Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών

Κατεύθυνση: Τεχνοοικονομική Διοίκηση

Διπλωματική εργασία

«Διαχείριση επικινδυνότητας σε πληροφοριακά συστήματα»

Παρασκευόπουλος Αλέξανδρος ΜΤΕ 1157

Επιβλέπων: Μ.Θεμιστοκλέους

ΠΕΙΡΑΙΑΣ 2013

Περιεχόμενα

Παρουσίαση πινάκων

Παρουσίαση εικόνων

Παρουσίαση Φύλλων κινδύνου

#	Ορισμοί και ακρωνύμια	Περιγραφή
#1	ΟΠΣ	Ολοκληρωμένο Πληροφοριακό σύστημα
#2	ΠΣ	Πληροφοριακό Σύστημα
#3	ERP	Enterprise Resource Planning
#4	ΛΣ	Λειτουργικό σύστημα
#5	ΒΔ	Βάση Δεδομένων
#6	Μ.Ο.	Μέσος όρος

Πίνακας 1: Ορισμοί και ακρωνύμια

Κεφάλαιο 1

Εισαγωγή

1.1 Περίληψη

Τα πληροφοριακά συστήματα στην σημερινή εποχή δεν είναι απλά για να μας διευκολύνουν στις χρονοβόρες εργασίες και να μας απλοποιούν την καθημερινότητα μας. Έχει γίνει πλέον μια ανάγκη για να μπορέσει μια επιχείρηση να γίνει ανταγωνιστική σε ένα δύσκολο και σκληρό περιβάλλον και το τίμημα πολλές φορές για υιοθέτηση τεχνολογίας που θα της δώσει το πλεονέκτημα στην αγορά δεν είναι μικρό. Το κόστος των πληροφοριακών συστημάτων είναι ανάλογο με τις δυνατότητες του και οι δυνατότητες κάθε συστήματος διευκολύνει την αποτελεσματικότητα μιας επιχείρησης για να μπορέσει να επιβιώσει στην ανταγωνιστικότητα .Με το σκεπτικό αυτό οι επιχειρήσεις ξοδεύουν σημαντικούς πόρους για την εγκατάσταση συστημάτων μεγάλου κόστους ,και το σίγουρο είναι ότι αυτό το κομμάτι θα πρέπει να το θωρακίσουν όσο καλύτερα γίνεται. Η λογική είναι ότι δεν θέλουν να διακινδυνέψουν το μέλλον της επιχείρησης τους αφήνοντας εκτεθειμένο στους διαφόρους κινδύνους το σημαντικότερο εργαλείο που κατέχουν. Με τον παραπάνω πρόλογο προσπαθώ με λίγα λόγια να δείξω πόση μεγάλη αξία δίνει η διαχείριση των κινδύνων για ένα πληροφοριακό σύστημα στις μέρες μας και πώς μπορεί να αποβεί μοιραία η κακή διαχείριση ή η άγνοια διαφόρων κινδύνων του συστήματος . Ένα σύστημα διακατέχεται από διαφόρους κινδύνους και ο κάθε κίνδυνος έχει διαφορετική στρατηγική αντιμετώπισης. Στην συγκεκριμένη διατριβή γίνεται ανάλυση των κινδύνων που διατρέχει ένα πληροφοριακό σύστημα και τρόποι αντιμετώπισης τους.

1.2 Στόχος

Ο στόχος της μελέτης επικινδυνότητας ενός ΠΣ είναι η καταγραφή και αποτίμηση τόσο των κινδύνων που υφίστανται τα πληροφοριακά συστήματα , όσο και οι πιθανές επιπτώσεις που είναι δυνατόν να υποστούν από κακόβουλες ή άστοχες ενέργειες ,ενέργειες που μπορεί να προκληθούν από εσωτερικούς ή εξωτερικούς παράγοντες ή ακόμα και τυχαία .Η επιλογή κατάλληλων τεχνολογιών ,τεχνολογικών και οργανωτικών μέτρων καθώς και ενεργειών κρίνονται απαραίτητα για την ασφάλεια των πληροφοριακών συστημάτων .Έτσι θα πρέπει να γίνει μια αποτίμηση και καταγραφή των κινδύνων που διατρέχει ή μπορεί να διατρέξει στο μέλλον ένα πληροφοριακό σύστημα και οι πιθανές επιπτώσεις που μπορεί να έχει .Με κατάλληλες μελέτες και ειδικότερα με πρόληψη και προνοητικότητα των κινδύνων αυτών , να μπορεί μια επιχείρηση να σταθεί προετοιμασμένη και έτοιμη να αντιμετωπίσει κάθε είδος κινδύνου που μπορεί να βλάψει το πληροφοριακό της σύστημα και εν συνεχεία την ίδια την επιχείρηση.

1.3 Σκοπός

Σκοπός της εκπόνησης της παρούσας εργασίας είναι να διατυπώσουμε προτάσεις και λύσεις για την αποφυγή, αντιμετώπιση και διασφάλιση της απρόσκοπτης λειτουργίας ενός πληροφορικού συστήματος και την μελέτη κινδύνων που διατρέχουν τα πληροφοριακά συστήματα την σημερινή εποχή βάζοντας σε κίνδυνο όχι μόνο το πληροφοριακό σύστημα ενός οργανισμού αλλά και όλη την επιχείρηση στο σύνολό της.

1.4 Δομή

Η παρούσα διατριβή παρουσιάζει την διαχείριση επικινδυνότητας στα πληροφοριακά συστήματα . Στο πρώτο κεφάλαιο παρουσιάζουμε την διπλωματική εργασία με μια μικρή περίληψη, τον στόχο και τον σκοπό της διατριβής. Στο δεύτερο γίνεται μία βιβλιογραφική ανασκόπηση για το τι είναι η διαχείριση της επικινδυνότητας ,ποια βήματα ακολουθούνται για την διαχείριση και ποιες είναι οι κατηγορίες κινδύνων και πώς ταξινομούνται. Στην συνέχεια αναλύονται βασικές έννοιες για το τι είναι ένα πληροφοριακό σύστημα , ποια είναι τα κριτήρια υιοθέτησης του και τι ακριβώς είναι τα ERP συστήματα.

Στο τρίτο κεφάλαιο εξετάζουμε σε βάθος πως θα πρέπει να γίνεται η οργάνωση ασφαλείας ενός πληροφοριακού συστήματος αρχίζοντας με τον ορισμό μιας επιτροπής ασφαλείας που θα είναι υπεύθυνη για τον συντονισμό του έργου .Κάνουμε προσδιορισμό των κινδύνων βάσει των προσβάσεων στο πληροφοριακό σύστημα ,την ταξινόμηση των πόρων και την διαβάθμιση της πληροφορίας. Αναλύεται η ασφάλεια του προσωπικού , τα καθήκοντά τους και η απαιτούμενη εκπαίδευση που είναι απαραίτητη να γίνει για την ασφάλεια του ολοκληρωμένου πληροφοριακού συστήματος .Στην συνέχεια περιγράφεται η αναφορά συμβάντων ,καταγραφή αδυναμιών ασφαλείας σε υλικό και λογισμικό.

Στο τέταρτο κεφάλαιο εξετάζονται τα μέτρα φυσικής πρόσβασης που θα πρέπει να εφαρμοστούν για ένα ασφαλές έργο, την φυσική ασφάλεια της πληροφορίας, την ασφάλεια βάσεων δεδομένων κ.α. Ακόμα περιγράφονται τα μέτρα προστασίας από επιβλαβές λογισμικό και πολιτικές αντιμετώπισης τους και τέλος παραθέτουμε κάποιες οδηγίες και νόμους που περιβάλλουν ένα ολοκληρωμένο πληροφοριακό σύστημα.

Στο πέμπτο κεφάλαιο κάνουμε μια μελέτη περίπτωσης μιας εταιρίας που θέλει να εγκαταστήσει ένα πληροφοριακό σύστημα ERP και κάνουμε διαχείριση της επικινδυνότητας του έργου βάσει πραγματικών στοιχείων. Δημιουργούμε ξεχωριστές πολιτικές αντιμετώπισης και αξιολόγησης κατηγοριοποιώντας τους κινδύνους ανάλογα με την σημαντικότητα και την επίδραση που θα έχουν στο σύστημα.

Στο έκτο κεφάλαιο της διατριβής γίνεται μια πλήρης ανάλυση της παραπάνω μελέτης περίπτωσης και παραθέτονται τα φύλλα κινδύνου.

Κεφάλαιο 2

Βιβλιογραφική Ανασκόπηση

2.1 Τι είναι Κίνδυνος

Κίνδυνος ορίζεται ο συνδυασμός της πιθανότητας ενός γεγονότος σε σχέση με τις συνέπειες που τον διέπουν. Δεν πρέπει να συγχέονται με διάφορα θέματα (ζητήματα) που έχουν συμβεί στο παρελθόν και έχουν αντιμετωπιστεί. Οι κίνδυνοι είναι μόνο μελλοντικά γεγονότα. Οι συνέπειες ενός γεγονότος μπορούν να αποφέρουν όφελος ή απειλές προς την επιτυχία. Η διαχείριση κινδύνου εξετάζει και τις θετικές και τις αρνητικές πλευρές ,όμως στον τομέα τις ασφάλειας η διαχείριση του κινδύνου εξετάζει μόνο τις αρνητικές επιπτώσεις και εστιάζει , αναλύει και μετριάζει τον κίνδυνο.

2.2 Διαχείριση κινδύνου

Η διαχείριση κινδύνου θεωρείται το σημαντικότερο κομμάτι της στρατηγικής διαχείρισης ενός οργανισμού .Είναι μια μεθοδολογική προσέγγιση των κινδύνων που σχετίζονται με τις διάφορες δραστηριότητες που ασχολείται ο κάθε οργανισμός με σκοπό την ελαχιστοποίηση της επικινδυνότητας και κατά συνέπεια την αύξηση του κέρδους .Η σωστή διαχείριση και η έγκαιρη αναγνώριση των κινδύνων κάθε δραστηριότητας αυξάνει την πιθανότητα επιτυχίας των συνολικών στόχων, εφόσον γίνουν και οι σωστοί χειρισμοί . Οι σωστοί χειρισμοί των κινδύνων που μπορεί να προβλεφθούν δεν δίνει την απόλυτη εξασφάλιση ότι ο κίνδυνος έχει αποφευχθεί .Προβλέπει διάφορα μέτρα τα οποία βοηθούν στην ελαχιστοποίηση της πιθανότητας να εμφανιστεί και εάν εμφανιστεί να έχει εξασφαλίσει τις κατάλληλες ενέργειες γρήγορης αντιμετώπισης του. Ο γενικός

κανόνας είναι ότι δεν υπάρχει σχεδόν κανένα έργο που να μην εμπεριέχει κινδύνους και απλά να αναπτύσσεται σε ιδανικό και αρμονικό περιβάλλον. Οι τρείς βασικοί τομείς στην διαχείριση κινδύνων είναι:

1)Αναγνώριση των κινδύνων

2)Ο ποσοτικός προσδιορισμός τους

3)Ο έλεγχος ή μετριασμός των επιπτώσεών τους

Παρακάτω παραθέτουμε σχεδιάγραμμα με τον κύκλο ζωής διαχείρισης των κινδύνων.

εικόνα 1: κύκλος ζωής διαχείρισης κινδύνων

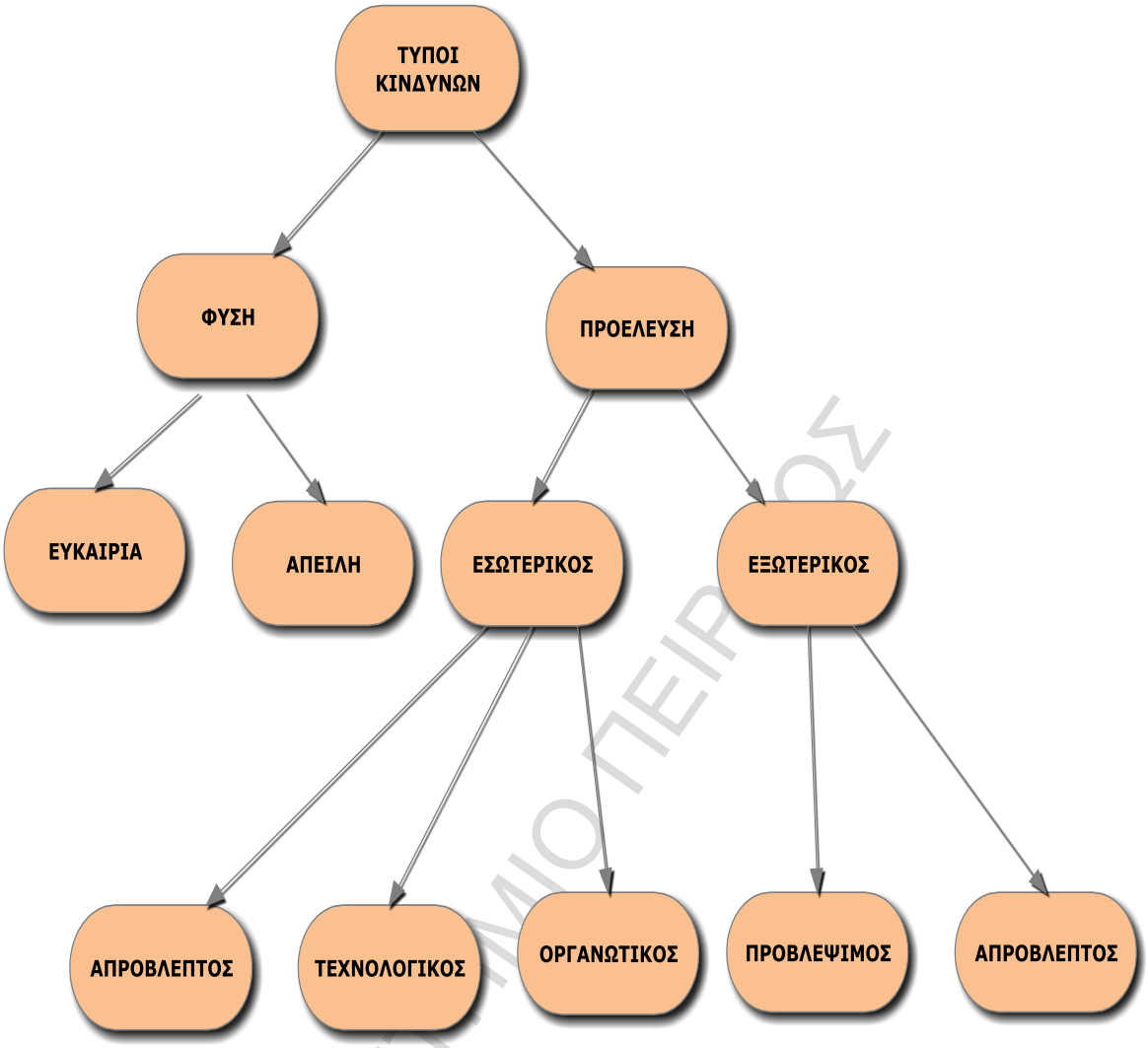
Η αναγνώριση των κινδύνων είναι τα χαρακτηριστικά εκείνα που μας δείχνουν ότι κάτι δεν πάει καλά στο έργο και συνήθως δημιουργείται μία συγκεκριμένη ομάδα ανθρώπων (επιτροπή) για την ανάλυση και τις επιπτώσεις που μπορεί να έχουν . Την επιτροπή αυτή θα την αναλύσουμε παρακάτω στο κομμάτι «οργάνωση ασφάλειας».

Ο ποσοτικός προσδιορισμός των κινδύνων μας δείχνει κατά πόσο ένας κίνδυνος είναι σημαντικός και γίνεται μία διαβάθμιση ανάλογα με την

επικινδυνότητά του (Κρίσιμος , σημαντικός ,δευτερεύουσας σημασίας κ.α).Ακόμη ο ποσοτικός προσδιορισμός μας δίνει μία εκτίμηση της πιθανότητας να συμβεί ένας ενδεχόμενος κίνδυνος.

Ο έλεγχος ή μετριασμός των επιπτώσεων ενός κινδύνου είναι οι διαδικασίες που χρησιμοποιούνται για την μείωση πιθανότητας εμφάνισης και ο μετριασμός των επιπτώσεων που μπορεί να αποφέρει μία εμφάνιση κινδύνου.

Είναι σαφές ότι δεν μπορεί να προβλεφθεί κάθε κίνδυνος που μπορεί να διατρέξει ένα έργο, όμως είναι εφικτό να μπορέσουμε να αναγνωρίσουμε όσους περισσότερους μπορούμε για να γίνει μια αξιολόγηση αυτών. Η διαχείριση κινδύνων είναι μια καλύτερη αποτύπωση της πραγματικότητας και εξασφαλίζει την καλύτερη σχεδίαση ενός έργου, έτσι γίνεται μια εκπόνηση ενός σχεδίου ασφαλείας .Η εκπόνηση ενός σχεδίου ασφαλείας περιλαμβάνει την καταγραφή των υπαρχουσών αδυναμιών και την πρόταση για λήψη μέτρων προστασίας σε επίπεδο διοικητικών μέτρων, μέτρων για την ασφάλεια του υπολογιστικού συστήματος, μέτρων για τη φυσική ασφάλεια, καθώς και οργανωτικών μέτρων και ενεργειών για ανάθεση ρόλων και αρμοδιοτήτων .Η διατύπωση προτάσεων για την παρακολούθηση και διαχείριση της επικινδυνότητας, περιλαμβάνει πλαίσιο ενεργειών για την αντιμετώπιση κινδύνων.



Εικόνα 2: Τύποι κινδύνων

2.2.1 Τεχνικές Αναγνώρισης κινδύνου

- Ανταλλαγή απόψεων και ιδεών
- Ερωτηματολόγια
- Μελέτες που περιγράφουν εσωτερικούς και εξωτερικούς παράγοντες που επηρεάζουν τις διεργασίες
- Ανάλυση σεναρίου κινδύνου
- Έλεγχος και επιθεώρηση
- HAZOP (Hazard & Operability Studies) - Μελέτες Κινδύνου και Λειτουργικότητας[11]

2.2.2 Τεχνικές ανάλυσης της επικινδυνότητας

Για την ανάλυσης της επικινδυνότητας ενός πληροφοριακού συστήματος μπορούν να εφαρμοστούν πολλές τεχνικές ανάλυσης .Η πιο διαδεδομένη μέθοδος είναι η μέθοδος CRAMM.

Η CRAMM δημιουργήθηκε το 1987 από την Κεντρική Υπηρεσία Πληροφορικής και Τηλεπικοινωνιών (CCTA) της κυβέρνησης του Ηνωμένου Βασιλείου. Η μέθοδος αυτή αποτελείται από τρία στάδια .Στα δύο πρώτα στάδια εντοπίζει και να αναλύει τους κινδύνους για το σύστημα και στο τρίτο στάδιο συνιστά για το πώς αυτοί οι κίνδυνοι πρέπει να αντιμετωπιστούν. Τα τρία στάδια της CRAMM έχουν ως εξής:

Στάδιο 1: Ο καθορισμός των στόχων για την ασφάλεια.

Στάδιο 2: Η αξιολόγηση των κινδύνων για το προτεινόμενο σύστημα και τις απαιτήσεις για την ασφάλεια .

Στάδιο 3: Προσδιορισμός και επιλογή των αντισταθμιστικών μέτρων που είναι ανάλογες με τα μέτρα των κινδύνων που υπολογίζεται στο Στάδιο 2. [12]

2.2.3 Οφέλη Ανάλυσης Επικινδυνότητας

Με την διαδικασία της ανάλυσης των κινδύνων, προκύπτουν τα εξής οφέλη:

- Γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος
- Στόχευση της ασφάλειας
- Βελτίωση της κατανόησης του συστήματος

- Κατανόηση της αναγκαιότητας της ασφάλειας και
- Δικαιολόγηση των δαπανών για την ασφάλεια

2.3Η έννοια του Πληροφοριακού Συστήματος

Ένα πληροφοριακό σύστημα ορίζεται ως ένα σύνολο διασυνδεδεμένων υποσυστημάτων που συλλέγουν, επεξεργάζονται, αποθηκεύουν και διανέμουν πληροφορία σχετικά με την επιχείρηση ή το περιβάλλον της για την υποστήριξη της λήψης απόφασης, τον συντονισμό και έλεγχο σε μια επιχείρηση ή οργανισμό. Το πληροφοριακό σύστημα περιέχει εισόδους (δεδομένα, πληροφορίες, εντολές), επεξεργασίες (διαδικασίες, άνθρωποι, εξοπλισμός) και εξόδους (αναφορές, γραφήματα, υπολογισμοί).

Οι γενικές λειτουργίες ενός πληροφοριακού συστήματος είναι οι ακόλουθες:

Συλλογή δεδομένων. Τα δεδομένα συλλέγονται από διάφορες πηγές που μπορεί να είναι εσωτερικές πηγές (δεδομένα σχετικά με τις παραγγελίες),εξωτερικές πηγές (δεδομένα σχετικά με τις παραγγελίες των πελατών) και από το περιβάλλον (δεδομένα που συλλέγονται από εταιρίες δημοσκοπήσεων).

