σε οποιοδήποτε σύστημα/εφαρμογή στο δίκτυο της Εταιρείας.

Πολιτική

Οδηγίες δημιουργίας κωδικών πρόσβασης

Ο κωδικός πρόσβασης πρέπει**:**

- να μην είναι λέξη που μπορεί να βρεθεί σε λεξικό αναζήτησης, να μην περιέχει ονόματα, ημερομηνίες, επαναλαμβανόμενους χαρακτήρες (aaabbb, qwerty, 123321, κ.λπ.)
- να περιέχει κεφαλαία και μικρά γράμματα, αριθμούς και ειδικούς χαρακτήρες (!@#$%&*()[]{}<>/?=+-\….)
- να περιέχει τουλάχιστον έναν αλφαβητικό χαρακτήρα και τουλάχιστον ένα ψηφίο ή ειδικό χαρακτήρα
- να έχει μήκος τουλάχιστον οκτώ (8) χαρακτήρες

Οδηγίες προστασίας κωδικών πρόσβασης

- Να μην αποκαλύπτεται σε τρίτους, έστω και εάν αυτοί είναι υπάλληλοι της Εταιρείας, ανώτερα διοικητικά στελέχη ή ακόμα και οι διαχειριστές (μμηχανικοί) των πληροφοριακών Συστημάτων της Εταιρείας.
- Να μη σημειώνεται ούτε ηλεκτρονικά (π.χ. κινητά τηλέφωνα, σημειώσεις του outlook, κ.λπ.) ούτε χειρόγραφα, (π.χ. ατζέντες, ημερολόγια, post-it κ.λπ.).
- Οι χρήστες να μην αποκαλύπτουν τον κωδικό πρόσβασης σε συναδέλφους όταν πρόκειται να απουσιάσουν (πχ. λόγω αδείας ή ασθενείας).
- Οι κωδικοί πρόσβασης των διαχειριστών Συστημάτων/εφαρμογών που δεν κατέχουν πλέον τη συγκεκριμένη θέση πρέπει να αλλάζονται άμεσα.
- Οι Υπεύθυνοι Ασφάλειας Συστημάτων πρέπει να πραγματοποιούν ελέγχους για την ασφάλεια των κωδικών πρόσβασης.
- Να αλλαχτεί αμέσως αν υπάρχει η υπόνοια ότι έχει αποκαλυφθεί.
- Να αλλάζει τουλάχιστον κάθε 4 μήνες (120 ημέρες).
- Να είναι διαφορετικός από τον εξ’ ορισμού (default) κωδικό (public, private, system) της υπηρεσίας που

6. ΠΟΛΙΤΙΚΗ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΛΟΓΙΚΗΣ ΠΡΟΣΒΑΣΗΣ

Εισαγωγή

Η υπηρεσία απομακρυσμένης λογικής πρόσβασης παρέχει σύνδεση στο δίκτυο της Εταιρείας μέσω ενός, μη ελεγχόμενου από την Εταιρεία, δικτύου, συσκευής ή μέσου. Χρησιμοποιώντας την υπηρεσία απομακρυσμένης λογικής πρόσβασης, οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο, τις υπηρεσίες αρχείων, τις επιχειρησιακές εφαρμογές και τις IP-βασισμένες υπηρεσίες της Εταιρείας, εφόσον μπορούν να παρασχεθούν.

Πεδίο Εφαρμογής

Η πολιτική αυτή ισχύει για όλο το προσωπικό της Εταιρείας, τους αναδόχους και προμηθευτές που χρησιμοποιούν εταιρικό ή ιδιόκτητο Η/Υ για να συνδεθούν στο δίκτυο της Cosmos Business Systems. Η πολιτική αυτή ισχύει για τις συνδέσεις απομακρυσμένης πρόσβασης που χρησιμοποιούνται για την εκτέλεση εργασίας για λογαριασμό της Εταιρείας.