Αποθήκευση δεδομένων. Με την αποθήκευση τα δεδομένα φυλάσσονται με έναν οργανωμένο τρόπο για μελλοντική χρήση.

Επεξεργασία δεδομένων. Περιλαμβάνει υπολογισμούς, συγκρίσεις, ταξινομήσεις και κατηγοριοποιήσεις.

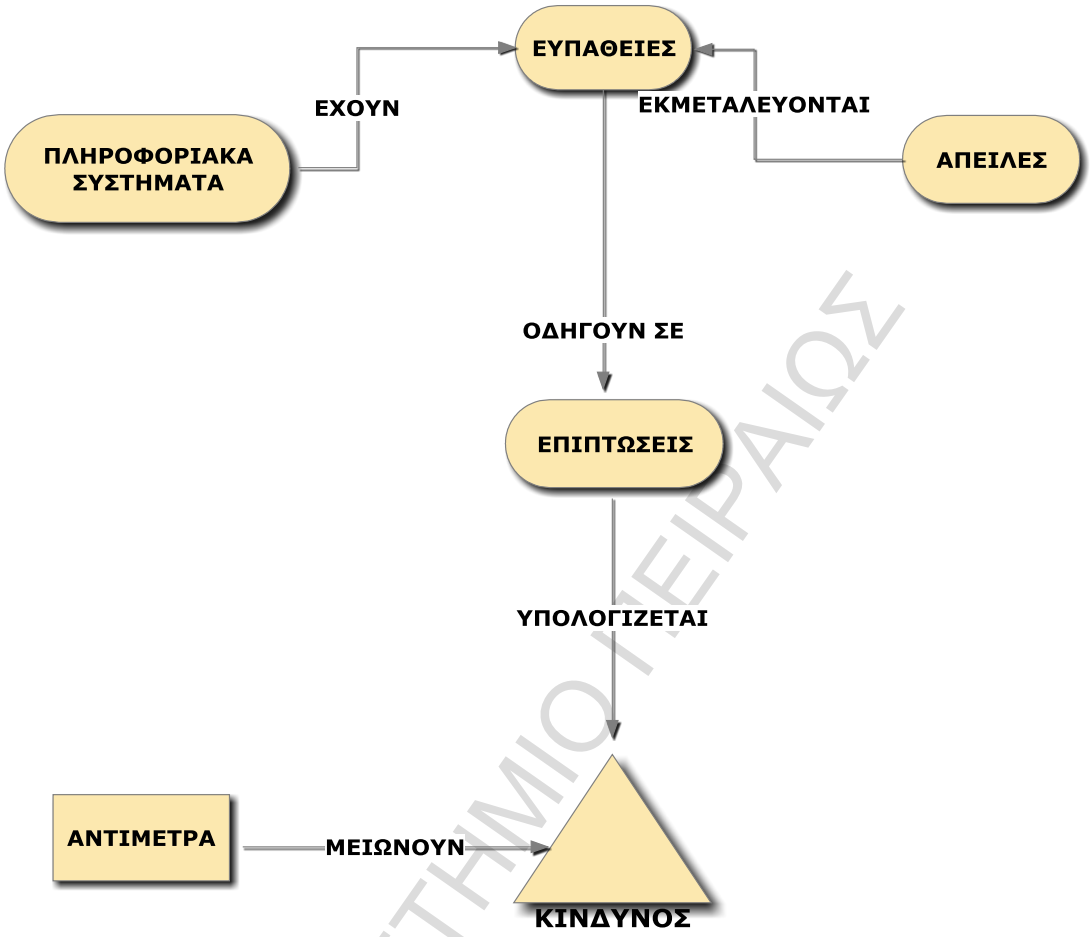
Διάδοση πληροφοριών .Η πληροφορία μπορεί να διαδοθεί σε διάφορες μορφές, όπως αναφορές, λίστες, γραφήματα, μηνύματα, φόρμες.

2.4 Υιοθέτηση Πληροφοριακού Συστήματος

Η υιοθέτηση ενός πληροφοριακού συστήματος και η ένταξη του σε μια επιχείρηση βασίζεται σε μια σειρά από κριτήρια ή παράγοντες. Η επιλογή ενός πληροφοριακού συστήματος βασίζεται σε οικονομικούς παράγοντες, που εμπεριέχουν το κόστος αγοράς, εφαρμογής και υλοποίησης του συστήματος και τη σημασία απόδοσης επένδυσης, στην ευκολότερη αντιμετώπιση του ανταγωνισμού, με άλλα λόγια σημασία δίνεται στο αν το χρησιμοποιούν άλλες επιχειρήσεις στον ίδιο τομέα.

Επίσης υπάρχουν κριτήρια που σχετίζονται με το εσωτερικό της επιχείρησης, δηλαδή εξετάζεται ποια λειτουργία της επιχείρησης θα καλυφθεί, ποιες ανάγκες βραχυπρόθεσμες ή μακροπρόθεσμες θα ικανοποιεί. Λαμβάνονται υπόψη παράγοντες και τίθενται ερωτήματα, όπως αν ταιριάζει με το προφίλ της επιχείρησης, αν θα συμβάλλει στη βελτιστοποίηση και τον αυτοματισμό των διαδικασιών, αν θα διευκολύνει την διεκπεραίωση εργασιών των εργαζομένων, ποια θα είναι η συνεργασία με άλλα τμήματα της επιχείρησης, αν θα έχει δυνατότητα εσωτερικού ελέγχου .Επίσης εξετάζονται τα χαρακτηριστικά του συστήματος, όπως η ταχύτητα εγκατάστασης του, η δυνατότητα αναβάθμισης του, η ασφάλεια εφαρμογής, και η υποστήριξη στη λήψη αποφάσεων .Τέλος, σημαντικό ρόλο επίσης στην επιλογή του συστήματος έχει ο προμηθευτής ,η αξιοπιστία που τον χαρακτηρίζει, η γνώση που έχει στο αντικείμενο, η διάθεση που έχει να εξυπηρετήσει και να δώσει λύσεις στον πελάτη και γενικά το

συνολικό πακέτο που προσφέρει για το σύστημα (υποστήριξη, εκπαίδευση).



Εικόνα 3: Κίνδυνος στα πληροφοριακά συστήματα

2.5 ERP συστήματα (λογισμικά διαχείρισης επιχειρηματικών πόρων)

Ορισμός :

ERP σύστημα είναι το πληροφοριακό σύστημα που ενοποιεί όλες τις διαδικασίες μιας επιχείρησης , ολοκληρώνοντας αποτελεσματικά τις λειτουργικές ανάγκες με σκοπό μια να επιτύχει επιχειρηματικούς

στόχους μέσω της ταχύτατης ,ακριβέστερης και έγκαιρη μετάδοσης της πληροφορίας στο εσωτερικό της.

Τα λογισμικά διαχείρισης επιχειρηματικών πόρων (ERP) στην χώρα μας έχουν μια τεράστια αύξηση τα τελευταία χρόνια .Είναι πλέον μια επιχειρηματική στρατηγική που ακολουθούν όσες εταιρίες θέλουν να μείνουν και να εδραιωθούν στην δύσκολη και ανταγωνιστική αγορά των ημερών μας. Με τα ERP συστήματα κάνουν μια επένδυση για να εξυπηρετηθούν οι στόχοι τους είτε αυτοί αφορούν την εσωτερική της οργάνωση είτε το εξωτερικό της περιβάλλον.

Στόχοι ERP

- Μείωση του συνολικού κόστους της επιχείρησης
- Αύξηση της ποιότητας των υπηρεσιών και των προϊόντων της επιχείρησης.
- Γρηγορότερη και αποτελεσματικότερη εξυπηρέτηση των πελατών.
- Μείωση του χρόνου παραγωγής.
- Αποτελεσματικότερος συντονισμός της ζήτησης, της παραγωγής και της προσφοράς.
- Καλύτερη διαχείριση των αποθηκών και των αποθεμάτων .

Κεφάλαιο 3

Ασφάλεια Πληροφοριακού Συστήματος

3.1 Οργάνωση Ασφάλειας

Η ενότητα οργάνωσης ασφάλειας, περιλαμβάνει το σύνολο των προδιαγραφών για την οργάνωση της ασφάλειας στο ΟΠΣ. Προδιαγράφεται η ίδρυση μιας επιτροπής για τη διαχείριση της ασφάλειας του συστήματος και καθορίζεται το πλαίσιο που θα ενεργεί και τα θέματα με τα οποία θα ασχολείται.

Προδιαγράφεται η κατανομή των ευθυνών στα μέλη της επιτροπής και τονίζεται η σημασία της συνεργασίας όλου του ανθρώπινου δυναμικού του συστήματος, υπό τον συντονισμό της επιτροπής. Προβλέπεται η ανάγκη ύπαρξης εξειδικευμένου προσωπικού σε θέματα ασφάλειας και η συνεργασία της επιτροπής με εξωτερικούς εμπειρογνώμονες, ώστε να διασφαλίζεται η ευθυγράμμιση με σύγχρονα πρότυπα και μεθόδους ασφάλειας, καθώς και με τακτικές αντιμετώπισης περιστατικών εισβολής στο σύστημα.

3.1.1 Επιτροπή Διοικητικής Υποστήριξης Ασφάλειας

Η επιτροπή μπορεί να είναι τμήμα ενός ήδη υπάρχοντος διοικητικού σχήματος. Καθήκοντά της είναι τα εξής:

- Να εξετάζει και να εγκρίνει την πολιτική ασφαλείας και την κατανομή καθηκόντων.
- Να παρακολουθεί σημαντικές αλλαγές του πληροφοριακού συστήματος (που μπορεί να προκαλέσουν την έκθεση πόρων σημαντικές απειλές).

- Να εξετάζει, να παρακολουθεί και να αναλύει περιστατικά σχετιζόμενα με την ασφάλεια του πληροφοριακού συστήματος.
- Να εγκρίνει πρωτοβουλίες που αποσκοπούν στην βελτίωση της ασφάλειας του πληροφοριακού συστήματος.
- Να αποτιμά την επάρκεια και να συντονίσει την υλοποίηση συστημάτων ελέγχου σε νέα συστήματα και υπηρεσίες.

3.1.2 Ομάδα Ασφάλειας

Η ομάδα ασφάλειας πρέπει να αποτελείται από τα ακόλουθα μέλη, τα οποία θα έχουν τα αναφερόμενα καθήκοντα:

- Υπεύθυνος Ασφάλειας:

  Ενδεικτικά καθήκοντα

  - Η εξασφάλιση επαρκούς φυσικής ασφάλειας στο ΟΠΣ, βάσει της πολιτικής ασφάλειας και των προδιαγραφών του.
  - Η εξασφάλιση επαρκούς λογικής ασφάλειας στο ΟΠΣ , βάσει της πολιτικής ασφάλειας και των προδιαγραφών του.
  - Ο συντονισμός της εκπαίδευσης και διαρκούς επαγρύπνησης των χρηστών σε θέματα ασφάλειας.
- Τεχνικός υπεύθυνος ασφάλειας συστημάτων, δικτύων, εφαρμογών και βάσεων δεδομένων:

  Ενδεικτικά καθήκοντα :

  - Η τεχνική υποστήριξη της ασφάλειας των συστημάτων (υλικού και λειτουργικού συστήματος).
  - Η τεχνική υποστήριξη της ασφάλειας των εφαρμογών.
  - Η τεχνική υποστήριξη της ασφάλειας των δικτύων.

- Η τεχνική υποστήριξη της ασφάλειας των βάσεων δεδομένων.

3.2 Πρόσβαση τρίτων οντοτήτων

Σε αυτήν την ενότητα θα περιγράψουμε τα είδη πρόσβασης αιτίες πρόσβασης από τρίτους, τις απαιτήσεις ασφαλείας και τα δικαιώματα που έχουν εξωτερικοί φορείς στο έργο.

3.2.1 Προσδιορισμός κινδύνων από πρόσβαση εξωτερικώνφορέων

Είδη πρόσβασης

Το είδος της πρόσβασης που δίνεται σε εξωτερικούς φορείς είναι ιδιαίτερης σημασίας. Για παράδειγμα, οι κίνδυνοι πρόσβασης μέσω δικτυακής σύνδεσης είναι διαφορετικοί από τους κινδύνους που προέρχονται από φυσική πρόσβαση.

Είδη πρόσβασης που πρέπει να εξεταστούν είναι:

- φυσική πρόσβαση, π.χ. σε γραφεία, αίθουσες υπολογιστών, αρχειοθήκες.
- λογική πρόσβαση, π.χ. στο ΟΠΣ και στις βάσεις δεδομένων του.

Αιτίες Πρόσβασης

Είναι δυνατό να δοθεί πρόσβαση σε εξωτερικούς φορείς για διάφορους λόγους. Για παράδειγμα, υπάρχουν εξωτερικοί φορείς που παρέχουν υπηρεσίες στο Πληροφοριακό σύστημα και που δε βρίσκονται στις εγκαταστάσεις του, αλλά είναι δυνατό να τους δοθεί φυσική ή λογική πρόσβαση, όπως:

- προσωπικό υποστήριξης υλικού και λογισμικού, που χρειάζεται πρόσβαση σε επίπεδο συστήματος ή σε χαμηλό λειτουργικό επίπεδο εφαρμογής
- συνεργαζόμενοι φορείς που ανταλλάσσουν πληροφορίες, προσπελαύνουν το ΟΠΣ ή μοιράζονται βάσεις δεδομένων.

3.2.2 Συμβαλλόμενοι Εντός Του Χώρου

Εξωτερικοί φορείς που εγκαθίστανται εντός του χώρου του ΟΠΣ για κάποια χρονική περίοδο όπως ορίζεται στο συμβόλαιό τους, μπορούν επίσης να αποτελέσουν αιτία για αδυναμίες ασφάλειας. Παραδείγματα εξωτερικών φορέων εντός της τοποθεσίας του ΟΠΣ περιλαμβάνουν:

- προσωπικό συντήρησης εξοπλισμού και λογισμικού
- συνεργεία καθαρισμού, τροφοδοσίας, φύλακες ασφαλείας και άλλες υπηρεσίες ανατεθειμένες σε εξωτερικούς φορείς

3.2.3 Απαιτήσεις ασφάλειας σε συμβόλαια εξωτερικών φορέων

Γενικά όλες οι απαιτήσεις ασφάλειας που πηγάζουν από την πρόσβαση εξωτερικών φορέων θα πρέπει να απεικονίζονται στο συμβόλαιο του εξωτερικού συνεργάτη. Για παράδειγμα, εάν υπάρχει ιδιαίτερη απαίτηση για εμπιστευτικότητα της πληροφορίας, θα μπορούσαν να χρησιμοποιηθούν συμφωνίες που απαγορεύουν την αποκάλυψη πληροφοριών.

Δε θα πρέπει να παρέχεται πρόσβαση στην πληροφορία και στις διαδικασίες επεξεργασίας αυτής σε εξωτερικούς φορείς μέχρι να υλοποιηθούν κατάλληλα μέτρα ασφάλειας και να υπογραφεί συμβόλαιο που καθορίζει τους όρους της σύνδεσης ή της πρόσβασης.

3.2.4 Απαιτήσεις ασφαλείας σε συμβόλαια ανάθεσης έργου σε εξωτερικό φορέα

Ενδεικτικά, το συμβόλαιο πρέπει να περιλαμβάνει:

- πως θα ικανοποιηθούν οι νομικές απαιτήσεις , π.χ. νομοθεσία περί προστασίας προσωπικών δεδομένων
- πώς θα εξασφαλίζονται και θα ελέγχονται η ακεραιότητα και η εμπιστευτικότητα των πόρων του ΟΠΣ
- τι φυσικοί και λογικοί έλεγχοι θα χρησιμοποιηθούν για να περιορίσουν την πρόσβαση σε ευαίσθητη πληροφορία του ΟΠΣ στους εξουσιοδοτημένους χρήστες
- πώς θα διατηρηθεί η διαθεσιμότητα των υπηρεσιών σε περίπτωση καταστροφής

3.3 Ταξινόμηση και Έλεγχος Πόρων

Η ταξινόμηση και ο έλεγχος των πόρων του ΟΠΣ, είναι μια διαδικασία καθοριστικής σημασίας για την ασφάλεια αυτού. Οι κύριοι πόροι του συστήματος, πρέπει να καταγράφονται και να έχουν ορισμένο ένα ιδιοκτήτη, ο οποίος θα είναι και υπεύθυνος για τους πόρους που του αναλογούν.

Προδιαγράφεται η ταξινόμηση των πόρων ανάλογα με τη φύση τους, ώστε να είναι εφικτός ο άμεσος προσδιορισμός της σπουδαιότητάς τους και το επίπεδο ασφάλειας που τους αναλογεί.

3.3.1 Κατάλογος Πόρων

Ένας επίσημος κατάλογος πόρων όλου του εξοπλισμού θα πρέπει να διατηρείται και να ενημερώνεται ανελλιπώς. Θα πρέπει να ορίζεται ιδιοκτήτης για κάθε καταγεγραμμένο πόρο.

Τα ευρετήρια πόρων βοηθούν να εξασφαλισθεί ότι λαμβάνει χώρα αποτελεσματική προστασία πόρων. Η διαδικασία κατάρτισης ενός ευρετηρίου πόρων είναι ένα σημαντικό τμήμα της διαχείρισης κινδύνων. Η Εταιρία πρέπει να είναι σε θέση να προσδιορίζει τους πόρους της και να ορίζει ιδιοκτήτες για τη διαχείριση αυτών. Βασισμένο σε αυτές τις πληροφορίες το ΟΠΣ δύναται τότε να παρέχει βαθμίδες προστασίας ανάλογες με την αξία και τη σπουδαιότητα των πόρων.

Ένα ευρετήριο θα πρέπει να σχεδιάζεται και να συντηρείται από τους σημαντικούς πόρους που σχετίζονται με κάθε πληροφοριακό σύστημα. Κάθε πόρος θα πρέπει να προσδιορίζεται επακριβώς και η ιδιοκτησία του και **διαβάθμιση ασφάλειας** να συμφωνείται και να καταγράφεται, μαζί με την τρέχουσα θέση του (σημαντικό όταν επιχειρείται ανάκτηση από απώλεια ή ζημιά).

3.3.2 Ταξινόμηση Πόρων

Κάθε πόρος πρέπει να ταξινομηθεί σύμφωνα με το βαθμό εμπιστευτικότητας, ευαισθησίας, αξίας και κρισιμότητάς του.

Όταν ο πόρος έχει προσδιοριστεί και ο ιδιοκτήτης οριστεί, το επόμενο βήμα είναι να ταξινομηθεί σύμφωνα με την αξία της για την Εταιρία

που θα εγκαταστήσει το Πληροφοριακό σύστημα . Υπάρχουν ποικίλα πλαίσια για να επιτευχθεί αυτό.

Προσοχή πρέπει να δοθεί στα ακόλουθα:

- Ακατάλληλη Ταξινόμηση ασφάλειας πόρων μπορεί να οδηγήσει σε διαρροή ιδιαίτερα εμπιστευτικής πληροφορίας, με αποτέλεσμα την απώλεια αξιοπιστίας της Εταιρίας .
- Έλλειψη ενός τυποποιημένου συστήματος Ταξινόμησης θα έχει ως αποτέλεσμα την ασυνεπή εφαρμογή αυτής της πολιτικής ασφάλειας.
- Έλλειψη επίγνωσης των τυποποιημένων διαδικασιών Ταξινόμησης του ΠΣ θα έχει ως αποτέλεσμα στην ακατάλληλη Ταξινόμηση της πληροφορίας.

3.3.3 Διαβάθμιση Πληροφορίας

Είναι σημαντικό να ορίζεται ένα κατάλληλο σύνολο διαδικασιών για τη σήμανση και της πληροφορίας σύμφωνα με το σχέδιο Ταξινόμησης που υιοθετείται από το ΟΠΣ, καλύπτοντας τα ακόλουθα είδη επεξεργασίας της πληροφορίας:

- αντιγραφή
- αποθήκευση
- μετάδοση μέσω ταχυδρομείου, φαξ, και ηλεκτρονικού ταχυδρομείου
- μετάδοση μέσω ομιλίας, συμπεριλαμβανομένου κινητού τηλεφώνου, φωνητικού μηνύματος, τηλεφωνητών
- καταστροφή

Τα παραγόμενα από συστήματα που περιέχουν πληροφορία που είναι ευαίσθητη ή κρίσιμη θα πρέπει να φέρουν κατάλληλη σήμανση

ταξινόμησης, που να εκφράζει την ταξινόμηση σύμφωνα με τους κανόνες που έχουν οριστεί.

Η φυσική σήμανση (χρήση ετικετών) είναι γενικά η πιο κατάλληλη μορφή σήμανσης. Ωστόσο, για κάποιους πληροφοριακούς πόρους, όπως έγγραφα σε ηλεκτρονική μορφή, δεν μπορεί να γίνει φυσικός χαρακτηρισμός τους, και χρειάζεται να χρησιμοποιηθούν ηλεκτρονικοί τρόποι σήμανσης.

3.4 Ασφάλεια Προσωπικού

Στόχος της ενότητας ασφάλειας προσωπικού, είναι η μείωση των κινδύνων που προέρχονται από ανθρώπινα λάθη, κλοπή, απάτη και κακή χρήση του συστήματος. Ορίζονται διαδικασίες, όπως η αναλυτική εξέταση του βιογραφικού κάθε εργαζόμενου, ειδικά για ευαίσθητες θέσεις και η υποχρέωση των εργαζομένων να υπογράψουν συμφωνίες διασφάλισης του απόρρητου της πληροφορίας. Τονίζεται ιδιαίτερα η ενσωμάτωση των προδιαγραφών ασφάλειας στις ευθύνες και υποχρεώσεις του ανθρώπινου δυναμικού του συστήματος. Σημαντικό επίσης ρόλο παίζει η εκπαίδευση και συνεχής ενημέρωση του προσωπικού σε θέματα ασφάλειας.

Τέλος, ζωτικής σημασίας για το ΟΠΣ, είναι η ύπαρξη διαδικασιών αναφοράς περιστατικών εισβολής στο σύστημα, ατελειών και κενών ασφάλειας στην υποδομή του και δυσλειτουργιών υλικού και λογισμικού.

3.4.1 Ασφάλεια και καθήκοντα προσωπικού

Περιλαμβάνοντας την ασφάλεια στις υποχρεώσεις του εργαζομένου ,όλοι οι υπάλληλοι πρέπει να συμμορφώνονται με την πολιτική

ασφαλείας του ΟΠΣ. Η επιβολή της συμμόρφωσης είναι ευθύνη της διοίκησης της Εταιρίας ή της ομάδας επίβλεψης ασφαλείας του ΠΣ της Εταιρίας. Η συμμόρφωση με την πολιτική ασφαλείας του οργανισμού είναι υποχρεωτική. Οποιαδήποτε περιστατικό ασφαλείας του πληροφοριακού συστήματος προκύπτει από μη συμμόρφωση με την πολιτική ασφαλείας θα πρέπει να οδηγεί σε λήψη άμεσων πειθαρχικών μέτρων.

Οι ευθύνες των χρηστών σε θέματα ασφάλειας είναι οι ακόλουθες:

- Είναι υπευθυνότητα του καθενός να προστατεύει τα δεδομένα και την πληροφορία που βρίσκεται στα χέρια του.
- Να διακρίνονται όποια δεδομένα είναι ευαίσθητα. Σε περίπτωση άγνοιας ή αμφιβολίας, να γίνονται οι απαραίτητες ερωτήσεις.
- Να γίνεται χρήση των διαθέσιμων πόρων μόνο προς όφελος της εκάστοτε Εταιρίας .
- Να είναι κατανοητό ότι ο καθένας είναι υπεύθυνος για τη δραστηριότητά του στο σύστημα.
- Σε περίπτωση που παρατηρηθεί οτιδήποτε ασυνήθιστο, πρέπει να ενημερώνεται ο άμεσα προϊστάμενος και η ομάδα ασφαλείας του οργανισμού.

Κατά τη χρήση του ΟΠΣ οι χρήστες πρέπει να συμμορφώνονται με τις ακόλουθες συνοπτικές οδηγίες (αναλυτικές οδηγίες συνιστούν το σύνολο της πολιτικής ασφάλειας):

ΕΠΙΒΑΛΛΕΤΑΙ

- Η επιλογή κωδικών που είναι δύσκολο να μαντέψει κανείς.
- Να γίνεται αποσύνδεση πριν την απομάκρυνση του χρήστη από το σταθμό εργασίας του.
- Να προστατεύεται ο εξοπλισμός από κλοπή και να αποφεύγεται η κατανάλωση τροφής και ποτού κοντά σε αυτόν.

- Να εξασφαλίζεται σε κάθε περίπτωση ότι οι δισκέτες και άλλα αποθηκευτικά μέσα που εισέρχονται στους χώρους του οργανισμού ελέγχονται για ιούς από τις υπηρεσίες πληροφορικής πριν από τη χρήση τους.
- Να ενημερώνονται αμέσως οι υπηρεσίες πληροφορικής εάν υπάρχει υποψία ότι κάποιος σταθμός εργασίας έχει προσβληθεί από ιό.

ΑΠΑΓΟΡΕΥΕΤΑΙ

- Η σημείωση των κωδικών σε χαρτί
- Το μοίρασμα ή η αποκάλυψη ενός προσωπικού κωδικού.
- Το να δίδεται σε άλλους η δυνατότητα παρακολούθησης κατά τη διάρκεια εργασίας σε κάτι ευαίσθητο.
- Η χρήση αυθαίρετου λογισμικού.
- Η αντιγραφή λογισμικού.
- Η εγκατάσταση οποιουδήποτε λογισμικού στους σταθμούς εργασίας ή η αλλαγή της παραμετροποίησης τους. Η εργασία αυτή θα πρέπει να γίνεται μόνο από το προσωπικό υπηρεσιών πληροφορικής.

3.4.2 Έλεγχος και Διαχείριση Προσωπικού

Η διοίκηση θα πρέπει να καθορίσει τον βαθμό επίβλεψης του προσωπικού με πρόσβαση σε ευαίσθητα συστήματα. Η εργασία όλου του προσωπικού θα πρέπει να υπόκειται περιοδικά σε διαδικασίες αποτίμησης και εγκρίσεως από ανώτερα στελέχη της Εταιρίας. Γενικά το προσωπικό του συστήματος θα πρέπει να κατέχει το ελάχιστο σύνολο δικαιωμάτων που χρειάζεται.

Όταν η τοποθέτηση σε μια θέση εργασίας, είτε αυτό προκύπτει από διορισμό είτε από προαγωγή, συνεπάγεται πρόσβαση σε εγκαταστάσεις του ΟΠΣ, και ιδιαίτερα εάν αυτή περιλαμβάνει και πρόσβαση σε

εμπιστευτικά δεδομένα, η Εταιρία θα πρέπει επίσης να κάνει έλεγχο αξιοπιστίας του εργαζομένου. Σε εργαζόμενους σε κρίσιμες θέσεις αυτός ο έλεγχος θα πρέπει να επαναλαμβάνεται περιοδικά. Προσοχή επίσης πρέπει να δοθεί στα παρακάτω:

Χειρισμός δυσαρεστημένου προσωπικού: Η διοίκηση θα πρέπει να αποκρίνεται άμεσα, αλλά και διακριτικά σε ενδείξεις δυσαρέσκειας του προσωπικού, συνεργαζόμενη με την αρμόδια διοίκηση προσωπικού και τον υπεύθυνο ασφαλείας του πληροφοριακού συστήματος. Δυσαρεστημένο προσωπικό μπορεί να αποτελέσει σοβαρό κίνδυνο ασφαλείας καθώς ως έμπιστοι υπάλληλοι μπορούν να επιφέρουν σημαντική ζημία στην Εταιρία. Όλα τα μέρη του προσωπικού συνήθως αποκτούν γνώση του ποια είναι τα σημαντικά μέρη του πληροφοριακού συστήματος και ακόμη και αν δεν έχουν απευθείας πρόσβαση σε αυτά μπορούν να αποκτήσουν μέσω των διαπροσωπικών σχέσεων τους με άλλους υπαλλήλους που έχουν τέτοια πρόσβαση. Υπάλληλοι των οποίων έχει αλλάξει η προσωπική τους κατάσταση (π.χ. η οικονομική τους θέση) ή έχουν έντονη δυσαρέσκεια απέναντι στον εργοδότη τους μπορεί να αρχίσουν να δρουν διαφορετικά. Η αλλαγή στην συμπεριφορά τους μπορεί να αποτελέσει προειδοποίηση για ενδεχόμενη παραβίαση (ή απόπειρα παραβίασης) της ασφάλειας του ΟΠΣ.

Χειρισμός παραιτήσεων προσωπικού: Όταν γνωστοποιηθεί η παραίτηση ή μετάθεση μέλους του προσωπικού, η αρμόδια διοίκηση προσωπικού θα πρέπει να εκτιμήσει σε συνεργασία με τον υπεύθυνο ασφαλείας του ΟΠΣ, εάν τα δικαιώματα πρόσβασης του παραιτηθέντος υπαλλήλου στα πληροφοριακά συστήματα της Εταιρίας αποτελούν πρόβλημα ασφαλείας, και αν ναι να αφαιρούνται άμεσα αυτά τα δικαιώματα.

Σεβασμός του ιδιωτικού απορρήτου: Οι υπεύθυνοι της Εταιρίας θα πρέπει να έχουν πρόσβαση στα δεδομένα που βρίσκονται στο

πληροφοριακό σύστημα, λαμβάνοντας υπόψη τις διατάξεις περί σεβασμού του ιδιωτικού απορρήτου στο χώρο εργασίας, Η νομοθεσία έχει λάβει μέριμνα για τον σεβασμό του προσωπικού απορρήτου. Όμως το αν η νομοθεσία έχει εφαρμογή ή όχι στο περιβάλλον εργασίας εξαρτάται από το εάν τα δεδομένα που υπάρχουν στο ΟΠΣ μπορούν να θεωρηθούν σαν προσωπικά. Όταν η επιτήρηση του πληροφοριακού συστήματος γίνεται σε υπερβολικό βαθμό και σε παραβίαση των σχετικών νόμων η Εταιρία μπορεί να υποστεί νομικές κυρώσεις.

3.4.3 Προδιαγραφές Εκπαίδευσης

Οι χρήστες πρέπει να εκπαιδεύονται και να ενημερώνονται, σχετικά με τις διαδικασίες ασφάλειας και στην σωστή χρήση των πόρων του πληροφοριακού συστήματος προκειμένου να ελαχιστοποιηθούν οι πιθανοί κίνδυνοι που απειλούν το ΟΠΣ.

Σκοπός της εκπαίδευσης θα πρέπει αφενός μεν να είναι η ενημέρωση και κατάρτιση των υπαλλήλων των τμημάτων σε θέματα ασφάλειας (γενικά θέματα, εξειδικευμένα θέματα, θέματα Πολιτικής Ασφάλειας) και αφετέρου η εμπέδωση από το προσωπικό της βούλησης της Διοίκησης της Εταιρίας, να υπάρξει διαρκής εκσυγχρονισμός του επιπέδου γνώσεων των υπευθύνων αλλά και αυστηρή τήρηση των κανόνων ασφάλειας που θα αποφασισθούν.

Η μεθοδολογία για την επίτευξη των σκοπών της εκπαίδευσης προτείνεται να είναι η ακόλουθη:

1)Διαχωρισμός της διαδικασίας εκπαίδευσης σε στάδια ξεκινώντας από την εκπαίδευση του Υπεύθυνου Ασφαλείας μέχρι την εκπαίδευση του συνόλου του προσωπικού.

2)Προσωπική εμπλοκή του Υπευθύνου Ασφαλείας στην εκπαίδευση όλων των υπολοίπων ώστε να τονισθεί η διοικητική βούληση για τήρηση των κανόνων ασφαλείας.

3)Σταδιακή εμβάθυνση σε θέματα ασφάλειας.

4)Παροχή των κατάλληλων πόρων από μεριάς του οργανισμού όσον αφορά τόσο σε υλικοτεχνική υποδομή όσο και σε διοικητική υποστήριξη ώστε να αναδειχθεί η έμπρακτη απόφαση του οργανισμού για στήριξη των διαδικασιών ασφαλείας.

5)Περιοδική επανάληψη των εκπαιδεύσεων του προσωπικού ανά τακτά χρονικά διαστήματα ώστε να εμπεδωθούν οι διαδικασίες και οι έννοιες ασφάλειας.

6)Συνεχής κατάρτιση της Ομάδας Ασφάλειας σε θέματα τεχνολογικής αιχμής.

3.5 Αναφορά συμβάντων

Στην ενότητα αναφορά συμβάντων εξετάζουμε την σημαντικότητα των αρχείων καταγραφής συμβάντων , την καταγραφή των αδυναμιών ασφαλείας , δυσλειτουργιών λογισμικού και υλικού μιας εταιρίας.

3.5.1 Καταγραφή Συμβάντων Ασφάλειας

Ένα συμβάν ασφάλειας μπορεί να οριστεί ως οποιοδήποτε περιστατικό που εκθέτει την ασφάλεια του πληροφοριακού συστήματος ή που από μόνο του δεν εκθέτει απαραίτητα την ασφάλεια, αλλά που θα μπορούσε να αποτελέσει αιτία έκθεσής της. Ένα παράδειγμα είναι μια επανειλημμένη αποτυχία απόπειρας

Το συμβάν μπορεί να είναι φυσικό (π.χ. μια διάρρηξη και επακόλουθη κλοπή) ή διαδικαστικό (π.χ. μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή, με αποτέλεσμα την απώλεια δεδομένων, ή κάποιος λάθος

χειρισμός του συστήματος από το προσωπικό), με αποτέλεσμα τη ζημιά ή απώλεια δεδομένων του συστήματος.

Τα συμβάντα ασφάλειας θα πρέπει να αναφέρονται μέσω κατάλληλων διοικητικών διαύλων το συντομότερο δυνατό. Όλοι οι εργαζόμενοι και συμβαλλόμενοι θα πρέπει να είναι ενήμεροι για τη διαδικασία αναφοράς συμβάντων ασφαλείας, και θα πρέπει να αναφέρουν τέτοια συμβάντα το συντομότερο δυνατό. Αυτοί οι οποίοι αναφέρουν συμβάντα ενημερώνονται για τα αποτελέσματα αφού το συμβάν αντιμετωπιστεί και τερματιστεί. Τα συμβάντα αυτά μπορούν να χρησιμοποιηθούν στην ενημερωτική εκπαίδευση των χρηστών ως παραδείγματα του τι μπορεί να συμβεί, πώς μπορούν να αντιμετωπιστούν τέτοια συμβάντα και πώς να αποφεύγονται στο μέλλον.

Αποδεικτικά σχετικά με υποψιασμένη παραβίαση πληροφοριακής ασφάλειας πρέπει να καταγράφονται επί τόπου και να επεξεργάζονται. Η πρακτική της καταγραφής όλων των πτυχών των παραβιάσεων πληροφοριακής ασφάλειας βοηθά την Εταιρία να αναπτύξει αποτρεπτικά μέτρα που περιορίζουν την πιθανότητα επανάληψής τους.

3.5.2 Καταγραφή Αδυναμιών Ασφάλειας

Χρήστες υπηρεσιών πληροφορίας θα πρέπει να σημειώνουν και να αναφέρουν όποιες αδυναμίες ασφάλειας ή απειλές για συστήματα ή υπηρεσίες που παρατηρούν ή υποψιάζονται, Θα πρέπει να αναφέρουν αυτά τα ζητήματα στον Υπεύθυνο Ασφάλειας το δυνατόν συντομότερα. Οι χρήστες θα πρέπει να ενημερώνονται ότι δεν πρέπει, υπό οποιεσδήποτε συνθήκες, να επιχειρούν να αποδεικνύουν μια υποπτευόμενη αδυναμία. Αυτό ισχύει για δική τους προστασία, αφού οι δοκιμές αδυναμιών μπορεί να ερμηνευθούν ως πιθανή παράνομη χρήση του συστήματος.

3.5.3 Καταγραφή Δυσλειτουργιών Λογισμικού

Οι ακόλουθες δραστηριότητες πρέπει να συντελούνται:

1)Τα συμπτώματα του προβλήματος και όποια μηνύματα εμφανίζονται στην οθόνη θα πρέπει να σημειώνονται σαν σχόλια.

2)Ο υπολογιστής θα πρέπει να απομονώνεται, εάν είναι δυνατό, και η χρήση του να διακόπτεται. Οι δισκέτες δε θα πρέπει να μεταφέρονται σε άλλους υπολογιστές.

3)Το ζήτημα πρέπει να αναφέρεται αμέσως στον Υπεύθυνο Ασφάλειας.

3.5.4 Καταγραφή Δυσλειτουργιών Υλικού

Οι ακόλουθες δραστηριότητες πρέπει να συντελούνται:

1)Τα συμπτώματα του προβλήματος θα πρέπει να σημειώνονται σαν σχόλια.

2)Το υλικό θα πρέπει να απομονώνεται, εάν είναι δυνατό, και η χρήση του να διακόπτεται. Εάν πρέπει να ελεγχθεί εξοπλισμός, θα πρέπει να αποσυνδέεται από το δίκτυο του συστήματος προτού επανενεργοποιηθεί. Οι δισκέτες δε θα πρέπει να μεταφέρονται σε άλλους υπολογιστές.

3)Το ζήτημα πρέπει να αναφέρεται αμέσως στον Υπεύθυνο Ασφάλειας.

Κεφάλαιο 4

Φυσική ασφάλεια και ασφάλεια περιβάλλοντος εργασίας

Στόχος του κεφαλαίου φυσικής ασφάλειας είναι η αποφυγή μη εξουσιοδοτημένης πρόσβασης σε χώρους του ολοκληρωμένου πληροφοριακού συστήματος και η προστασία από καταστροφές που θα παρεμποδίσουν την ομαλή λειτουργία αυτού. Προβλέπονται συστήματα ασφάλειας για προστασία από πυρκαγιές, πλημμύρες και άλλες φυσικές καταστροφές και τονίζεται ιδιαίτερα ο σαφής ορισμός μιας ασφαλούς περιμέτρου γύρω από το πληροφοριακό σύστημα.

Όσο αφορά στην πρόσβαση στους χώρους του συστήματος, προβλέπονται διαδικασίες για προσωπικό και επισκέπτες σε συνδυασμό με εγκατάσταση συστημάτων ελέγχου φυσικής πρόσβασης. Ιδιαίτερη σημασία δίνεται στην προστασία χώρων που φυλάσσονται συστήματα που διαχειρίζονται ευαίσθητη πληροφορία.

Άλλες συστάσεις, αφορούν στην συντήρηση του εξοπλισμού και την προστασία του από κλοπή, εκρήξεις, καπνό, σκόνη, δονήσεις, χημικά, ακτινοβολία κλπ., τη διασφάλιση παροχής ηλεκτρικής ενέργειας και την προστασία της καλωδίωσης.

4.1 Περίμετρος Φυσικής Ασφάλειας

Η φυσική ασφάλεια μπορεί να επιτευχθεί τοποθετώντας φυσικούς φραγμούς γύρω από τους χώρους των εγκαταστάσεων του ΟΠΣ. Κάθε τέτοιος φυσικός φραγμός αποτελεί τμήμα μίας φυσικής περιμέτρου, η οποία αυξάνει το παρεχόμενο επίπεδο ασφαλείας. Οι εγκαταστάσεις του πληροφοριακού συστήματος θα πρέπει να βρίσκονται εντός μίας τέτοιας περιμέτρου ασφαλείας.

Η περίμετρος ασφαλείας αποτελείται από σύνολο φυσικών φραγμών όπως τοίχους, εισόδους με συσκευές ελέγχου κάρτας ή με ύπαρξη προσωπικού φύλαξης κ.τ.λ. Η τοποθέτηση και ο βαθμός ασφαλείας κάθε τέτοιας περιμέτρου θα εξαρτάται από τα αποτελέσματα της αποτίμησης κινδύνου. Οι ακόλουθες οδηγίες θα πρέπει να λαμβάνονται υπ' όψιν και να εφαρμόζονται:

- Η περίμετρος ασφαλείας θα πρέπει να είναι ορισμένη με ακρίβεια.
- Η περίμετρος κτιρίου ή χώρων που περιέχουν στοιχεία του πληροφοριακού συστήματος θα πρέπει να είναι επαρκής από φυσικής απόψεως (δηλ. δεν θα πρέπει να υπάρχουν κενά και σημεία όπου να είναι εφικτή η είσοδος).
- Οι επισκέπτες του χώρου του συστήματος θα πρέπει να καταγράφονται και να συνοδεύονται.
- Ύπαρξη προσωπικού ελέγχου στην είσοδο ή άλλα μέτρα ελέγχου της φυσικής πρόσβασης στις εγκαταστάσεις του ΟΠΣ θα πρέπει να έχουν υλοποιηθεί. Η είσοδος στις εγκαταστάσεις θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.
- Το κτίριο θα πρέπει να έχει κατασκευαστεί με τέτοιο τρόπο που να αντέχει σε σεισμούς αυξημένης εντάσεως.
- Φυσική ασφάλεια θα πρέπει εφαρμοστεί στα modem και το hardware, που χρησιμοποιείται για την υπηρεσία απομακρυσμένης πρόσβασης, για την προστασία τους από μη εξουσιοδοτημένη χρήση.