Πολιτική

1. Η Εταιρεία οφείλει να εξασφαλίζει ότι για την απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών στο δίκτυο της, δίνεται η ίδια σημασία με την τοπική σύνδεση του χρήστη, καθώς και ότι η πρόσβαση του χρήστη θα πρέπει να περιορίζεται στις περιπτώσεις που αυτό είναι αναγκαίο για τις επιχειρησιακές του ανάγκες.
2. Η υπηρεσία απομακρυσμένης λογικής πρόσβασης παρέχεται από την Διεύθυνση Πληροφορικής (οι πύλες της υπηρεσίας εγκαθιδρύονται και ρυθμίζονται από το τμήμα Τεχνικής Υποστήριξης). Σε κανένα άλλο τμήμα δεν επιτρέπεται να υλοποιήσει υπηρεσίες αυτής.
3. Όλη η δικτυακή δραστηριότητα, κατά τη διάρκεια μιας συνόδου απομακρυσμένης πρόσβασης, υπόκειται στις Πολιτικές Ασφάλειας της Εταιρείας και μπορεί να καταγράφεται.
4. Η απομακρυσμένη πρόσβαση ελέγχεται με τη χρήση κωδικού πρόσβασης
5. Η απομακρυσμένη πρόσβαση πραγματοποιείται με χρήση μηχανισμών ασφαλούς αυθεντικοποίησης και κρυπτογράφησης (π.χ. μέσω VPN)
6. Οι υπάλληλοι και οι ανάδοχοι της Εταιρείας με προνόμια απομακρυσμένης πρόσβασης πρέπει να εξασφαλίσουν ότι ο προσωπικός Η/Υ, με τον οποίο συνδέονται στο εταιρικό δίκτυο της Cosmos Business Systemsαπό απόσταση, δε συνδέεται συγχρόνως με οποιοδήποτε άλλο δίκτυο.

7. Οι χρήστες απομακρυσμένης πρόσβασης θα αποσυνδέονται αυτόματα από το εταιρικό δίκτυο της Cosmos Business Systems μετά από τριάντα λεπτά αδράνειας. Τα "Pings" ή άλλες τεχνητές διαδικασίες δικτύων δε μπορούν να χρησιμοποιηθούν για να κρατήσουν τη σύνδεση ανοικτή.
8. Η Εταιρεία οφείλει να εξασφαλίζει ότι η απομακρυσμένη πρόσβαση συνεργατών θα πρέπει να επιτρέπεται μόνο για συγκεκριμένο χρονικό διάστημα και να γίνεται είτε με την χρήση κωδικών μιας πρόσβασης είτε με την απενεργοποίηση των λογαριασμών μετά το πέρας του διαστήματος αυτού. Τουλάχιστον κάθε τρεις μήνες θα πρέπει να ελέγχεται η υλοποίηση των απαιτούμενων μεταβολών των κωδικών και η απενεργοποίηση των λογαριασμών.
9. Η Εταιρεία οφείλει να εξασφαλίζει ότι η απομακρυσμένη πρόσβαση συνεργατών θα επιτρέπεται μόνο μετά από έγκριση σχετικών αιτημάτων, όπου θα αναγράφεται ο λόγος της πρόσβασης, το σύστημα στο οποίο θα πραγματοποιηθεί η πρόσβαση καθώς και το χρονικό διάστημα που απαιτείται.
10. Ο προσωπικός τεχνικός εξοπλισμός του χρήστη της υπηρεσίας, αποτελεί μια de facto επέκταση του εταιρικού δικτύου, και ως τέτοιος υπόκειται στις Πολιτικές Ασφάλειας της Cosmos Business Systems.
11. Η εταιρεία οφείλει να διατηρεί αρχείο στο οποίο θα καταγράφονται τα στοιχεία χρηστών απομακρυσμένης πρόσβασης (εργαζόμενοι, συνεργάτες) καθώς και τα δικαιώματα πρόσβασης τους. Τουλάχιστον κάθε τρεις μήνες θα πρέπει να ελέγχεται η αντιστοίχιση των λογαριασμών απομακρυσμένης πρόσβασης και των στοιχείων του αρχείου αυτού.
12. Η εταιρεία οφείλει να διατηρεί αρχείο στο οποίο θα καταγράφονται για εργαζόμενους και συνεργάτες τα ΠΕΣ στα οποία επιτρέπεται η απομακρυσμένη πρόσβαση καθώς και οι τεχνικοί τρόποι απομακρυσμένης πρόσβασης.
    Για το συγκεκριμένο αρχείο πρέπει να καταγραφεί και υλοποιηθεί διαδικασία διαχείρισης των λογαριασμών.

7. ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Εισαγωγή

Σύμφωνα με την Ελληνική και Ευρωπαϊκή Νομοθεσία που αφορά τις ηλεκτρονικές επικοινωνίες, η Εταιρεία οφείλει να διαθέτει σαφή Δδιαδικασία Χειρισμού Περαστικών Ασφάλειας, τα οποία απειλούν την ασφάλεια των επικοινωνιακών υποδομών αλλά και τη διασφάλιση του απορρήτου των επικοινωνιών που διεξάγονται μέσω του παρόχου.
Η ύπαρξη μιας επίσημα τεκμηριωμένης και σαφώς κατανοητής διαδικασίας χειρισμού περιστατικών ασφάλειας θα καταστήσει εφικτή τη γρήγορη και αποτελεσματική ανταπόκριση της Εταιρείας σε καταστάσεις που μπορούν να θέσουν σε κίνδυνο τους πληροφοριακούς της πόρους.

Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους χρήστες, διαχειριστές και υπεύθυνους Συστημάτων της Εταιρείας.

Πολιτική
Διαδικασίες & Οδηγίες

- Όλα τα αναφερόμενα περιστατικά ασφάλειας θα αντιμετωπίζονται άμεσα και σύμφωνα με τις διαδικασίες χειρισμού περιστατικών ασφάλειας που ορίζει το τμήμα Ασφάλειας της Εταιρείας.
- Η Εταιρεία οφείλει να δημιουργήσει "Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας" και να καθιερώσει διαδικασίες αντιμετώπισης περιστατικών ασφάλειας πληροφοριών που θα εξετάζουν τα περιστατικά ασφάλειας υπολογιστών, συμπεριλαμβανομένης της κλοπής, της κακής χρήσης των δεδομένων, των εισβολών και του κακόβουλου λογισμικού. Οι διαδικασίες ενδεικτικά θα πρέπει να περιλαμβάνουν τα ακόλουθα:
    1. Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας πρέπει να υλοποιούνται οι παρακάτω ενέργειες:
        - Λεπτομερής καταγραφή κάθε περιστατικού ασφάλειας
            - Ημερομηνία, ώρα εκδήλωσης και περιγραφή του περιστατικού

- Ημερομηνία και ώρα που έγινε αντιληπτό το περιστατικό από την εταιρεία
- Σημείο στο οποίο εκδηλώθηκε το περιστατικό (σύστημα, υπηρεσία, εφαρμογή, πρωτόκολλα, κ.α.)
- Συλλεχθέντα στοιχεία από την εταιρεία για τη διερεύνηση του περιστατικού (αρχεία καταγραφής, στοιχεία παραβίασης, κ.α.)
- Ενημέρωση για την ενδεχόμενη εμφάνιση του περιστατικού περισσότερες φορές
- Ενδεχόμενες συστάσεις σε θιγόμενα άτομα που επηρεάστηκαν από το περιστατικό
- Διερεύνηση των αιτιών και προσδιορισμός τεχνικών ή/και οργανωτικών αδυναμιών στις οποίες ενδεχομένως οφείλεται το περιστατικό ασφάλειας
- Καθορισμός των συνεπειών (αριθμός χρηστών που επηρεάστηκαν, τύπος και όγκος των δεδομένων που επηρεάστηκαν, κ.α) και υλοποίηση ενεργειών αποκατάστασης με συγκεκριμένο χρονοδιάγραμμα
- Ενημέρωση αρμόδιων στελεχών της εταιρείας, καθώς και θιγόμενων χρηστών των παρεχόμενων δικτύων ή υπηρεσιών
- Σύνταξη και διατήρηση σε αρχείο όλων των εγγράφων που σχετίζονται με τα περιστατικά ασφάλειας, από τα οποία θα τεκμηριώνεται και η εκτέλεση των αντίστοιχων προβλεπόμενων ενεργειών

2. Η εταιρεία οφείλει να δώσει υψηλή προτεραιότητα στο χειρισμό κρίσιμων περιστατικών για να παρεμποδιστεί η περαιτέρω ζημιά στους πληροφοριακούς πόρους της Εταιρείας.
3. Η εταιρεία οφείλει να παρέχει στους χρήστες των δικτύων ή υπηρεσιών του την δυνατότητα να καταγγέλλουν μα απλά μέσα την ενδεχόμενη παραβίαση του απορρήτου των επικοινωνιών τους.