4.1.1 Μέτρα ελέγχου φυσικής πρόσβασης

Οι ασφαλείς περιοχές θα πρέπει να προστατεύονται από κατάλληλους μηχανισμούς ελέγχου εισόδου που θα εξασφαλίζουν ότι μόνο

εξουσιοδοτημένο προσωπικό θα έχει πρόσβαση στις εγκαταστάσεις του πληροφοριακού συστήματος. Τα ακόλουθα μέτρα θα ληφθούν υπόψη:

- Θα πρέπει να υπάρχει φύλαξη των χώρων σε 24ώρη βάση.
- Οι επισκέπτες στις ασφαλείς περιοχές να είναι υπό επίβλεψη και οι χρόνοι εισόδου και εξόδου να καταγράφονται.
- Η πρόσβαση σε κρίσιμες πληροφορίες και εγκαταστάσεις του πληροφοριακού συστήματος να ελέγχεται, και να δίδεται μόνο στο εξουσιοδοτημένο προσωπικό.
- Όλα τα μέλη του προσωπικού θα πρέπει να φέρουν εμφανή στοιχεία αναγνωρίσεως (π.χ. κάρτα) και θα πρέπει να ενθαρρύνονται να ελέγχουν αγνώστους ή άτομα που δεν φέρουν τα εμφανή σημάδια αναγνωρίσεως.
- Τα δικαιώματα πρόσβασης στις ασφαλείς περιοχές θα πρέπει να αναθεωρούνται περιοδικά και να ανανεώνονται.

Τα δικαιώματα φυσικής πρόσβασης κάθε μέλους του προσωπικού στις ασφαλείς περιοχές θα πρέπει να είναι καταγεγραμμένα

4.1.2 Ασφαλίζοντας γραφεία, δωμάτια και εγκαταστάσεις

Μία ασφαλής περιοχή μπορεί να είναι ένα κλειδωμένο γραφείο ή ένας αριθμός δωματίων εντός μίας περιμέτρου φυσικής ασφαλείας, που μπορεί να έχουν ασφαλείς κλειδαριές ή να περιέχουν χρηματοκιβώτια. Η εκλογή και ο σχεδιασμός των ασφαλών περιοχών θα πρέπει να λαμβάνει υπ’ όψιν του την πιθανότητα βλαβών από φωτιά, πλημμύρα. έκρηξη, επεισόδια και άλλες μορφές φυσικής ή ανθρώπινης προελεύσεως καταστροφής. Επίσης πρέπει να ληφθεί μέριμνα για τήρηση των υπαρχόντων κανονισμών και προτύπων υγιεινής και ασφαλείας, ενώ πρέπει να εξεταστούν και πιθανές συνέπειες της

γειτνίασης με άλλες εγκαταστάσεις, π.χ. τι θα συμβεί σε περίπτωση διαρροής υδάτων σε μία εξ' αυτών.

Τα ακόλουθα μέτρα θα πρέπει να εξεταστούν:

- Σημαντικές εγκαταστάσεις θα πρέπει να είναι έτσι διαμορφωμένες ώστε να αποφεύγεται η πρόσβαση τρίτων.
- Εγκατάσταση συστήματος πρόσβασης μέσω κάρτας ή άλλου παρόμοιου τρόπου ισχυρής αυθεντικοποίησης.
- Υποστηρικτικές διαδικασίες και εξοπλισμός, π.χ. φωτοτυπικά και fax, θα πρέπει να διεξάγονται / βρίσκονται εντός ασφαλούς περιοχής ώστε να μην υπάρξει διαρροή πληροφοριών.
- Οι πόρτες και τα παράθυρα θα πρέπει να είναι ασφαλισμένα όταν δεν είναι υπό επίβλεψη και θα πρέπει να υπάρχει εξωτερική προστασία για τα παράθυρα, ιδιαίτερα αυτά που βρίσκονται σε χαμηλό επίπεδο.
- Κατάλληλα συστήματα εντοπισμού εισβολέων θα πρέπει να είναι εγκατεστημένα, με βάση επαγγελματικά πρότυπα και να ελέγχονται περιοδικά, συστήματα τα οποία θα προστατεύουν όλα τα εξωτερικώς προσβάσιμα σημεία εισόδου όπως πόρτες και παράθυρα.
- Επικίνδυνα και εύφλεκτα υλικά θα πρέπει να αποθηκεύονται με ασφάλεια σε επαρκή απόσταση από μία ασφαλή περιοχή.
- Εφεδρικός εξοπλισμός και εφεδρικά δεδομένα του συστήματος θα πρέπει να αποθηκεύονται σε ασφαλή απόσταση ώστε να μην καταστραφούν μαζί με τον κύριο εξοπλισμό σε έκτακτο περιστατικό.
- Τα διάφορα έγγραφα θα πρέπει να αποθηκεύονται με ασφαλή τρόπο ανάλογα το επίπεδο ταξινόμησής τους.

- Η χρήση ασφαλών από φωτιά αποθηκευτικών χώρων θα πρέπει να εξεταστεί προκειμένου να προστατευτούν δεδομένα από πυρκαγιά αλλά και από νερό που θα χρησιμοποιηθεί για την κατάσβεσή της.
- Όταν τοποθετούνται οι υπολογιστές και το λοιπό υλικό του ΟΠΣ πρέπει να ληφθούν προφυλάξεις προκειμένου να αποφευχθούν καταστροφές από υπερβολική θερμοκρασία.

4.1.3 Τοποθέτηση και προστασία του εξοπλισμού

Στον τομέα της πληροφοριακής ασφάλειας, ο όρος «εγκαταστάσεις» αναφέρεται σε οποιαδήποτε περιοχή στην οποία έχει τοποθετηθεί υπολογιστικό υλικό. Μπορεί να είναι από μια γωνία κάποιου γραφείου, μέχρι ένα ολόκληρο κτίριο. Είναι σημαντικό να μελετάται προσεκτικά η επιλογή της τοποθεσίας εγκατάστασης του υπολογιστικού υλικού διότι είναι δύσκολο να γίνουν αλλαγές αφού η τοποθεσία έχει οριστεί. Το μέγεθος της περιοχής καθορίζεται από τον όγκο υπολογιστικού υλικού που θα στεγαστεί. Οι περιβαλλοντολογικές ανάγκες για την επιλεγμένη περιοχή πρέπει να προσδιορίζονται από τον κατασκευαστή του υπολογιστικού υλικού, την ευαισθησία των δεδομένων, και το επιθυμητό επίπεδο ανθεκτικότητας της υπηρεσίας.

Ο εξοπλισμός θα πρέπει να έχει τοποθετηθεί ώστε να ελαχιστοποιηθούν οι περιβαλλοντικοί κίνδυνοι και οι δυνατότητες μη εξουσιοδοτημένης πρόσβασης .Μέτρα θα πρέπει να ληφθούν ώστε να ελαχιστοποιηθεί ο κίνδυνος από :

- Κλοπή
- Φωτιά
- Εκρηκτικά
- Καπνό

- Νερό (ή αδυναμία παροχής του)
- Σκόνη
- Δονήσεις
- Χημικούς παράγοντες
- Ηλεκτρικού ρεύματος
- Ηλεκτρομαγνητικής ακτινοβολίας
- Η Εταιρία θα πρέπει να εξετάσει αν θα επιτρέπει στους υπαλλήλους να τρώνε, να πίνουν και να καπνίζουν στους χώρους του ΟΠΣ. Γενικά συνίσταται η απαγόρευση των παραπάνω.
- Οι συνθήκες του περιβάλλοντος θα πρέπει να εξετάζονται καθώς μπορεί να επηρεάσουν την λειτουργία του ΟΠΣ.
- Κάθε μετακίνηση υλικού στις εγκαταστάσεις της Εταιρίας θα πρέπει να γίνεται από εξουσιοδοτημένο προσωπικό.
- Το σύνολο του υπολογιστικού εξοπλισμού και άλλο σχετικό υλικό που ανήκει στην Εταιρία πρέπει να εντάσσεται υπό κατάλληλη ασφαλιστική κάλυψη ενάντια κλοπής, ζημιάς ή απώλειάς του.
- Όλες οι εργασίες συντήρησης πρέπει να έχουν εγκριθεί και να ελέγχονται.

4.1.4 Φυσική Ασφάλεια Πληροφορίας

Όπου κρίνεται απαραίτητο, το έντυπο υλικό και τα υπολογιστικά μέσα θα πρέπει να αποθηκεύονται σε κατάλληλα κλειδωμένο θάλαμο και/ ή άλλες μορφές εξοπλισμού όταν αυτός δεν χρησιμοποιείται, ειδικά εκτός του ωραρίου εργασίας και ποτέ δεν πρέπει να τοποθετούνται απροστάτευτα (πχ στα γραφεία των υπαλλήλων). Ένα ακόμη σημαντικό στοιχείο είναι ότι οι εκτυπώσεις ευαίσθητης πληροφορίας θα

πρέπει να γίνεται μόνο σε συγκεκριμένους εκτυπωτές και όλοι οι χρήστες των σταθμών εργασίας να παύουν ενεργές συνδέσεις με τους κεντρικούς εξυπηρετητές όταν έχουν τελειώσει.

4.2 Ασφάλεια συστημάτων και εφαρμογών

Στόχος της παρούσας διαδικασίας είναι να εγκαθιδρύσει πρότυπα για την βασική παραμετροποίηση ολόκληρου του εξοπλισμού των εξυπηρετητών (server) που ανήκει ή/ και χρησιμοποιείται στην εκάστοτε εταιρία που θέλει να εγκαταστήσει έναολοκληρωμένο πληροφοριακό σύστημα . Αποτελεσματική εφαρμογή αυτής της πολιτικής θα ελαχιστοποιήσει την μη-εξουσιοδοτημένη πρόσβαση στην πληροφορία και τεχνολογία.

Όλοι οι εξυπηρετητές που αναπτύσσονται στην Εταιρία θα πρέπει να βρίσκονται υπό την κατοχή μία ομάδας υπεύθυνης για την διαχείριση του συστήματος υπό την εποπτεία του Τεχνικού Υπεύθυνου Ασφάλειας Συστημάτων. Οι εγκεκριμένες οδηγίες για την παραμετροποίηση των εξυπηρετητών πρέπει να εγκαθιδρυθούν και να συντηρούνται από τις υπεύθυνες ομάδες διαχείρισης, βασισμένες στις ανάγκες της εταιρίας. Οι ομάδες διαχείρισης πρέπει να παρακολουθούν την συμβατότητα με τις παραμετροποιήσεις και να εφαρμόσουν μία ξεχωριστή πολιτική προσαρμοσμένης στο περιβάλλον τους.

Αλλαγές παραμετροποίησης πρέπει να ακολουθούν τις απαραίτητες διαδικασίες για την διαχείριση των αλλαγών.

Η παραμετροποίηση του κεντρικού εξυπηρετητή πρέπει να περιλαμβάνει τα ακόλουθα:

- Υπηρεσίες και εφαρμογές οι οποίες δεν θα χρησιμοποιηθούν πρέπει να απενεργοποιούνται.
- Πρόσβαση σε υπηρεσίες πρέπει να καταχωρείται και/ ή να προστατεύεται μέσω μεθόδων ελέγχου πρόσβασης, όταν είναι δυνατόν.
- Τα πιο πρόσφατα patches θα πρέπει να εγκατασταθούν στο σύστημα το συντομότερο δυνατό, η μόνη εξαίρεση γίνεται στην περίπτωση που άμεση εφαρμογή έρχεται σε αντιπαράθεση με τις απαιτήσεις της Εταιρίας.
- Οι εξυπηρετητές πρέπει να είναι εγκατεστημένοι σε ένα περιβάλλον ελεγχόμενης πρόσβασης.
- Η τήρηση αρχείων καταγραφής πρέπει να ακολουθεί τις ορισμένες πολιτικές.

4.2.1 Αρχεία Συστήματος

Όλα τα αρχεία συστήματος και εφαρμογών που ορίζουν και κατευθύνουν τη λειτουργία του πρέπει να προστατεύονται επαρκώς και να περιορίζεται στα άτομα που είναι εξουσιοδοτημένα να εφαρμόζουν λειτουργίες διαχείρισης σε συστήματα.

4.2.2 Προστασία των εργαλείων καταγραφής και ελέγχου

Πρόσβαση στα εργαλεία καταγραφής, π.χ. λογισμικό και αρχεία δεδομένων, θα πρέπει να αποτρέπεται προκειμένου να αποφευχθεί παραβίαση ή κακόβουλη χρήση του μηχανισμού ασφαλείας. Αυτά τα εργαλεία θα πρέπει να διαχωρίζονται από τα τμήματα ανάπτυξης και τα λειτουργικά τμήματα του πληροφοριακού συστήματος, και να μην

βρίσκονται σε σημεία προσβάσιμα από τους χρήστες εκτός και αν τους δίδεται επιπρόσθετη προστασία.

4.2.3 Έλεγχος λογισμικού εν λειτουργία

Θα πρέπει να παρέχεται έλεγχος για την υλοποίηση του λογισμικού σε εν λειτουργία συστήματα. Για την ελαχιστοποίηση του κινδύνου αλλοίωσης των εν λειτουργία συστημάτων, θα πρέπει να μελετηθούν τα ακόλουθα μέτρα ασφάλειας:

- Η ενημέρωση των βιβλιοθηκών του εν λειτουργία προγράμματος θα πρέπει να διενεργείται μόνο μετά από κατάλληλη διοικητική εξουσιοδότηση.
  - Θα πρέπει να τηρείται μια λίστα αλλαγών όλων των ενημερώσεων στις βιβλιοθήκες των εν λειτουργία προγραμμάτων.
  - Προηγούμενες εκδόσεις λογισμικού θα πρέπει να φυλάσσονται ως μέτρο αντιμετώπισης απροόπτων.

Το λογισμικό που χρησιμοποιείται σε εν λειτουργία συστήματα θα πρέπει να διατηρείται σε επίπεδο που υποστηρίζεται από τον φορέα παροχής. Για οποιαδήποτε απόφαση για αναβάθμιση σε νέα έκδοση θα πρέπει να λαμβάνεται υπόψη η ασφάλεια της έκδοσης. Θα πρέπει να εφαρμόζονται διορθωτικά προγράμματα λογισμικού όταν μπορούν να βοηθήσουν στην εξαφάνιση ή στη μείωση των αδυναμιών ασφάλειας.

Φυσική ή λογική πρόσβαση θα πρέπει να δίνεται μόνο σε πάροχους για σκοπούς υποστήριξης όταν υπάρχει ανάγκη και με την έγκριση της διοίκησης. Οι δραστηριότητες του παρόχου θα πρέπει να παρακολουθούνται.

4.3 Ασφάλεια δεδομένων συστήματος

Στην ενότητα αυτή παραθέτονται πληροφορίες για τον έλεγχο των δεδομένων του συστήματος, την πιστοποίηση των μηνυμάτων μέσα

στο πληροφοριακό σύστημα , την ασφάλεια των βάσεων δεδομένων που αποθηκεύεται η πληροφορία και την καταγραφή των συμβάντων συγκεκριμένα για το πληροφοριακό σύστημα που θα εξετάσουμε.

4.3.1 Έλεγχος αξιοπιστίας εισαγομένων δεδομένων

Τα εισαγόμενα δεδομένα σε συστήματα εφαρμογών θα πρέπει να ελέγχονται για την αξιοπιστία τους και την ορθότητα και την καταλληλότητά τους. Θα πρέπει να εφαρμόζονται έλεγχοι στην εισαγωγή δεδομένων. Τα ακόλουθα μέτρα ασφάλειας θα πρέπει να ληφθούν υπόψη:

- ελλιπή ή ατελή δεδομένα
- υπέρβαση του ανώτατου και του κατώτατου ορίου του όγκου δεδομένων
- μη εξουσιοδοτημένα ή ασύμβατα δεδομένα ελέγχου
- περιοδική αναθεώρηση του περιεχομένου των πεδίων κλειδιών ή των αρχείων δεδομένων ώστε να επαληθεύεται η εγκυρότητα και η ακεραιότητά τους
- αντιμετώπιση σφαλμάτων ελέγχου εγκυρότητας

4.3.2 Πιστοποίηση μηνυμάτων

Η πιστοποίηση μηνυμάτων είναι μια τεχνική που χρησιμοποιείται για την ανίχνευση μη εξουσιοδοτημένων αλλαγών ή αλλοίωσης των περιεχομένων ενός μεταδιδόμενου ηλεκτρονικού μηνύματος. Μπορεί να υλοποιηθεί σε υλικό ή λογισμικό που υποστηρίζει μια συσκευή φυσικής πιστοποίησης μηνυμάτων ή αλγόριθμο λογισμικού.

Η πιστοποίηση μηνυμάτων θα πρέπει να μελετηθεί για εφαρμογές όπου υπάρχει απαίτηση ασφάλειας για προστασία της ακεραιότητας του περιεχομένου του μηνύματος, Θα πρέπει να διενεργείται αξιολόγηση των κινδύνων για την ασφάλεια ώστε να προσδιορίζεται

εάν χρειάζεται η πιστοποίηση μηνυμάτων και να καθορίζεται η πλέον κατάλληλη μέθοδος υλοποίησης.

Θα πρέπει να χρησιμοποιηθούν κρυπτογραφικές τεχνικές ως το κατάλληλο μέσο υλοποίησης της πιστοποίησης μηνυμάτων.

4.3.3 Ασφάλεια Βάσεων Δεδομένων.

Περιλαμβάνει όλα τα μέτρα για την ενεργοποίηση των μηχανισμών ασφαλείας που προσφέρει ένα σύστημα διαχείρισης βάσεων δεδομένων. Αναλύονται οι μηχανισμοί που είναι παρόντες στην έκδοση του λογισμικού βάσεων δεδομένων που χρησιμοποιείται και που διαφοροποιούνται ανάλογα το πληροφοριακό σύστημα που χρησιμοποιεί η κάθε εταιρία ή οργανισμός .Στο δικό μας παράδειγμα που θα παραθέσουμε στην συνέχεια υπάρχει η oracle 10g Enterprise Edition(περιγράφεται η διαδικασία για την διαχείριση χρηστών ενώ δίνονται και κατευθυντήριες γραμμές για την διαχείριση των συνθηματικών των χρηστών πάνω στη βάση.)

4.3.4 Καταγραφή Συμβάντων

Δύο επίπεδα καταγραφής προτείνεται να υλοποιηθούν στο Πληροφοριακό Σύστημα της Εταιρίας που εξετάζουμε στην δική μας έρευνα. Το ένα αναφέρεται σε καταγραφή στο επίπεδο λειτουργικού συστήματος ή/και βάσης δεδομένων και το δεύτερο αναφέρεται σε καταγραφή σε επίπεδο εφαρμογής.

Στο πρώτο επίπεδο, οι τυπικοί (default) μηχανισμοί της βάσης δεδομένων θα πρέπει να χρησιμοποιηθούν ώστε να παράγεται ένα ίχνος παρακολούθησης (audittrail). Τα είδη πληροφορίας που θα συλλέγονται στο ίχνος εξαρτώνται από τα γεγονότα (events) που θα επιλεγούν.

Ο λόγος για τον οποίο προτείνεται η υλοποίηση της καταγραφής και σε ενέργειες πρόσβασης σε στοιχεία του Πληροφοριακού Συστήματος είναι προκειμένου να παρασχεθεί η τεχνική δυνατότητα απόδοσης ευθυνών ή αποκλεισμού υπόπτων σε περίπτωση διαρροής στοιχείων σε μια συγκεκριμένη χρονική στιγμή ή περίοδο. Το μέγεθος και η διάρκεια διατήρησης των στοιχείων καταγραφής στην βάση προτείνεται να αποτελέσει αντικείμενο συμφωνίας μεταξύ της Εταιρίας και των αναδόχων. Σε κάθε περίπτωση ωστόσο προτείνεται να διατηρούνται τα στοιχεία καταγραφής on-line για περίοδο 6-μηνών και στην συνέχεια να μεταφέρονται σε ταινίες αποθήκευσης. Τυχόν εργαλεία αναζήτησης θα ήταν επίσης χρήσιμα αλλά η υλοποίησή τους αφήνεται να συμφωνηθεί μεταξύ του αναδόχου και της Εταιρίας.

4.4 Μέτρα προστασίας από επιβλαβές λογισμικό

Πρέπει να ληφθούν μέτρα επισήμανσης και αντιμετώπισης επιβλαβούς λογισμικού και ενημέρωσης των χρηστών. Αυτά θα βασίζονται στην ενημέρωση για θέματα ασφαλείας, και στα μέτρα ελέγχου πρόσβασης. Τα κάτωθι θα πρέπει να εξετασθούν:

- Εγκατάσταση και περιοδική ενημέρωση λογισμικού αντιμετώπισης ιών υπολογιστών και χρήση του για έλεγχο αποθηκευτικών μέσων (προβλέπεται κατά την υλοποίηση του έργου).
- Τακτικός έλεγχος λογισμικού και δεδομένων συστημάτων που υποστηρίζουν κρίσιμες διαδικασίες του ΟΠΣ. Η εμφάνιση περίεργων αρχείων ή με εγκεκριμένου λογισμικού θα πρέπει να διερευνάται.
- Έλεγχος αρχείων σε μεταφέρσιμα μέσα αποθήκευσης από αβέβαια ή μη εγκεκριμένη πηγή και αρχείων που μεταφέρονται από ανασφαλή δίκτυα για πιθανή ύπαρξη ιών.

- Έλεγχος επισυναπτόμενων αρχείων ηλεκτρονικού ταχυδρομείου και λοιπών αρχείων δικτυακής προελεύσεως για πιθανή ύπαρξη ιών. Αυτός ο έλεγχος μπορεί να πραγματοποιηθεί σε διάφορα σημεία όπως ο εξυπηρετητής ηλεκτρονικού ταχυδρομείου, οι υπολογιστές των χρηστών ή τα σημεία εισόδου στο δίκτυο του ΟΠΣ.

4.4.1 Πολιτική αντιμετώπισης ιών

Για την αντιμετώπιση των ίων θα πρέπει πάντα να γίνεται χρήση του καθιερωμένου και υποστηριζόμενου στην εκάστοτε Εταιρία λογισμικού αντιμετώπισης ιών. Όποτε γίνεται διαθέσιμη νεότερη έκδοσή του αυτή θα πρέπει να εγκαθίσταται και να χρησιμοποιείται. Περιοδικά πρέπει να ενημερώνεται το λογισμικό αντιμετώπισης ιών και οι χρήστες να λαμβάνουν τις προφυλάξεις τους, επειδή εμφανίζονται συνεχώς νέοι ιοί υπολογιστών.

Η λήψη εισερχόμενου ηλεκτρονικού ταχυδρομείου να γίνεται με την μέγιστη προσοχή λόγω των κινδύνων ασφαλείας που αυτό εμπεριέχει. Το άνοιγμα επισυναπτόμενων αρχείων δεν θα επιτρέπεται εκτός εάν έχει προηγηθεί έλεγχος τους για ύπαρξη ιών ή οποιουδήποτε άλλου είδους επιβλαβούς κώδικα. ΠΟΤΕ να μην ανοίγονται επισυναπτόμενα αρχεία σε ηλεκτρονικό ταχυδρομείο από αναξιόπιστη προέλευσή. Αυτά πρέπει να διαγράφονται και αμέσως μετά να γίνεται οριστική διαγραφή τους καθαρίζοντας και την ενδιάμεση περιοχή αποθήκευσης διαγραμμένων αρχείων. Πρέπει να διαγράφονται άχρηστα μηνύματα ηλεκτρονικού ταχυδρομείου και να μην προωθούνται αυτά σε άλλου χρήστες του ΟΠΣ.

Να μην γίνεται κατέβασμα (downloading) αρχείων από ύποπτες πηγές. Η μεταφορά αρχείων-«κατέβασμα» από το διαδίκτυο (όποτε αυτό γίνει διαθέσιμο) πρέπει να γίνεται με μεγάλη προσοχή προκειμένου να προστατευθεί ο τοπικός υπολογιστής από επιβλαβές λογισμικό και να μην βρεθεί σε αυτό παντός είδους ανάρμοστο υλικό.

Να μην γίνεται διαμοιρασμός αρχείων σε άλλους χρήστες, δίνοντας τους δικαιώματα τροποποίησης και ανάγνωσης χωρίς αυτό να είναι απολύτως απαραίτητο.

Όλα τα μαγνητικά μέσα αποθήκευσης θα πρέπει να καταστρέφονται ασφαλώς.

Πάντα να ελέγχονται δισκέτες και γενικά μεταφέρσιμα μέσα αποθήκευσης π.χ. δίσκων και CD-ROM από άγνωστη προέλευση για ύπαρξη ιών.

Μεταφέρσιμα μέσα αποθήκευσης που περιέχουν ευαίσθητα δεδομένα πριν επαναχρησιμοποιηθούν πρέπει να διαγράφονται πλήρως.

Τα μέσα αποθήκευσης θα πρέπει να είναι προσβάσιμα χρησιμοποιώντας περισσότερα από ένα κανάλι εισόδου/ εξόδου, για να παρέχουν εναλλακτικές οδούς και να διευκολύνουν το φόρτο σε συγκεκριμένα κανάλια.

Η πρόσβαση σε μεταφερόμενες μονάδες αποθήκευσης θα πρέπει να ελέγχεται με λογικό και όχι με φυσικό τρόπο.

Υλικό αποθήκευσης δεδομένων που περιέχει ευαίσθητα δεδομένα πρέπει ή να διαγράφεται με ασφαλή τρόπο πριν σταλεί για συντήρηση ή πρέπει να συνοδεύεται από εξουσιοδοτημένο άτομο.

Αν το λογισμικό του συστήματος σε κάποιο σημείο δεν μπορεί να εκτελεστεί ταυτόχρονα με το λογισμικό αντιμετώπισης ιών τότε το δεύτερο θα χρησιμοποιηθεί για τον έλεγχο του πρώτου και κατόπιν θα απενεργοποιηθεί προκειμένου να εκτελεστεί η εκάστοτε εφαρμογή με την προϋπόθεση ότι δεν θα δίδεται η δυνατότητα μεταφοράς ιών π.χ. από ηλεκτρονικό ταχυδρομείο ή διαμοιρασμό αρχείων.

4.4.2 Λογισμικό αντιμετώπισης ιών

Χωρίς εξαίρεση το λογισμικό αντιμετώπισης ιών θα τοποθετηθεί σε όλους τους προσωπικούς υπολογιστές και θα ενημερώνεται τακτικά ανιχνεύοντας εξυπηρετητές, προσωπικούς και φορητούς υπολογιστές.

Η πιθανότητα προσβολής από ιούς ελαχιστοποιείται εάν χρησιμοποιείται αποτελεσματικό λογισμικό αντιμετώπισής τους και ενημερώνονται τακτικά οι βιβλιοθήκες απειλών του. Πολλές εταιρείες που παράγουν λογισμικό αντιμετώπισης ιών προσφέρουν τέτοιου είδους ενημέρωση στις ιστοσελίδες τους.

Το λογισμικό ανίχνευσης ιών θα πρέπει να προέρχεται από ένα αξιόπιστο προμηθευτή. Η ανάπτυξη λογισμικού ανίχνευσης-αντιμετώπισης ιών (anti-virus) είναι μία εξειδικευμένη και με απαιτήσεις σημαντικής τεχνογνωσίας εργασία . Επιλογή μη επαρκούς λογισμικού αντιμετώπισης ιών μπορεί να αφήσει το ΟΠΣ εκτεθειμένο σε ιούς. Επειδή οι ορισμοί-βιβλιοθήκες του λογισμικού αντιμετώπισης ιών είναι πάντα ενδεικτικές η επιλογή ενός γνωστού προμηθευτή θα πρέπει να εξεταστεί προσεκτικά καθώς η ταχύτητα απόκρισής του είναι πολύ σημαντική.

Προσοχή πρέπει να δοθεί στα παρακάτω:

- Εάν δεν υπάρχει σχεδιασμός αντιμετώπισης προσβολής από ιούς τότε οι αντιδράσεις των χρηστών και των διαχειριστών του συστήματος θα είναι πιθανότατα ανεπαρκείς μετατρέποντας ένα ελέγξιμο πρόβλημα σε ιδιαιτέρως σοβαρό.
- Η έλλειψη ενός προτύπου ή μη τήρησή του κατά την τοποθέτηση του λογισμικού αντιμετώπισης ιών μπορεί να αυξήσει σοβαρά τον κίνδυνο από προσβολή και διάδοση ενός ιού.

- Η μη ενημέρωση του λογισμικού αντιμετώπισης ιών σε τακτά χρονικά διαστήματα μπορεί να προκαλέσει προσβολή από μία νέα παραλλαγή ιού ή από καινούργιο ιό.

4.5 Ευρωπαϊκό Νομοθετικό Πλαίσιο

Στην ενότητα παραθέτουμε νόμους για την προστασία προσωπικών δεδομένων. Στην συγκεκριμένη διατριβή μας ενδιαφέρει περισσότερο η συλλογή και διαχείριση που μπορεί να έχει ένα πληροφοριακό σύστημα και οι νόμοι που το πλαισιώνουν για τυχών διαρροή προσωπικών στοιχείων .

- ***Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου*** – ΕΣΔΑ (European Human Rights Convention - EHRC) του 1950. Το άρθρο 8 προστατεύει την ιδιωτική ζωή, στην οποία συγκαταλέγονται και τα προσωπικά δεδομένα.
- ***Οδηγία 95/46/ΕΚ*** (Directive 95/46/EC) της ΕΕ προς τα κράτη-μέλη, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών.
- ***Οδηγία 97/66/ΕΚ*** (Directive 97/66/EC) για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα, η οποία αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ (2002/58/EC) για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών.
- ***Χάρτης (διακήρυξη) των Θεμελιωδών Δικαιωμάτων της ΕΕ*** (Charter of Fundamental Rights of the European Union), που αποτελεί τη πιο πρόσφατη εξέλιξη στον τομέα των θεμελιωδών δικαιωμάτων των πολιτών. Το άρθρο 8 ορίζει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη

συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο.

- ***Οδηγία No R (99) 5*** (Recommendation No R (99) 5), η οποία έγινε αποδεκτή από το Συμβούλιο της Ευρώπης το 1999, και η οποία παρέχει κατευθυντήριες γραμμές (guide lines) για την προστασία των ατόμων σε σχέση με τη συλλογή και επεξεργασία προσωπικών δεδομένων σε λεωφόρους πληροφοριών (information highways).

4.6 Εθνική Νομοθεσία

Όσον αφορά στον Ελληνικό χώρο:

Τα προσωπικά δεδομένα προστατεύονται καταρχάς από το ***άρθρο 9Α του Συντάγματος***: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.», και η επεξεργασία τους επιτρέπεται μόνο υπό τις προϋποθέσεις που ορίζει ο νόμος. Το άρθρο 9Α κατοχυρώνει και ρητά πλέον το ατομικό δικαίωμα προστασίας απέναντι στη συλλογή, αποθήκευση και επεξεργασία, με συμβατικό ή ηλεκτρονικό τρόπο των προσωπικών πληροφοριών και δεδομένων. Πρόκειται για τη συνταγματική επιβεβαίωση και επιστέγαση των βημάτων που έχει κάνει ήδη η ελληνική έννομη τάξη με την υπογραφή της σχετικής σύμβασης του 1981 του Συμβουλίου της Ευρώπης (η οποία κυρώθηκε με το νόμο 2068/1992), με την εναρμόνιση προς τη σχετική Κοινοτική Οδηγία 95/46ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και ιδίως με την ψήφιση του Νόμου 2472/1997.

Ο Νόμος 2472/97 μεταφέρει την Οδηγία 95/47/ΕΚ στο εσωτερικό δίκαιο και συγχρόνως εκπληρώνει την υποχρέωση της Ελλάδας που

απορρέει από τη Σύμβαση 108 του Συμβουλίου της Ευρώπης. Επιπλέον, η οδηγία 97/66/ΕΚ, που εξειδικεύει την Οδηγία 95/46/ΕΚ ως προς ορισμένες πτυχές που συνδέονται με τη συγκεκριμένη κατηγορία εφαρμογής, μεταφέρεται στο εσωτερικό δίκαιο με τον ελληνικό νόμο ***2774/99***.

Σύμφωνα με το Ν. 2472/97, με τον όρο ***«επεξεργασία»*** εννοούμε κάθε εργασία ή σειρά εργασιών που εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή. Η επεξεργασία ευαίσθητων δεδομένων, μπορεί να πραγματοποιείται μόνο μετά από λήψη άδειας από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και η νομιμότητα της επεξεργασίας αφορά σε όλα της τα στοιχεία, δηλαδή ποια δεδομένα, από ποιόν και για ποιο σκοπό θα συλλεχθούν και θα επεξεργασθούν, σε ποιόν και για ποιο σκοπό θα ανακοινωθούν ή ποιος θα έχει πρόσβαση. Τα σημεία αυτά θα ληφθούν ιδιαίτερα υπόψη σε συνάρτηση με τα απαραίτητα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των δεδομένων.

Όσον αφορά τις διασυνοριακές ροές δεδομένων, αυτές καθορίζονται από τα ***άρθρα 25 και 26 της Οδηγίας 95/46/ΕΚ*** (και από τις σχετικές διατάξεις του ***Ν. 2472/1997*** για τη χώρα μας). Έτσι, για παράδειγμα, η μεταφορά προσωπικών δεδομένων από μια χώρα μέλος της ΕΕ προς κάποια τρίτη χώρα επιτρέπεται μόνο στην περίπτωση που η χώρα αυτή εγγυάται ένα επαρκές επίπεδο προστασίας των δεδομένων αυτών. Η επάρκεια αποτιμάται με βάση την κάθε περίπτωση, ενώ ιδιαίτερη προσοχή δίνεται σε θέματα όπως η φύση των δεδομένων, ο σκοπός επεξεργασίας καθώς και το νομικό πλαίσιο και τα μέτρα ασφάλειας που ισχύουν στη χώρα προορισμού.

Κεφάλαιο 5

CASESTUDY

Στο παρακάτω κεφάλαιο θα γίνει η παρουσίαση της εταιρείας και η περιγραφή του ολοκληρωμένου πληροφοριακού συστήματος.

5.1 Η εταιρεία

Η εταιρεία δραστηριοποιείται στο χώρο του ανοξείδωτου χάλυβα. Παράγει και εμπορεύεται μία σειρά από προϊόντα τα οποία είναι αποτέλεσμα επεξεργασίας υποπροϊόντων ανοξείδωτου χάλυβα.

Πιο συγκεκριμένα οι δυο βασικές κατηγορίες προϊόντων – εμπορευμάτων είναι τα ρολά και τα φύλλα, καθώς και τα εξαρτήματα ανοξείδωτου χάλυβα (λάμες, τετράγωνα, σύρμα, άξονες, διάτρητα, γωνίες, σωλήνες, καμπύλες, στραντζαριστά, ανθρωποθυρίδες κ.τ.λ.).

Τα κεντρικά γραφεία της εταιρείας βρίσκονται στη Μαγούλα Αττικής (που στεγάζονται κυρίως οι οικονομικές υπηρεσίες), ενώ η αποθήκη – εργοστάσιο βρίσκεται στη Μάνδρα Αττικής (που στεγάζονται τα υπόλοιπα τμήματα). Η εταιρεία επίσης διατηρεί υποκατάστημα - αποθήκη και στη Σίνδο Θεσσαλονίκης.

Καθώς το ERP θα αποτελέσει το κεντρικό σύστημα διαχείρισης πληροφορίας της εταιρείας, όλα τα τμήματα θα έχουν πρόσβαση σε

αυτό, με συγκεκριμένα δικαιώματα πρόσβασης και κατάλληλα παραμετροποιημένες οθόνες προβολής.

Οι θέσεις εργασίας που έχουν πρόσβαση στο ERP αποτυπώνονται ως εξής :

Κεντρικά γραφεία Μαγούλα Αττικής

Διοίκηση	1
Λογιστήριο	6
Αγορές	2
Μηχανογράφηση	3

Πίνακας 2: Συστήματα κεντρικών γραφείων εταιρίας

Υποκατάστημα Μάνδρα Αττικής (εργοστάσιο - αποθήκη)

Διοίκηση	1
Πωλήσεις – Διακινήσεις	7
Τιμολόγηση – Εισπράξεις – Ταμείο	3
Παραγωγή	5
Αποθήκη - Φορτώσεις	3

Πίνακας 3: Συστήματα υποκαταστήματος Μάνδρας

Υποκατάστημα Θεσσαλονίκη (αποθήκη)

Πωλήσεις – Διακινήσεις	4
Τιμολόγηση – Εισπράξεις – Ταμείο	1
Αποθήκη - Φορτώσεις	1

Πίνακας 4: Συστήματα Υποκαταστήματος Θεσσαλονίκης

5.2 ΥποσυστήματαERP

Τα υποσυστήματα του ERPπου θα εγκατασταθούν στην εταιρία που εξετάζουμε θα είναι :

Α. Λογιστήριο

Β. Αποθήκη

Γ. Παραγωγή

Δ. Πωλήσεις

Ε. Πελάτες

ΣΤ. Αγορές – Προμηθευτές

Εικόνα 4:πληροφοριακό σύστημα

5.3 Λόγοι υιοθέτησης πληροφοριακού συστήματος

Οι εξειδικευμένες ανάγκες των πελατών της Εταιρίας που οδηγούν σε συνεχείς βελτιώσεις της παραγωγικής διαδικασίας και η ιδιαίτερη ανάγκη για αποτελεσματική διαχείριση των αποθεμάτων πρώτης ύλης, δημιουργούν την ανάγκη για το σχεδιασμό και την υλοποίηση ενός ολοκληρωμένου πληροφοριακού συστήματος, το οποίο θα παρέχει μηχανογραφική υποστήριξη σε όλες τις επιμέρους φάσεις της παραγωγικής διαδικασίας, θα εξασφαλίζει τη διάχυση της πληροφορίας μεταξύ των διαφόρων συνεργαζόμενων τμημάτων (συμπεριλαμβανομένου του τμήματος παραγωγής) και παράλληλα θα δίνει τη δυνατότητα στη Διοίκηση να ενημερώνεται έγκυρα και έγκαιρα για την πορεία των διαφόρων εργασιών των επιμέρους τμημάτων της εταιρείας και να προβαίνει στις απαραίτητες ενέργειες.

Αναγνωρίζοντας την ανωτέρω ανάγκη, η Διοίκηση της εταιρείας σκοπεύει να εγκαταστήσει ένα ενιαίο ολοκληρωμένο πληροφοριακό σύστημα.

Οι βασικοί στόχοι που θα πρέπει να διέπουν αυτό το σύστημα είναι οι ακόλουθοι :

1. Την αύξηση της παραγωγικότητας και της ανταγωνιστικότητας της εταιρείας.
2. Την πληροφοριακή υποστήριξη και μηχανοργάνωση του συνόλου των δραστηριοτήτων της εταιρείας π.χ. εμπορική διαχείριση, παραγωγή, παραγγελίες, εισαγωγές, λογιστική διαχείριση.
3. Την εξασφάλιση της ροής της πληροφορίας μεταξύ των διαφόρων τμημάτων.

4. Την υποστήριξη των αποφάσεων της διοίκησης με την παροχή της δυνατότητας άντλησης, επεξεργασίας και ενοποίησης επικαιροποιημένων δεδομένων.
5. Τη θέσπιση διαδικασιών ασφάλειας του συστήματος με την καθιέρωση κανόνων που αφορούν την προσπέλαση στο σύστημα και στα διαθέσιμα δεδομένα ανά χρήστη.
6. Τη βελτίωση των σχέσεων με πελάτες και προμηθευτές.
7. Την εξασφάλιση της επεκτασιμότητας του συστήματος.
8. Τη μεγιστοποίηση της αποδοτικότητας των εργαζομένων και της παραγωγικής δυνατότητας των μηχανημάτων της.