8. ΠΟΛΙΤΙΚΗ ΑΝΑΦΟΡΩΝ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ (Security Incident Reporting)

Εισαγωγή

Η διατήρηση της ασφάλειας των πληροφοριακών πόρων της Εταιρείας απαιτεί τη συνεργασία και τη συμμετοχή όλων. Είναι σημαντικό όλοι οι χρήστες πληροφοριών να βρίσκονται σε εγρήγορση σχετικά με την ασφάλεια των πληροφοριών και να αναφέρουν άμεσα οποιαδήποτε πιθανά περιστατικά προκειμένου να ελαχιστοποιηθεί η πιθανή ζημιά στην Εταιρεία.

Η πολιτική και οι διαδικασίες αναφοράς περιστατικών ασφάλειας της Εταιρείας επιτρέπουν στην Εταιρεία:

- γρήγορη και αποτελεσματική ανάκαμψη από τα περιστατικά ασφάλειας,
- απόκριση κατά τρόπο συστηματικό στα περιστατικά και ολοκλήρωση όλων των απαραίτητων βημάτων για το σωστό χειρισμό των περιστατικών,
- αποτροπή ή ελαχιστοποίηση της διάσπασης των κρίσιμων υπηρεσιών,
- και ελαχιστοποίηση της απώλειας ή της κλοπής των ευαίσθητων ή κρίσιμων πληροφοριών.

Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλους τους χρήστες των πληροφοριακών πόρων της Εταιρείας.

Πολιτική
Διαδικασίες & Οδηγίες

a) Όλα τα πιθανά περιστατικά ασφάλειας πρέπει να αναφέρονται άμεσα στο Τμήμα Ασφάλειας.

1) Ενδεικτικά και όχι περιοριστικά, τα περιστατικά περιλαμβάνουν:

- Πιθανές παραβιάσεις οποιασδήποτε πολιτικής ασφάλειας πληροφοριών της Εταιρείας.
- Απώλεια ή κλοπή φορητών υπολογιστών, κινητών συσκευών (όπως PDAs), security tokens ή άλλων στοιχείων που μπορούν να παρέχουν πρόσβαση στους πληροφοριακούς πόρους της Εταιρείας.
- Προσπάθειες από μη-εξουσιοδοτημένο εξωτερικό προσωπικό να αποκτήσει πρόσβαση στις πληροφορίες ή τα συστήματα της Εταιρείας.
- Τυχαία αποκάλυψη, τροποποίηση ή καταστροφή των πληροφοριών.

b) Όλα τα περιστατικά που αναφέρονται θα αντιμετωπίζονται σύμφωνα με τις πολιτικές και τις διαδικασίες Διαχείρισης Περιστατικών Ασφάλειας της Εταιρείας.

Για κάθε περιστατικό πρέπει να συμπληρώνεται και να υποβάλλεται ένα έντυπο αναφοράς περιστατικού της Εταιρείας.

9. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

Εισαγωγή

Οποιαδήποτε σύνδεση με συστήματα ή οργανισμούς εντός ή εκτός της Εταιρείας παρέχει ένα «άνοιγμα» σε μη- εξουσιοδοτημένα άτομα να αποκτήσουν πρόσβαση ή να επέμβουν στους πληροφοριακούς πόρους της Εταιρείας. Το εύρος των απειλών εκτείνεται από τους εισβολείς που παραβιάζουν το δίκτυο της Εταιρείας για να κλέψουν ή να τροποποιήσουν δεδομένα μέχρι τη διάσπαση υπηρεσιών που μπορεί να διαδοθεί από άλλα συστήματα. Για την αποτροπή, ανίχνευση και επίλυση των περιστατικών που προκύπτουν από αυτές τις απειλές, η Εταιρεία πρέπει να εφαρμόζει αντίστοιχα μέτρα προστασίας, όπως λύσεις Συστημάτων Firewall, ανίχνευσης εισβολών (IDS) καθώς και άλλων προφυλάξεων.

Πεδίο εφαρμογής

Η πολιτική αυτή ισχύει για όλο τον ενεργό εξοπλισμό δικτύων της Εταιρείας.