5.4 Οικονομικό πλάνο του έργου

ΆΔΕΙΑ ΧΡΗΣΗΣ ΛΟΓΙΣΜΙΚΟΥ

ΠΕΡΙΓΡΑΦΗ	ΤΙΜΗ ΛΙΑΝΙΚΗΣ	ΠΟΣΟΤΗΤΑ	ΕΚΠΤΩΣΗ	ΤΕΛΙΚΗ ΤΙΜΗ
Γενική –Αναλυτική λογιστική-Κέντρα Κόστους	**€2.500,00**	**1**	**0.00%**	**€2.500,00**
Διαχείριση Αποθήκης	**€9.000,00**	**1**	**0.00%**	**€9.000,00**
Διαχείριση παραγωγής – κοστολόγηση παραγωγής	**€12.000,00**	**1**	**0.00%**	**€12.000,00**
Διαχείριση πωλήσεων	**€6.000,00**	**1**	**0.00%**	**€6.000,00**

Διαχείριση Εισπράξεων	**€2.500,00**	**1**	**0.00%**	**€2.500,00**
ΔιαχείρισηΑγορών	**€4.000,00**	**1**	**0.00%**	**€4.000,00**
ΔιαχείρισηΠληρωμών	**€2.000,00**	**1**	**0.00%**	**€2.000,00**
ΔιαχείρισηΠαγίων	**€1.500,00**	**1**	**0.00%**	**€1.500,00**
Πληροφοριακό σύστημα Διοίκησης	**€5.000,00**	**1**	**0.00%**	**€5.000,00**
Μισθοδοσία – Διαχείριση ανθρώπινου δυναμικού (payroll)	**€5.000,00**	**1**	**0.00%**	**€5.000,00**
Κύκλωμα ωρομέτρησης ωροκτύπησης (Time attendance)	**€3.000,00**	**1**	**0.00%**	**€3.000,00**
Διαχείριση Ηλεκτρικού Πρωτοκόλλου	**€4.000,00**	**1**	**0.00%**	**€4.000,00**
Συνολικό κόστος Άδειας χρήσης	**€56.500,00**			**€56.500,00**
Κόστος Αγοράς πηγαίου κώδικα του παραπάνω συστήματος				**€50.000,00**
Σύνολο				**€106.500,00**

Πίνακας 5: Άδεια χρήσης λογισμικού

ΥΠΗΡΕΣΙΕΣ ΥΛΟΠΟΙΗΣΗΣ ΤΟΥ ΕΡΓΟΥ

ΠΕΡΙΓΡΑΦΗ	ΚΟΣΤΟΣ ΑΝΘΡΩΠΟΗΜΕΡΑΣ	ΗΜΕΡΕΣ	ΕΚΠΤΩΣΗ	ΤΕΛΙΚΗ ΤΙΜΗ
Υπηρεσίες προσαρμογής – παραμετροποίησης συστημάτων	**€400,00**	**155**	**0.00%**	**€62.000,00**
Υπηρεσίες εγκατάστασης – onsite παρουσίας με την επίσημη έναρξης λειτουργίας	**€400,00**	**44**	**0.00%**	**€17.600,00**
Υπηρεσίες εκπαίδευσης	**€400,00**	**25**	**0.00%**	**€10.000,00**
Υπηρεσίες Μετάπτωσης δεδομένων (Datamigration) από τα υφιστάμενα συστήματα	**€400,00**	**22**	**0.00%**	**€8.800,00**
Συνολικό κόστος Υπηρεσιών				**€98.400,00**
ΤΕΛΙΚΟ ΚΟΣΤΟΣ ΕΓΚΑΤΑΣΤΑΣΗΣ				**204.900,00**

Πίνακας 6: Υπηρεσίες υλοποίησης έργου

ΠΡΟΙΟΝ	ΤΙΜΗ ΛΙΑΝΙΚΗΣ	ΠΟΣΟΤΗΤΑ	ΕΚΠΤΩΣΗ	ΤΕΛΙΚΗ ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ
Oracle Database Standard Edition 10g-ΆδειαΧρήσης ASFU	**€251,00**	**40**	**50%**	**€5.020**
Ετήσιο συμβόλαιο συντήρησης αδειών χρήσης	**€47,69**	**40**	**50%**	**€953,80**
Συνολικό κόστος				**€5.973,80**

Πινάκας 7: Προϊόντων προμήθειας 1

ΠΡΟΙΟΝ	ΤΙΜΗ ΛΙΑΝΙΚΗΣ	ΠΟΣΟΤΗΤΑ	ΕΚΠΤΩΣΗ	ΤΕΛΙΚΗ ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ
Oracle Internet Application Server(IAS)Enterprise edition –Άδεια ΧρήσηςASFU	**€502,00**	**40**	**50%**	**€10.040,00**
Ετήσιο συμβόλαιο συντήρησης αδειών	**€95,38**	**40**	**50%**	**€1.907,00**

χρήσης				
Συνολικό κόστος				**€11.947,60**

Πινάκας 8: Προϊόντων προμήθειας 2

ΠΡΟΙΟΝ	ΤΙΜΗ ΛΙΑΝΙΚΗΣ	ΠΟΣΟΤΗΤΑ	ΕΚΠΤΩΣΗ	ΤΕΛΙΚΗ ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ
Oracle Business Intelligence Standard Edition One-ÄδειαΧρήσηςASFU	**€861,00**	**5**	**50%**	**€2.152,50**
Ετήσιο συμβόλαιο συντήρησης αδειών χρήσης	**€163,59**	**5**	**50%**	**€408,98**
Συνολικό κόστος				**€2.561,48**

Πινάκας 9: Προϊόντων προμήθειας 3

ΠΡΟΙΟΝ	ΤΙΜΗ ΛΙΑΝΙΚΗΣ	ΠΟΣΟΤΗΤΑ	ΕΚΠΤΩΣΗ	ΤΕΛΙΚΗ ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ
Internet Development Suite-ΆδειαΧρήσηςFull Use	**€4.162,00**	**2**	**20%**	**€6.659,20**
Ετήσιο συμβόλαιο συντήρησης αδειών χρήσης	**€915,64**	**2**	**0.00%**	**€1.831,28**
Συνολικό κόστος				**€8.490,48**

Πινάκας 10: Προϊόντων προμήθειας 4

ΠΡΟΙΟΝ	ΤΙΜΗ ΛΙΑΝΙΚΗΣ	ΠΟΣΟΤΗΤΑ	ΕΚΠΤΩΣΗ	ΤΕΛΙΚΗ ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ
Φορολογικός Μηχανισμός	**€600,00**	**6**	**25%**	**€2.700,00**
Συνολικό κόστος				**€2.700,00**

Πίνακας 11: Προμήθειας φορολογικών μηχανισμών

Προϊόντα/Υπηρεσίες	Συνολικό κόστος
Τελικό κόστος εγκατάστασης	**€204.900,00**
Oracle database και συμβόλαιο Συντήρησης	**€5.973,80**
Internet application server και συμβόλαιο συντήρησης	**€11.947,60**
Business intelligence και συμβόλαιο συντήρησης	**€2.561,48**
Internet development και συμβόλαιο συντήρησης	**€8.490,48**
Φορολογικοί μηχανισμοί	**€2.700**
Συνολικό κόστος επένδυσης	**€236.573,36**

Πίνακας 12: Συνολικό κόστος επένδυσης

Κεφάλαιο 6

Παρουσίαση Αποτελεσμάτων Έρευνας

Στην παρούσα μελέτη περίπτωσης εγκατάστασης ενός ολοκληρωμένου πληροφοριακού συστήματος η ομάδα ασφαλείας θα αποτελείται από τον project manager του έργου , το IT της εταιρίας και τον γενικό διευθυντή .Ο ρόλος του project manager είναι να μπορέσει να υιοθετήσει ένα επιτυχημένο ολοκληρωμένο πληροφοριακό σύστημα η εταιρία και το σημαντικότερο κομμάτι για να πετύχει κάτι τέτοιο , είναι να κάνει σωστή διαχείριση της επικινδυνότητας του συστήματος. Τα μέλη της μηχανογράφησης της εταιρίας με βάση τις τεχνικές γνώσεις τους θα βοηθήσουν στην διεκπεραίωση του έργου και θα συμβάλουν στην ασφάλεια του συστήματος τόσο κατά τον σχεδιασμό , όσο και κατά την διάρκεια του έργου, με την συντήρησή του. Ο γενικός διευθυντής στην ομάδα ασφαλείας του έργου , έχει περισσότερο ένα συντονιστικό ρόλο , τόσο για μια γενική επίβλεψη των διαδικασιών , όσο και για να μπορέσει το προσωπικό της εταιρίας να υιοθετήσει τους κανόνες ασφαλείας βλέποντας ένα ανώτερο μέλος της διοίκησης να ασχολείται με το συγκεκριμένο ζήτημα.

Η ανάλυση που γίνεται για την παρούσα διατριβή στο σενάριο που περιγράφεται στην προηγούμενη ενότητα , είναι η διερεύνηση των κινδύνων του πληροφοριακού συστήματος , αξιολόγησής τους με βάση την σημαντικότητα τους και τις επιπτώσεις που μπορεί να έχουν , ενέργειες αποφυγής τους ,όπως και τρόποι αντιμετώπισής τους σε ενδεχόμενη περίπτωση ευπάθειας.

Υπάρχουν τέσσερις τρόποι αντιμετώπισης των κινδύνων. Όπως όμως μπορούμε να καταλάβουμε , είναι σημαντικό να μπορέσουμε να προβλέψουμε όλους τους πιθανούς κινδύνους που μπορεί να προκαλέσει ζημιά στο σύστημά μας.

Ο πρώτος τρόπος είναι η αποφυγή του κινδύνου , κάνοντας τις κατάλληλες μελέτες για να μπορέσουμε να τον εξαλείψουμε εντελώς.

Ο δεύτερος τρόπος είναι η μείωση του κινδύνου , βρίσκοντας τρόπους βελτιστοποίησης και μετριασμό του.

Ο τρίτος τρόπος είναι ο καταμερισμός του κινδύνου , κάνοντας ανάθεση σε τρίτους με μεγαλύτερη εμπειρία και εξοπλισμό (outsourcing) ή ασφαλίζοντας τον σε περίπτωση μετάπτωσης και κακής λειτουργίας.

Ο τέταρτος τρόπος είναι η διατήρηση του κινδύνου ,δηλαδή αποδοχή του βάση προϋπολογισμού και η συνεχής παρακολούθησή του.

Όπως έχουμε αναφέρει για να μπορέσει να γίνει η διαχείριση των κινδύνων, θα πρέπει να υπάρχει ένα αποτελεσματικό σχέδιο , ένας αποτελεσματικός σχεδιασμός ,όμως δεν τελειώνει εκεί. Υπάρχει και η συνεχής παρακολούθηση που είναι απαραίτητη κάθε στιγμή. Υπάρχουν διάφοροι τρόποι για να μπορέσει κάποιος να κάνει την διαχείριση της επικινδυνότητας και αυτό διαφέρει από έργο σε έργο. Το κόστος είναι ένα σημαντικό κομμάτι για την διαχείριση των κινδύνων και είναι ο κεντρικός άξονας για να μπορέσει κάποιος να αξιολογήσει. Είναι φυσικό όμως όταν μιλάμε για κινδύνους να υπάρχει μια τεράστια συλλογή που θα ήταν δύσκολο κάποιος να αναλύσει. Μέσα στο σύνολο των κινδύνων θα μπορούσαν να συγκαταλέγονται και κίνδυνοι διαρροής απόρρητων και εμπιστευτικών δεδομένων ,όπου σε περίπτωση διαρροής δεν θα μπορούσε κάποιος να αναλογιστεί τις συνέπειες.

Στην δική μας μελέτη περίπτωσης η τακτική για την αξιολόγηση των κινδύνων είναι περισσότερο βάση κόστους επένδυσης και κόστους ζημίας που θα μπορούσε να προκαλέσει. Αξιολογείται βάση του

αρχικού κόστους επένδυσης , της πιθανότητας ύπαρξης και των συνεπειών που μπορεί να προκαλέσει, κυρίως οικονομικής φύσεως.

Είναι σημαντικό να αναφέρουμε ότι θα πρέπει να υπάρχει μια προτεραιότητα στην διαχείριση , διότι η χρονοβόρα ανάλυση των κινδύνων ενός έργου και οι τρόποι αντιμετώπισης τους μπορεί να προκαλέσουμε μεγάλες καθυστερήσεις ή ακόμα και να μην μπορέσει να ξεκινήσει η διαδικασία . Αυτό ισχύει ιδιαίτερα όταν μια άλλη εργασία αναστέλλεται έως ότου η διαδικασία διαχείρισης κινδύνων θεωρείται πλήρης.

6.1 Καθορισμός πιθανότητας και συνεπειών

Η ανάλυση της πιθανότητας και των συνεπειών που μπορεί να αποφέρει ένας κίνδυνος είναι το επόμενο βήμα μετά την αναγνώρισή του. Οι παρακάτω πίνακες μας δείχνουν τα επίπεδα για τον καθορισμό τους.

Καθορισμός πιθανότητας

Επίπεδο	παράμετρος	περιγραφή	εύρος	Μέση τιμή
1	Almost certain	Σχεδόν σίγουρο (κάθε μέρα)	>90%	0.95
2	Likely	Πιθανό (έχει πολλές πιθανότητες να συμβεί)	50%-90%	0.70
3	Possible	Ενδεχόμενος (να συμβεί κάποια χρονική στιγμή)	20%-50%	0.35
4	Unlikely	Απίθανο	10%-20%	0.15
5	Rare	Σπάνιο	<10%	0.05

Πίνακας 13: καθορισμός πιθανότητας

Καθορισμός συνεπειών

Επίπεδο	παράμετρος	Οικονομικό κόστος	Επιχειρησιακή αποδοτικότητα	Κόστος
1	Ασήμαντη	Ασήμαντο οικονομικό κόστος	Μικρή επίπτωση	<500€
2	Μικρή	Χαμηλή οικονομική ζημιά	Ενοχλητική/καθυστερήσεις	500€-1000€
3	Μέτρια	Μέτρια οικονομική ζημιά	Σημαντικές καθυστερήσεις	1000€-2000€
4	Μείζον	Υψηλή οικονομική ζημιά	Εκτεταμένες βλάβες	2000€-5000€
5	Καταστροφική	Σημαντικές οικονομικές απώλειες	Μη επίτευξη κύριων/βασικών στόχων	>5000€

Πίνακας 14: Καθορισμός συνεπειών

Πιθαν/συνέπ	ασήμαντες	μικρές	μέτριες	Μείζον	καταστροφικές
1(almost certain)	S	S	H	H	H
2(likely)	M	S	S	H	H
3(possible)	L	M	S	H	H
4(unlikely)	L	L	M	S	H
5(rare)	L	L	M	S	S

Πίνακας 15: πιθανότητα / συνέπεια

Υπόμνημα

L	Lowrisk (μικρός κίνδυνος)-διαδικασίες ρουτίνας
M	Moderaterisk (μέτριος κίνδυνος)-καθορισμός ευθύνης διαχείρισης
S	Significantrisk (σημαντικός κίνδυνος)-Ανωτέρου σημασίας
H	Highrisk (υψηλός κίνδυνος)-λεπτομερής προγραμματισμός

Πίνακας 16: Υπόμνημα

6.2 Κατηγορίες προτεραιοτήτων

Σύμφωνα με τον παραπάνω πίνακα θα δημιουργήσουμε προτεραιότητες για τους κινδύνους που διατρέχει το πληροφοριακό σύστημα ανάλογα με την πιθανότητα εμφάνισης και ανάλογα την χρηματική απώλεια της επιχείρησης.

Προτεραιότητα	**Τύπος κινδύνου**	**Περιγραφή**
#1	Υψηλός κίνδυνος	Α) Μέτριες έως καταστροφικές συνέπειες και με πιθανότητα σχεδόν σίγουρη >90% Β) Μείζον ή καταστροφικές συνέπειες σε πιθανό ή ενδεχόμενο κίνδυνο με μέσο όρο εμφάνισης περίπου 55% Γ) Καταστροφικός κίνδυνος >5000€ ζημιά με πιθανότητα περίπου 15%
#2	Σημαντικός κίνδυνος	Α) Ασήμαντες ή

		μικρές οικονομικές συνέπειες αλλά με σχεδόν σίγουρη εμφάνιση>90% Β) μικρές έως μέτριες συνέπειες με πιθανότητα από 50% έως 70% Γ) Μέτριες συνέπειες με πιθανότητα από 20% έως 50% Δ) Μείζον συνέπειες με πιθανότητα 10% έως 20% Ε) Μείζον ή καταστροφικές συνέπειες με πιθανότητα εμφάνισης <10%
#3	Μέτριος κίνδυνος	Α) Ασήμαντες συνέπειες αλλά με πιθανότητα 50% έως 70% Β) Μικρές συνέπειες με πιθανότητα 20% έως 50% Γ) Μέτριες συνέπειες με πιθανότητες <10% έως 20%

#4	Μικρός κίνδυνος	Α) Ασήμαντες συνέπειες με πιθανότητες εμφάνισης από <10% μέχρι 50% Β) Μικρές συνέπειες με πιθανότητα εμφάνισης <10% έως 20%

Πίνακας 17: κατηγορίες προτεραιοτήτων

6.3 Κίνδυνοι Έργου

Κίνδυνοι	Όνομα	Τύπος Κινδύνου
#1	Έργο εκτός ορίων χρονοπρογραμματισμού	Οργανωτικός κίνδυνος
#2	Έργο εκτός ορίων οικονομικού πλάνου	Οργανωτικός κίνδυνος
#3	Άρνηση προσωπικού στις τεχνολογικές αλλαγές	Οργανωτικός κίνδυνος
#4	Κίνδυνος πυρκαγιάς	Φυσικός κίνδυνος
#5	Κίνδυνος σεισμικής δόνησης	Φυσικός κίνδυνος
#6	Κίνδυνος πλημύρας	Φυσικός κίνδυνος
#7	Κίνδυνος κεραυνού	Φυσικός κίνδυνος
#8	Παρεμβολές στις επικοινωνίες από καιρικά φαινόμενα	Φυσικός κίνδυνος
#9	Δυσλειτουργία /αστοχία υλικού	Τεχνολογικός κίνδυνος

#10	Αστοχία μέσων αποθήκευσης	Τεχνολογικός κίνδυνος
#11	Γήρανση / συντήρηση εξοπλισμού	Τεχνολογικός κίνδυνος
#12	καταστροφή ηθελημένη / ακούσια εξοπλισμού	Ανθρώπινος κίνδυνος
#13	Αστοχία λογισμικού	Τεχνολογικός κίνδυνος
#14	Δυσλειτουργία λογισμικού /κακή ρύθμιση / μη συμβατότητα	Τεχνολογικός κίνδυνος
#15	Κακόβουλο λογισμικό	Ανθρώπινος κίνδυνος / τεχνολογικός κίνδυνος
#16	Παρεμβολές	Τεχνολογικός κίνδυνος
#17	Διακοπή επικοινωνίας συστημάτων	Τεχνολογικός κίνδυνος
#18	Διακοπή ηλεκτροδότησης	Τεχνολογικός κίνδυνος
#19	Διακοπή Κλιματισμού εγκατάστασης	Τεχνολογικός κίνδυνος
#20	Μη ομαλή μετάπτωση δεδομένων από παλαιότερο σύστημα	Τεχνολογικός κίνδυνος
#21	Υποκλοπή /αλλοίωση / καταστροφή πληροφοριών	Θεσμικός κίνδυνος
#22	Διαρροή προσωπικών / εταιρικών δεδομένων	Θεσμικός κίνδυνος
#23	Λάθος εξουσιοδοτήσεις σε χρήστες	Ανθρώπινος κίνδυνος / οργανωτικός κίνδυνος
#24	Κλοπή λογισμικού / υλικού	Ανθρώπινος κίνδυνος

Πίνακας 18: Κίνδυνοι ΟΠΣ

6.4 Φύλλα κινδύνου

<table>
<tr><th colspan="5">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ</th></tr>
<tr><td colspan="3">ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#1</td><td colspan="2">Έργο εκτός ορίων χρονοπρογραμματισμού</td></tr>
<tr><td colspan="3">ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ</td><td colspan="2">Έργο εκτός χρονικών ορίων υλοποίησης</td></tr>
<tr><td colspan="3">ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:</td><td colspan="2">Οργανωτικός κίνδυνος</td></tr>
<tr><td colspan="3">ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:</td><td colspan="2">01/01/2013</td></tr>
<tr><td colspan="3">ΥΠΘΥΘΥΝΟΣ:</td><td colspan="2">Παρασκευόπουλος Α.</td></tr>
<tr><td colspan="3">ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ</td><td colspan="2"></td></tr>
<tr><td>ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ</td><td>ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ</td><td>ΈΚΘΕΣΗ Μ.Ο. 15%</td><td>ΠΡΟΤΕΡΑΙΟΤΗΤΑ</td><td>ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ</td></tr>
<tr><td>10%-20%</td><td>Καταστροφική 236.573,36€</td><td>35.486,004€</td><td rowspan="2">1</td><td rowspan="2">11/03/2013</td></tr>
<tr><td></td><td>ΣΥΝΟΛΟ:</td><td>35.486,004€</td></tr>
<tr><th colspan="5">ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ</th></tr>
<tr><td>ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:</td><td colspan="4">Χρονοδιάγραμμα έργου: Το χρονοδιάγραμμα του έργου που μας δείχνει τις εργασίες που πρέπει να υλοποιηθούν και το χρονικό διάστημα στο οποίο είναι απαραίτητο να έχουν υλοποιηθεί , είναι το εργαλείο για την παρακολούθηση του συγκεκριμένου κινδύνου.</td></tr>
<tr><td>ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:</td><td colspan="4">Εργασία εκτός χρονοδιαγράμματος: Η μεγάλη χρονική καθυστέρηση κάποιας εργασίας είτε στην αρχή της είτε κατά την διάρκεια της υλοποίησης της φέρνει σαν αποτέλεσμα την καθυστέρηση των ακόλουθων εργασιών που έχουν προγραμματιστεί.</td></tr>
<tr><td>ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:</td><td colspan="4">Αποφυγή : Σίγουρα η στρατηγική αντιμετώπισης είναι να αποφύγουμε μία κατάσταση χρονοκαθυστέρησης όμως σε πολλές περιπτώσεις που δεν είναι εφικτό είναι προτιμότερο να έχουμε καθυστέρηση σε εργασίες που είναι ανεξάρτητες από επόμενες εργασίες και δεν καθυστερείται η συνέχιση της αλυσίδας.</td></tr>
<tr><td>ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:</td><td colspan="4">11/03/2013</td></tr>
<tr><td colspan="5">(Προαιρετική συμπλήρωση)</td></tr>
<tr><td>ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:</td><td colspan="4">Πλήρης οργάνωση και σωστός χρονοπρογραμματισμός : Η πλήρης οργάνωση και ο σωστός προγραμματισμός είναι το κυριότερο συστατικό</td></tr>
</table>

	μιας πετυχημένης υλοποίησης ενός ΠΣ.
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Επιτάχυνση των διαδικασιών /μείωση χρόνου διεκπεραίωσης εργασιών: Είναι αρμοδιότητα του project managerva μπορέσει να βρει διορθωτικούς τρόπους αντιμετώπισης της χρονοκαθυστέρησης μιας εργασίας και να επιταχύνει τους ρυθμούς διεκπεραίωσης της αξιολογώντας την κρισιμότητα της στο συνολικό έργο.
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Ανάθεση έργου σε έμπειρη εταιρία υλοποίησης ΟΠΣ: Μια έμπειρη εταιρία υλοποίησης ΠΣ είναι σε θέση να γνωρίζει από την εμπειρία της τον ακριβή χρόνο υλοποίησης και να μπορεί ο εκάστοτε πελάτης να θέσει ρήτρες για την μη ικανοποίηση του χρονοδιαγράμματος.
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Εβδομαδιαία (εντός διάρκειας υλοποίησης)
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	(31/12/2013) Ημερομηνία διεκπεραίωσης του έργου.