Πολιτική

Διαδικασίες & Οδηγίες

a) Η Εταιρεία καταρτίζει και διατηρεί ενημερωμένο αρχείο, στο οποίο περιγράφεται ο λογικός διαχωρισμός, η αρχιτεκτονική και οι ζώνες ασφαλείας του δικτύου

b) Η διαμόρφωση κάθε συσκευής τεκμηριώνεται λεπτομερώς. Η τεκμηρίωση αυτή ενημερώνεται κάθε φορά που λαμβάνει χώρα οποιαδήποτε αλλαγή.

c) Η απομακρυσμένη διαχείριση των δικτυακών συσκευών γίνεται μόνο με τη χρήση κρυπτογραφημένων συνδέσεων.

d) Ο έλεγχος και η καταγραφή ενεργοποιούνται σύμφωνα με τις πολιτικές και τις διαδικασίες ελέγχου της Εταιρείας.

e) Η πρόσβαση σε όλες τις συσκευές δικτύων της Εταιρείας συμμορφώνεται με τις πολιτικές "Λογική Πρόσβαση" και "Ταυτοποίηση και Αυθεντικοποίηση".

f) Οποιαδήποτε περιττή υπηρεσία τίθεται εκτός λειτουργίας. (π.χ. εάν ένας δρομολογητής δεν διαχειρίζεται με χρήση του SNMP, τότε το SNMP πρέπει να τεθεί εκτός λειτουργίας).

g) Οι συσκευές δικτύων τοποθετούνται σε εγκαταστάσεις με ελεγχόμενη πρόσβαση σύμφωνα με την "Πολιτική Φυσικής Ασφάλειας" της Εταιρείας.

10. ΠΟΛΙΤΙΚΗ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ ΚΑΙ ΑΠΟΘΗΚΕΥΤΙΚΩΝ ΜΕΣΩΝ

Οσοι χρησιμοποιούν φορητούς υπολογιστές εκτός εταιρείας φροντίζουν ώστε :

- Να επιτηρούν συνέχεια τον υπολογιστή τους
- Κρυπτογραφούν είτε να προστατεύουν με ισχυρό password τις διαβαθμισμένες πληροφορίες.

Η αποθήκευση διαβαθμισμένων πληροφοριών σε κινητά μέσα (flash drives, φορητοί δίσκοι, μαγνητικά και οπτικά) αποθηκευσης πρέπει να αποφεύγεται.

Σε περιπτώσεις που απαιτείται μεταφορά πληροφοριών μέσω κινητων μέσων πρέπει να δίνεται προσοχή ώστε να τηρούνται οι απαιτήσεις ασφάλειας.

11. ΠΟΛΙΤΙΚΗ ΑΔΕΙΟΥ ΓΡΑΦΕΙΟΥ (CLEAR DESK)

Για τα γραφεία των μελών των ομάδων που εργάζονται στην σύνταξη προσφορών καθώς και την υλοποίηση διαβαθμισμένων έργων ακολουθείται η πολιτική άδειου γραφείου (Clear Desk).

12. ΠΟΛΙΤΙΚΗ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗΣ ΣΥΝΕΧΕΙΑΣ (BCP)

Ο σκοπός ενός σχεδίου επιχειρηματικής συνέχειας είναι η επαναλειτουργία των κρίσιμων επιχειρησιακών διεργασιών μετά από μία απρογραμμάτιστη και απροσδόκητη διακοπή.

Η ανάπτυξη του σχεδίου επιχειρηματικής συνέχειας λαμβάνει υπόψη τα ακόλουθα.

1. Καθορισμό των λειτουργικών απαιτήσεων κάθε κρίσιμης διεργασίας, των απαιτούμενων ελάχιστων πόρων για την επαναλειτουργία της, της διαθεσιμότητας τηλεπικοινωνιών και κρίσιμων δεδομένων.
2. Μία αποτίμηση και ιεράρχηση των κινδύνων.
3. Την επιλογή ενός οικονομικά βιώσιμου σεναρίου, την υλοποίηση και την συντήρησή του.
4. Την ανάπτυξη και συντήρηση ενός προγράμματος ενημέρωσης και επιμόρφωσης των αποδεκτών του σχεδίου καθώς και των μελών των ομάδων που θα το υποστηρίξουν.

Οι επιχειρηματικές διεργασίας που έχουν ενταχθεί στο σχέδιο είναι εγκεκριμένες από την διοίκηση.

Ο αποδεκτός μέγιστος χρόνος αποκατάστασης της λειτουργίας μίας κρίσιμης διεργασίας μετά από διακοπή είναι εγκεκριμένος από την διοίκηση.