#1 Φύλλο κινδύνου: Έργο εκτός ορίων χρονοπρογραμματισμού

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#2			Έργο εκτός ορίων οικονομικού πλάνου	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Επιπλέον χρηματοδότηση έργου	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Οργανωτικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Παρασκευόπουλος Α.	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο. 15%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
10%-20%	Καταστροφική 236.573,36€	35.486,004€	1	11/03/2013
	ΣΥΝΟΛΟ:	35.486,004€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Έλεγχος προϋπολογισμού του έργου :Πρέπει να υπάρχει λεπτομερής παρακολούθηση των διαδικασιών και η χρηματική δαπάνη για κάθε εργασία να είναι καταγεγραμμένη από την αρχή.
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Επιπλέον έξοδα από τα προβλεπόμενα.
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή :Η αποφυγή του κινδύνου αυτού είναι ο πρώτος στόχος , όμως σε περίπτωση που μια εργασία βγει εκτός ορίου του οικονομικού πλάνου , θα πρέπει να μειωθεί ο προϋπολογισμός μιας δευτερεύοντος σημασίας εργασίας για να μπορεί να ισοσταθμιστεί το μέγεθος του κόστους.
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Πλήρης οικονομικός προγραμματισμός
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Οικονομικές περικοπές σε εργασίες που μπορούν να προγραμματιστούν στο μέλλον χωρίς την διακοπή του έργου.
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Ανάθεση έργου υλοποίησης σε εξωτερική εταιρία με αποδοχή του χρηματικού πλάνου και καταβολής χρηματικού προστίμου (ρήτρας) κατά την απόκλιση του οικονομικού πλάνου. Θα πρέπει η εταιρία υλοποίησης του έργου να επωμιστεί το επιπλέον χρηματικό κόστος.
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Εβδομαδιαία (εντός διάρκειας υλοποίησης)
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	(31/12/2013) Ημερομηνία διεκπεραίωσης του έργου

#2 Φύλλο κινδύνου: Έργο εκτός ορίων οικονομικού πλάνου

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#3			Άρνηση προσωπικού στις τεχνολογικές αλλαγές	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Άρνηση υιοθέτησης τεχνολογίας	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Οργανωτικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Υπεύθυνος Ασφαλείας / Διοίκηση οργανισμού	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο. 15%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
10%-20%	236.573,36€	35.486,004€	1	11/03/2013
	ΣΥΝΟΛΟ:	35.486,004€		
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Άρνηση υιοθέτησης της τεχνολογίας : Βρίσκοντας συνεχώς "προβλήματα" στο καινούριο ΠΣ με σκοπό την περιθωριοποίηση του.			
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Συνέχιση εργασιών με παλιότερες συνηθισμένες μεθόδους χωρίς να χρησιμοποιούν το καινούριο ΠΣ που είναι διαθέσιμο στην εταιρία.			
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή :θα πρέπει να γίνει αποφυγή της συγκεκριμένης κατάστασης ,διότι είναι ένας από τους λόγους αποτυχίας ενός έργου.			
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013			
(Προαιρετική συμπλήρωση)				
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	1)Εκπαίδευση χρηστών για την σαφή κατανόηση του καινούργιου ΠΣ και την κατανόηση της ταχύτερης απόκρισης για τις ανάγκες της εταιρίας 2)επιβράβευση των χρηστών για τους χρόνους απόκρισης του καινούριου ΠΣ 3)Bonusπαραγωγικότητας : Δίνοντας κίνητρο να εντάξουν τις καινούριες διαδικασίες στην εργασία τους με σκοπό την γρηγορότερη παραγωγική διαδικασία.			
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Επιπλέον εκπαιδεύσεις / απόρριψη παλαιότερων μεθόδων εργασίας			

ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Εργασία με δύο εναλλακτικούς τρόπους μέχρι την πλήρη κατανόηση του καινούργιου ΟΠΣ από τους χρήστες με ένα χρονικό περιθώριο.
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή εντός διάρκειας υλοποίησης /training /livetou έργου
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	01/06/2014 (5 Μήνες μετά το Livetou πληροφοριακού συστήματος)

#3 Φύλλο κινδύνου: Άρνηση προσωπικού στις τεχνολογικές αλλαγές

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#4			Κίνδυνος πυρκαγιάς	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Φωτιά στις εγκαταστάσεις του οργανισμού	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Φυσικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Υπεύθυνος Ασφαλείας	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗΜ.Ο 0.5%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
<10%	236.573,36€	11.828,668€	2	11/03/2013
	ΣΥΝΟΛΟ:	11.828,668€		
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Αισθητήρες Πυρασφάλειας και αισθητήρες θερμοκρασίας μέσα στο server room του ΠΣ.			
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Alert / συναγερμός πυρόσβεσης			
ΣΤΡΑΤΗΓΙΚΗ	Αποφυγή			

ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	1)Πυρασφάλεια στους χώρους της εγκατάστασης και αυτόματη ενεργοποίηση σε περίπτωση μεγάλης θερμοκρασίας.2) Πυροσβεστήρες σε διαφορετικά μέρη της εγκατάστασης για μικρές εστίες φωτιάς και αποφυγή της εξάπλωσης της.
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Τα Ασφαλιστικά μέτρα είναι αναγκαία στον συγκεκριμένο κίνδυνο ,για τον λόγο ότι σε περίπτωση πυρκαγιάς θα υπάρξουν καταστροφικές συνέπειες όχι μόνο για το ΠΣ αλλά και για τις κτηριακές εγκαταστάσεις.
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#4 Φύλλο κινδύνου: Κίνδυνος πυρκαγιάς

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ	
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#5	Κίνδυνος σεισμικής δόνησης
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ	Σεισμική δόνηση στην ευρύτερη περιοχή της εγκατάστασης.
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:	Φυσικός κίνδυνος
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:	01/01/2013
ΥΠΘΥΘΥΝΟΣ:	Υπεύθυνος Ασφαλείας
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ	

ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο.5%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
<10%	236.573,36€	11.828,668€	2	11/03/2013
	ΣΥΝΟΛΟ:	11.828,668€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Παρακολούθηση της σεισμικής δραστηριότητας της περιοχής .
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Σεισμογενής περιοχή εγκατάστασης ΟΠΣ. Η περιοχή εγκατάστασης του ΠΣ δεν είναι σεισμογενής.
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Αντισεισμικά Μέτρα στις εγκαταστάσεις .
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	1)Backupσε διαφορετικό χώρο εκτός εγκατάστασης είναι ένας τρόπος να κρατήσουμε τα δεδομένα μας ασφαλή χωρίς όμως να διασφαλίσουμε την ακεραιότητα του ΠΣ στο σύνολο του 2) ασφαλιστικά μέτρα για την αποκατάσταση των υλικών ζημιών του ΠΣ
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	Ασφαλιστικά μέτρα.

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Απρόβλεπτος κίνδυνος
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#5 Φύλλο κινδύνου: Κίνδυνος σεισμικής δόνησης

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#6			Κίνδυνος πλημύρας	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Εισροή υδάτων από μεγάλη νεροποντή , είτε από διαρροή υδάτων μέσα στις εγκαταστάσεις.	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Φυσικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Υπεύθυνος Ασφαλείας	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο. 5%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
<10%	236.573,36€	11.828,668€	2	11/03/2013
	ΣΥΝΟΛΟ:	11.828,668€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Μορφολογία του εδάφους για την κατεύθυνση των υδάτων βάση της κλίσης .
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	1)Ακραία καιρικά φαινόμενα βάση μετεωρολογικών προβλέψεων για την περιοχή 2) παλαιές εγκαταστάσεις σωληνώσεων (σκουριασμένες /ασυντήρητες / φθαρμένες) στην ευρύτερη περιοχή ή εντός του συγκροτήματος της εταιρίας.
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	20/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	1)Υπερυψωμένοdatacenter 2)Μελέτη κλίσης δαπέδου από ειδικούς 3)ανοιχτές-καθαρές υδρορροές εντός και εκτός εγκαταστάσεων 4)datacenterαπομακρυσμένο από σωληνώσεις υδροδότησης (σε περίπτωση διαρροής)
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Backupσε διαφορετικό χώρο εκτός εγκατάστασης.
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ	Ασφαλιστικά μέτρα.

ΜΕΤΑΠΤΩΣΗΣ:	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#6 Φύλλο κινδύνου: Κίνδυνος πλημύρας

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#7			Κίνδυνος κεραυνού	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Χτύπημα κεραυνού στις εγκαταστάσεις του ΟΠΣ.	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Φυσικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Υπεύθυνος Ασφαλείας	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο. 5%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
<10%	236.573,36€	11.828,668€	2	11/03/2013
	ΣΥΝΟΛΟ:	11.828,668€		
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Πρόγνωση καιρικών συνθηκών στην περιοχή εγκατάστασης.			
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Ακραία καιρικά φαινόμενα			
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή			
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	20/03/2013			

(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Αλεξικέραυνο / μονωτικά μέτρα
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Backupσε διαφορετικό χώρο εκτός εγκατάστασης
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	Ασφαλιστικά μέτρα
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Απρόβλεπτος κίνδυνος
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#7 Φύλλο κινδύνου: Κίνδυνος κεραυνού

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ	
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#8	Παρεμβολές στις επικοινωνίες από καιρικά φαινόμενα
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ	Παρεμβολές στις επικοινωνίες από ακραία καιρικά φαινόμενα . Στις εγκαταστάσεις της εταιρίας λόγο της απομακρυσμένης επικοινωνίας Μαγούλα – Μάντρα μέσω καλωδιώσεων / μισθωμένων γραμμών είτε με ασύρματες επικοινωνίες.
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:	Φυσικός κίνδυνος
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:	01/01/2013
ΥΠΘΥΘΥΝΟΣ:	Τεχνικός υπεύθυνος

ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο. 5%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
20%-50%		<250€	4	11/03/2013
	ΣΥΝΟΛΟ:	<250€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Τοπικές καιρικές προγνώσεις.
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Ακραία καιρικά φαινόμενα
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Μείωση: Σκοπός είναι να μειωθεί ο χρόνος επαναφοράς των συνδέσεων σε περίπτωση που χαθεί κάποια επικοινωνία .
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	20/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	1)Έμπιστος πάροχος μίσθωσης 2) Ενίσχυση των ασύρματων σημάτων γ
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Άμεση αποκατάσταση επικοινωνιών από πάροχο
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Ενσύρματες και ασύρματες επικοινωνίες αντίστοιχα μπορούν να δώσουν την λύση σε μια επικείμενη κατάσταση αλλάζοντας τον τρόπο επικοινωνίας πχ σε ενσύρματο εάν οι ασύρματες επικοινωνίες έχουν επιπλοκές.
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Απρόβλεπτος κίνδυνος
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#8 Φύλλο κινδύνου: Παρεμβολές στις επικοινωνίες από καιρικά φαινόμενα

➢ ΠΕΡΙΓΡΑΦΗ	➢ ΤΙΜΗ
➢ Α1)Διαχείριση αποθήκης	➢ 9.000,00€
➢ Α2)Διαχείριση παραγωγής	➢ 12.000,00€
➢ Α3)Διαχείριση Πωλήσεων	➢ 6.000,00€
➢ Α4)Διαχείριση Εισπράξεων	➢ 2.500,00€
➢ Α5)Διαχείριση Αγορών	➢ 4.000,00€
➢ Α6)Διαχείριση Πληρωμών	➢ 2.000,00€
➢ Α7)Διαχείριση Παγίων	➢ 1.500,00€
➢ Α8)Πληροφοριακό Σύστημα Διοίκησης	➢ 5.000,00€
➢ Α9)Μισθοδοσία	➢ 5.000,00€
➢ Α10)κύκλωμα ωρομέτρησης	➢ 3.000,00€
➢ Α11)διαχείριση πρωτοκόλλου	➢ 4.000,00€
➢ Α12)Γενική-Αναλυτική λογιστική	➢ 2.500,00€
ΣΥΝΟΛΟ:56.000.00€	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ	
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#9	Δυσλειτουργία/αστοχία Υλικού
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ	Παραλαβή ελαττωματικού hardwareαπό προμηθευτή /αστοχία hardwareστην διασύνδεση του με το πληροφοριακό σύστημα στο σύνολο του.
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:	Τεχνολογικός κίνδυνος
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:	01/01/2013

ΥΠΘΥΘΥΝΟΣ:				Τεχνικός υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ					
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ		ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο.5%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
Α1	<10%	ΣΥΝΟΛΟ:56.000.00€	450,00€	3	11/03/2013
Α2	<10%		600,00€		
Α3	<10%		300,00€		
Α4	<10%		100,00€		
Α5	<10%		200,00€		
Α6	<10%		100,00€		
Α7	<10%		50,00€		
Α8	<10%		250,00€		
Α9	<10%		250,00€		
Α10	<10%		150,00€		
Α11	<10%		200,00€		
Α12	<10%		125,00€		
		ΣΥΝΟΛΟ	2,800€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	1) Έλεγχος των hardware που παραλαμβάνει η εταιρία για τυχών χτυπήματα κατά την μεταφορά. 2)Δοκιμή συστήματος κατά την διάρκεια υλοποίησης του έργου
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Μη λειτουργία υλικού (Hardware)
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Μείωση ή Αποφυγή
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	06/11/2012
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Εύρεση αξιόπιστου προμηθευτή/ συντήρηση
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Συμβόλαια συντήρησης με την εταιρία προμήθειας
ΕΝΑΛΛΑΚΤΙΚΟ	Εύρεση εναλλακτικού προμηθευτή με βάση την απόκριση

ΣΧΕΔΙΟ:	
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Πριν το live του έργου / καθημερινή
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#9 Φύλλο κινδύνου: Δυσλειτουργία/αστοχία Υλικού

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#10			Αστοχία μέσων αποθήκευσης	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Δυσλειτουργία συστήματος αποθήκευσης	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Τεχνολογικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Τεχνικός υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο.35%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
20%-50%	5,000,00€	250,00€	4	11/03/2013
	ΣΥΝΟΛΟ:	250,00€		
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Log Files			
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Χαμένα παλαιά αρχεία ή κατεστραμμένα και δεν μπορεί να γίνει επαναφορά τους σε περίπτωση που χρειαστεί.			
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Μείωση - Αποφυγή			
ΗΜΕΡΟΜΗΝΙΑ	11/11/2012			

ΕΝΗΜΕΡΩΣΗΣ:	
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Back up Files /extra drives /mirror drives /disaster plan
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Συμβόλαιο συντήρησης
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Reverse to Last good Back up
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#10 Φύλλο κινδύνου: Αστοχία μέσων αποθήκευσης

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#11			Γήρανση / συντήρηση εξοπλισμού	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Φθορά εξοπλισμού λόγο παλαιότητας	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Τεχνολογικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Τεχνικός υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	Έκθεση για τα επόμενα 5 χρόνια λειτουργίας Μ.Ο.= 0.5% βάση του συνολικού εξοπλισμού	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
<10%	Συνολικός εξοπλισμός	2,800€	3	11/03/2013

	hardware ΣΥΝΟΛΟ:56.000.00€			
	ΣΥΝΟΛΟ:	2,800€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Θόρυβος μηχανημάτων server room / Τεστ μηχανημάτων (UPSκ.τ.λ.)
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	απρόβλεπτη υπερθέρμανση μηχανημάτων / Προειδοποιητικά signalsσε μπαταρίες κ.α.
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Μείωση
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Συντήρηση εξοπλισμού
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Ειδικά καθαριστικά εργαλεία / ανανέωση παλαιωμένου-φθαρμένου εξοπλισμού
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Επέκταση εγγύησης / συμβόλαια συντήρησης
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	Άμεση απόκριση προσωπικού /SLAπρομηθευτών.

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Μηνιαία
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#11 Φύλλο κινδύνου: Γήρανση / συντήρηση εξοπλισμού

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#12			καταστροφή ηθελημένη / ακούσια εξοπλισμού	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Καταστροφή εξοπλισμού	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Ανθρώπινος κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Υπεύθυνος Ασφαλείας	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο. 35%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
20%-50%	250 έως 1000€	87.5€-350€	4	11/03/2013
	ΣΥΝΟΛΟ:	Μ.Ο.218,75€		
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:				
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Απειρία χρηστών / δυσαρεστημένοι χρήστες / κακός καθαρισμός από συνεργείο καθαρισμού			
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Μείωση			
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013			
(Προαιρετική συμπλήρωση)				
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Ενημέρωση χρηστών για τυχών ζημίες / ενημέρωση συνεργείου καθαρισμό για τον τρόπο καθαρισμού και τους χώρους ευθύνης του			
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Extra storage για τα καθημερινές (μικρές) αντικαταστάσεις / συμβόλαιο συντήρησης			
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-			
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-			
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ				
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή			

ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#12 Φύλλο κινδύνου: καταστροφή ηθελημένη / ακούσια εξοπλισμού

Καταγραφή Δυσλειτουργιών Λογισμικού

➢ ΠΕΡΙΓΡΑΦΗ	➢ ΤΙΜΗ
➢ B1)Database standard edition 10gx40	➢ 5.020,00€
➢ B2)Internet Application server(IAS)Enterprise editionx40	➢ 10.040,00€
➢ B3)Business intelligence standard edition one x5	➢ 2.152,50€
➢ B4)Internet development suite	➢ 6.659,20€
➢ B5)Φορολογικός Μηχανισμός	➢ 2.700,00€
➢ ΣΥΝΟΛΟ:26.571,70€	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ

ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#13	Αστοχία λογισμικού
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ	Αστοχία εγκατάστασης/παραμετροποίησης από τους υπεύθυνους εγκατάστασης. Ο συγκεκριμένος κίνδυνος εστιάζει στις

<table>
<tr><td colspan="4"></td><td colspan="2">παραμετροποιήσεις που θα δεχτεί το ΟΠΣ για να προσαρμοστεί στην συγκεκριμένη εταιρία.</td></tr>
<tr><td colspan="4">ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:</td><td colspan="2">Τεχνολογικός Κίνδυνος</td></tr>
<tr><td colspan="4">ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:</td><td colspan="2">01/01/2013</td></tr>
<tr><td colspan="4">ΥΠΘΥΘΥΝΟΣ:</td><td colspan="2">Τεχνικός Υπεύθυνος</td></tr>
<tr><td colspan="4">ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ</td><td colspan="2"></td></tr>
<tr><td colspan="2">ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ</td><td>ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ</td><td>ΈΚΘΕΣΗ (Μ.Ο. 5%)</td><td>ΠΡΟΤΕΡΑΙΟΤΗΤΑ</td><td>ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ</td></tr>
<tr><td>Β1</td><td><10%</td><td rowspan="5">26.571,70€</td><td>250,00€</td><td rowspan="6">2</td><td rowspan="6">11/03/2013</td></tr>
<tr><td>Β2</td><td><10%</td><td>500,00€</td></tr>
<tr><td>Β3</td><td><10%</td><td>100,00€</td></tr>
<tr><td>Β4</td><td><10%</td><td>300,00€</td></tr>
<tr><td>Β5</td><td><10%</td><td>135,00€</td></tr>
<tr><td colspan="2"></td><td>ΣΥΝΟΛΟ:</td><td>1300,00€</td></tr>
<tr><td colspan="6">ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ</td></tr>
<tr><td colspan="2">ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:</td><td colspan="4">1)καθημερινή παρακολούθηση των συμβούλων κατά την δημιουργία παραμετροποίησης σύμφωνα με τα ζητούμενα της εταιρίας 2)Δοκιμή λογισμικού μετά τις παραμετροποιήσεις</td></tr>
<tr><td colspan="2">ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:</td><td colspan="4">Μη λειτουργία λογισμικού στην δοκιμαστική περίοδο.</td></tr>
<tr><td colspan="2">ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:</td><td colspan="4">Μείωση ή Αποφυγή</td></tr>
<tr><td colspan="2">ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:</td><td colspan="4">06/11/2012</td></tr>
<tr><td colspan="6">(Προαιρετική συμπλήρωση)</td></tr>
<tr><td colspan="2">ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:</td><td colspan="4">Εύρεση αξιόπιστου προμηθευτή ΟΠΣ με εμπειρία στις παραμετροποιήσεις λογισμικού και έμπειρους προγραμματιστές με αντίστοιχες εμπειρίες παραμετροποιήσεων</td></tr>
<tr><td colspan="2">ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:</td><td colspan="4">-</td></tr>
<tr><td colspan="2">ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:</td><td colspan="4">Πρόσληψη εναλλακτικών (εξωτερικών) συμβούλων / προγραμματιστών σε τυχών λανθασμένες παραμετροποιήσεις λογισμικού.</td></tr>
</table>

ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή στην διάρκεια της υλοποίησης (Οι παραμετροποιήσεις του κώδικα μπορεί να γίνουν και μετά την χρονική παράδοση του ΟΠΣ στην εταιρία)
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#13 Φύλλο κινδύνου: Αστοχία λογισμικού

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#14			Δυσλειτουργία λογισμικού /κακή ρύθμιση / μη συμβατότητα	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Δυσλειτουργία(crash)/κακή ρύθμιση /μη συμβατότητα λογισμικού εγκατάστασης κυρίως στους servers του πληροφοριακού συστήματος αλλά και στους τελικούς χρήστες	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Τεχνολογικός Κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			01/01/2013	
ΥΠΘΥΘΥΝΟΣ:			Τεχνικός υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	Έκθεση	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
B1<10%	26.571,70€	250,00€	3	11/03/2013
B2<10%		500,00€		
B3<10%		100,00€		
B4<10%		300,00€		
B5<10%		135,00€		

	ΣΥΝΟΛΟ:	1.300,00€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	1)system alert σε περίπτωση πτώσης servertou ΟΠΣ 2)Monitoringλειτουργιών μέσω reportstou συστήματος
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	1)Μη σωστή λειτουργία του πληροφοριακού συστήματος 2)System error3)ανυπαρξία συστήματος σε σοβαρό πρόβλημα του λογισμικού
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Έμπιστος προμηθευτής / επαγγελματικός έλεγχος και παραμετροποίηση
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	1)Συμβόλαια συντήρησης 2)extraάδειες λογισμικού 3)επανεγκατάσταση λογισμικού
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Αλλαγή προμηθευτή
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή :Κατά την διάρκεια υλοποίησης ΟΠΣ
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	31/12/2013

#14 Φύλλο κινδύνου: Δυσλειτουργία λογισμικού /κακή ρύθμιση / μη συμβατότητα

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#15			Κακόβουλο λογισμικό	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Αμέλεια προσωπικού/Εσκεμμένος (εξωτερικός παράγοντας)	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Ανθρώπινος / τεχνολογικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			07/11/2012	
ΥΠΘΥΘΥΝΟΣ:			Τεχνικός υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο. 5%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
<10%	ΣΥΝΟΛΟ:26.571,70€ Λογισμικού	1328,585€	3	11/03/2013
	ΣΥΝΟΛΟ:	1328,585€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Παρακολούθηση ενεργειών προσωπικού /Συστήματα Antivirus
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Security alert /Antivirus
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Ελαχιστοποίηση
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	07/11/2012
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Μέτρα παρακολούθησης / Εκπαίδευση Προσωπικού /Απενεργοποίηση USB port Αποκοπή δικαιωμάτων ανά χρήστη/Πολιτικές Ασφαλείας
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Updated Antivirus systems
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	Recovery system /back up

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή /Scanning ΟΠΣ
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#15 Φύλλο κινδύνου: Κακόβουλο λογισμικό

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#16			Παρεμβολές	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Παρεμβολές σήματος από κεραίες κ.α.	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Τεχνολογικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			11/03/2013	
ΥΠΘΥΘΥΝΟΣ:			Τεχνικός υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
-	-	-	-	11/03/2013
	ΣΥΝΟΛΟ:			
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Μελέτη περιοχή εγκατάστασης ΟΠΣ στην αρχή της εγκατάστασης αλλά και κατά την διάρκεια.			
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Κακή επικοινωνία τηλεπικοινωνιών και ψηφιακών μέσων επικοινωνίας			
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή			
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013			
(Προαιρετική συμπλήρωση)				

ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Έλεγχος περιοχής εγκατάστασης
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Απομόνωση θορύβου και ενίσχυση σήματος
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Ενσύρματες επικοινωνίες σε περίπτωση παρεμπόδισης των ασύρματων επικοινωνιών
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#16 Φύλλο κινδύνου: Παρεμβολές

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#17			Διακοπή επικοινωνίας συστημάτων	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Διακοπή επικοινωνίας συστημάτων εντός εγκατάστασης π.χ. συστημάτων παραγωγής / τιμολόγησης	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Τεχνολογικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			20/03/2013	
ΥΠΟΥΘΥΝΟΣ:			Τεχνικός υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
10%-20%		1η ώρα 1000€	1η ώρα προτεραιότητα 4 2η ώρα προτεραιότητα 3 3η 4η ώρα προτεραιότητα 2	11/03/2013
		2η ώρα 2000€		
		3η ώρα 3000€		
		4η ώρα 4000€		
		5η ώρα 5000€		

	ΣΥΝΟΛΟ:	15.000€ σε 5 ώρες	5η ώρα προτεραιότητα 1	

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	1)System error και documentsνα μην μπορούν να μεταφερθούν από το ένα σύστημα στο άλλο με συνέπεια να είναι κολλημένα 2) Έλεγχος σκληρών δίσκων για την κατάσταση των δεδομένων 3)Μηνύματα σφάλματος (error messages).
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	1) Αργό σύστημα στις διαδικασίες 2) Πτώση servertου συστήματος 3)Υπερχειλίσει δεδομένων λόγο υπερφόρτωσης server
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Μείωση
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	20/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	1)Συμβόλαια συντήρησης με ρήτρες ανάλογα με την ώρα που δεν υπάρχει σύστημα.2)Εφεδρικούς serversμικρότερης ισχύος σε περίπτωση που οι κεντρικοί serversέχουν κάποιο πρόβλημα είτε softwareείτε hardware και αλλαγή των εταιρικών διαδικασιών σε αυτούς.
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	1)Restart - server / router / ενδιάμεσων μέσων2)Έλεγχος καλωδιώσεων
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Αλλαγή αυτοματοποιημένης διαδικασίας σε χειροκίνητη.
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	Χειροκίνητη διαδικασία , περνώντας τα δεδομένα που μπορεί να έχουν κολλήσει με χειροκίνητο τρόπο μέχρι να αποκατασταθεί η επικοινωνία των συστημάτων.
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#17 Φύλλο κινδύνου: Διακοπή επικοινωνίας συστημάτων

<table>
<tr><th colspan="5">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ</th></tr>
<tr><td colspan="3">ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#18</td><td colspan="2">Διακοπή ηλεκτροδότησης</td></tr>
<tr><td colspan="3">ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ</td><td colspan="2">Διακοπή ηλεκτρικού ρεύματος εγκαταστάσεων</td></tr>
<tr><td colspan="3">ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:</td><td colspan="2">Τεχνολογικός κίνδυνος</td></tr>
<tr><td colspan="3">ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:</td><td colspan="2">20/03/2013</td></tr>
<tr><td colspan="3">ΥΠΘΥΘΥΝΟΣ:</td><td colspan="2">Τεχνικός Υπεύθυνος</td></tr>
<tr><td colspan="3">ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ</td><td colspan="2"></td></tr>
<tr><td>ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ</td><td>ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ</td><td>ΈΚΘΕΣΗ</td><td>ΠΡΟΤΕΡΑΙΟΤΗΤΑ</td><td>ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ</td></tr>
<tr><td>10%-20%</td><td rowspan="5">Η διακοπή της ηλεκτροδότησης σημαίνει διακοπή όλων των διαδικασιών που έχει μια εταιρία. Σημαίνει διακοπή των παραγγελιών-φορτώσεις και ξεφορτώσεις των φορτηγών ,διακοπή της παραγωγικής διαδικασίας κ.α. Με συνέπεια να υπάρχει μεγάλη οικονομική ζημία όταν θα υπάρχει μεγάλο χρονικό διάστημα διακοπής.</td><td>1η ώρα 1000€</td><td rowspan="5">1η ώρα προτεραιότητα 4
2η ώρα προτεραιότητα 3
3η 4η ώρα προτεραιότητα 2
5η ώρα προτεραιότητα 1</td><td rowspan="5">20/03/2013</td></tr>
<tr><td></td><td>2η ώρα 2000€</td></tr>
<tr><td></td><td>3η ώρα 3000€</td></tr>
<tr><td></td><td>4η ώρα 4000€</td></tr>
<tr><td></td><td>5η ώρα 5000€</td></tr>
<tr><td></td><td>ΣΥΝΟΛΟ:</td><td>15.000€ σε 5 ώρες</td></tr>
<tr><td colspan="5">ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ</td></tr>
<tr><td colspan="2">ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:</td><td colspan="3">-</td></tr>
<tr><td colspan="2">ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:</td><td colspan="3">Απότομες αλλαγές τάσης</td></tr>
<tr><td colspan="2">ΣΤΡΑΤΗΓΙΚΗ</td><td colspan="3">Αποφυγή</td></tr>
</table>

ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	20/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	1)Γεννήτρια ρεύματος σε εξωτερικό χώρο της εταιρίας σε περίπτωση που υπάρχει πτώση του ηλεκτρικού ρεύματος της περιοχής.2)Χρησιμοποίηση ups για την προσωρινή διακοπή ή τις μικρές αλλαγές της τάσης.
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Ενημέρωση ηλεκτρικού παρόχου έγκαιρα .
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή παρακολούθηση
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#18 Φύλλο κινδύνου: Διακοπή ηλεκτροδότησης

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#19			Διακοπή Κλιματισμού εγκατάστασης	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Διακοπή κλιματισμού εγκατάστασης ΟΠΣ με αποτέλεσμα υπερθέρμανσης και διακοπής της λειτουργίας του μέχρι την αποκατάσταση του.	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Τεχνολογικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			11/03/2013	
ΥΠΘΥΘΥΝΟΣ:			Τεχνικός υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ

10%-20%		1η ώρα 1000€	1η ώρα προτεραιότητα 4 2η ώρα προτεραιότητα 3 3η 4η ώρα προτεραιότητα 2 5η ώρα προτεραιότητα 1	11/03/2013
		2η ώρα 2000€		
		3η ώρα 3000€		
		4η ώρα 4000€		
		5η ώρα 5000€		
	ΣΥΝΟΛΟ:	15.000€ σε 5 ώρες		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Θερμόμετρο στο server room (θερμόμετρο δωματίου) που θα μετράει την θερμοκρασία σε περίπτωση που δεν είναι στα κανονικά επίπεδα.
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Alarmσε περίπτωση αύξησης της θερμοκρασίας του server room.
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Συχνή συντήρηση κλιματισμού και
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Εγγύηση συστημάτων κλιματισμού και άμεση αντικατάσταση από εξωτερική εταιρία συντήρησης .
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Εναλλακτικός κλιματισμός εντός του χώρου του ΠΣ.
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	καθημερινή
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#19 Φύλλο κινδύνου: Διακοπή Κλιματισμού εγκατάστασης

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#20			Μη ομαλή μετάπτωση δεδομένων από παλαιότερο σύστημα	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Η μετάπτωση των παλαιών δεδομένων στο καινούριο σύστημα θα πρέπει να είναι ακριβής για την αποφυγή επαναδημιουργίας των δεδομένων που θα βγάλει το έργο εκτός χρονοδιαγράμματος.	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Τεχνολογικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			11/03/2013	
ΥΠΘΥΘΥΝΟΣ:			Τεχνικός Υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ		ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
	Η προβληματική μετάπτωση παλαιών δεδομένων στο καινούριο πληροφοριακό σύστημα , θα προκαλέσει αποτυχία της υλοποίησης του ΟΠΣ με συνέπεια να μην προχωρήσει η διαδικασία εγκατάστασης. Οι συνέπειες θα είναι καταστροφικές βάση του ότι το έργο θα αποτύχει.		1	11/03/2013
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Testσε παρόμοιο περιβάλλον εγκατάστασης πριν την εφαρμογή του καινούριου συστήματος την ημέρα έναρξης toulive .			
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	1) Λανθασμένη μετάπτωση στο testπεριβάλλον (virtual) που θα τρέχει πριν την μετάπτωση στο κανονικό σύστημα.2)Λανθασμένα reports με μη αντικειμενικά δεδομένα			
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή			
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013			
(Προαιρετική συμπλήρωση)				
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Αξιόπιστος συνεργάτης με εμπειρία στην υλοποίηση πληροφοριακών			

	συστημάτων
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Αλλαγή συνεργατών outsourcing που θα είναι υπεύθυνοι για την καλή λειτουργία του συστήματος και συνεπώς για την μετάπτωση των δεδομένων.
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	2 μήνες πριν αρχίσει να λειτουργεί το σύστημα .
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	3 μήνες μετά το τέλος του έργου.

#20 Φύλλο κινδύνου: Μη ομαλή μετάπτωση δεδομένων από παλαιότερο σύστημα

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#21			Υποκλοπή /αλλοίωση / καταστροφή πληροφοριών	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Υποκλοπή /αλλοίωση / καταστροφή πληροφοριών από υπαλλήλους της εταιρίας	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Θεσμικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			11/03/2013	
ΥΠΘΥΘΥΝΟΣ:			Υπεύθυνος Ασφαλείας	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ		ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
	Δεν μπορεί να μετρηθεί με βάση το κόστος .Η Υποκλοπή-αλλοίωση-καταστροφή πληροφοριών μπορεί να αποφέρει τεράστια ζημία όχι μόνο στο πληροφοριακό σύστημα αλλά στην εταιρία στο σύνολό της.		1	11/03/2013
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ	Παρακολούθηση ενεργειών προσωπικού(Event logs) /κάμερες			

ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	παρακολούθησης χώρων εντός του Π.Σ και μη.
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Event logs Alert
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Μέτρα παρακολούθησης / Εκπαίδευση Προσωπικού / Δέσμευση προσωπικού με υπογραφή συμβάσεως για την διασφάλιση εταιρικών δεδομένων με νομικές συνέπειες κατά την παράβαση.
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Back up σημαντικών αρχείων
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Καθημερινή
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#21 Φύλλο κινδύνου: Υποκλοπή /αλλοίωση / καταστροφή πληροφοριών

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ	
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#22	Διαρροή προσωπικών δεδομένων / Διαρροή εταιρικών μυστικών και διαδικασιών
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ	Αμέλεια προσωπικού/Εσκεμμένο

ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Θεσμικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			07/11/2012	
ΥΠΘΥΘΥΝΟΣ:			Υπεύθυνος Ασφαλείας	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ		ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
	Δεν μπορεί να μετρηθεί με βάση το κόστος .Η Διαρροή προσωπικών δεδομένων / Διαρροή εταιρικών μυστικών και διαδικασιών μπορεί να αποφέρει τεράστια ζημία όχι μόνο στο πληροφοριακό σύστημα αλλά στην εταιρία στο σύνολό της.		1	11/03/2013

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	Παρακολούθηση ενεργειών προσωπικού(Event logs)
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Event logs Alert / ανάλογες κινήσεις ανταγωνιστών στον κλάδο της εταιρίας λόγο διαρροής πληροφοριών
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	07/11/2012
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Μέτρα παρακολούθησης / Εκπαίδευση Προσωπικού / Δέσμευση προσωπικού με υπογραφή συμβάσεως για την διασφάλιση εταιρικών δεδομένων με νομικές συνέπειες κατά την παράβαση.
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Εντοπισμός και απόλυση εργαζόμενου που δεν εφαρμόζει τους κανόνες ασφαλείας της εταιρίας.
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Αν είναι για εταιρικά μυστικά που έχουν διαρρεύσει η αλλαγή στρατηγικής της εταιρίας είναι ένα εναλλακτικό σχέδιο.
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	1 ημέρα / εβδομάδα

ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#22 Φύλλο κινδύνου: Διαρροή προσωπικών δεδομένων / Διαρροή εταιρικών μυστικών και διαδικασιών

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#23			Λάθος εξουσιοδοτήσεις σε χρήστες	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Λάθος εξουσιοδοτήσεις σε χρήστες με αρμοδιότητες παραπάνω των καθηκόντων τους για παράδειγμα : εγκρίσεις εντολών αγοράς μέσω πληροφοριακού συστήματος.	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Ανθρώπινος / οργανωτικός κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			11/03/2013	
ΥΠΘΥΘΥΝΟΣ:			Υπεύθυνος Ασφαλείας	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ		ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
	Λάθος εξουσιοδοτήσεις σε χρήστες μπορεί να αποφέρει από μικρές ζημίες μέχρι καταστροφικές για το πληροφοριακό σύστημα και για την εταιρία στο σύνολό της.		1	11/03/2013
ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ				
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	1)Ενημέρωση στρατηγικών ομάδων με συγκεκριμένα δικαιώματα ανά ομάδα2) καταγραφή εξουσιοδοτήσεων του προσωπικού 3)Event logs για μη εξουσιοδοτημένη είσοδο στο σύστημα.			
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	Alertσε reportsγια μη εξουσιοδοτημένο χρήστη.			
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή			

ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	1)Group policies 2) στρατηγικές ομάδες υπευθύνων
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	1)Αποκοπή δικαιωμάτων ανά χρήστη 2)Πολιτικές Ασφαλείας σε τοπικό επίπεδο
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	Επιλογή υπευθύνου εξουσιοδοτήσεων και ανάθεσης καθηκόντων ανά χρήστη.
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Εβδομαδιαία
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

#23 Φύλλο κινδύνου: Λάθος εξουσιοδοτήσεις σε χρήστες

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ				
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:#24			Κλοπή λογισμικού / υλικού	
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ			Κλοπή λογισμικού / υλικού από τις εγκαταστάσεις της εταιρίας από εσωτερικούς ή εξωτερικούς συμβαλλόμενους.	
ΚΑΤΗΓΟΡΙΑ ΚΙΝΔΥΝΟΥ:			Ανθρώπινος κίνδυνος	
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΓΝΩΡΙΣΗΣ:			11/03/2013	
ΥΠΘΥΘΥΝΟΣ:			Τεχνικός Υπεύθυνος	
ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ				
ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΣΥΝΕΠΕΙΑ/ΕΠΙΠΤΩΣΗ	ΈΚΘΕΣΗ Μ.Ο.5%	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΗΜ/ΝΙΑ ΕΝΗΜΕΡΩΣΗΣ
<10%	Λογισμικό 26.571,70	1328,585€	3	11/03/2013

	ΣΥΝΟΛΟ:	1328,585€		

ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΟΥ	
ΔΕΙΚΤΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:	1)Καταγραφή σε καταλόγους η επιστροφή Λογισμικών / αδειών που δεν χρησιμοποιούνται για να μπορέσουν σε χρησιμοποιηθούν σε άλλους χρήστες που μπορεί να επιθυμούν πρόσβαση.2) καταγραφή και αποθήκευση του hardwareπου δεν χρησιμοποιείται.
ΠΡΟΠΟΜΠΟΣ ΚΙΝΔΥΝΟΥ:	1)Μη εξουσιοδοτημένη χρήση σε χρήστη που προσπαθεί να εισέλθει στο σύστημα.2) Μη έγκυρος κωδικός authenticationπου ήδη χρησιμοποιείται από άλλον χρήστη που δεν είναι εξουσιοδοτημένος 3)να μην υπάρχει στον τόπο εγκατάστασης το hardwareαλλά ούτε και να είναι καταγεγραμμένο σαν stock.
ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ:	Αποφυγή
ΗΜΕΡΟΜΗΝΙΑ ΕΝΗΜΕΡΩΣΗΣ:	11/03/2013
(Προαιρετική συμπλήρωση)	
ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ:	Καταγραφή των χρηστών και τι λογισμικά χρησιμοποιούν / καταγραφή hardwareπου χρησιμοποιούν και να είναι χρεωμένα ονομαστικά .
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ:	Ρήτρες για τυχών μη επιστροφή ή καταστροφή της εταιρικής περιουσίας από χρήστες που έχουν χρεωθεί συγκεκριμένο hardware.
ΕΝΑΛΛΑΚΤΙΚΟ ΣΧΕΔΙΟ:	-
ΣΧΕΔΙΟ ΜΕΤΑΠΤΩΣΗΣ:	-
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ	
ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Μηνιαία
ΚΑΤΑΣΤΑΣΗ:	Ανοιχτή κατάσταση
ΗΜΕΡΟΜΗΝΙΑ ΚΛΕΙΣΙΜΑΤΟΣ:	-

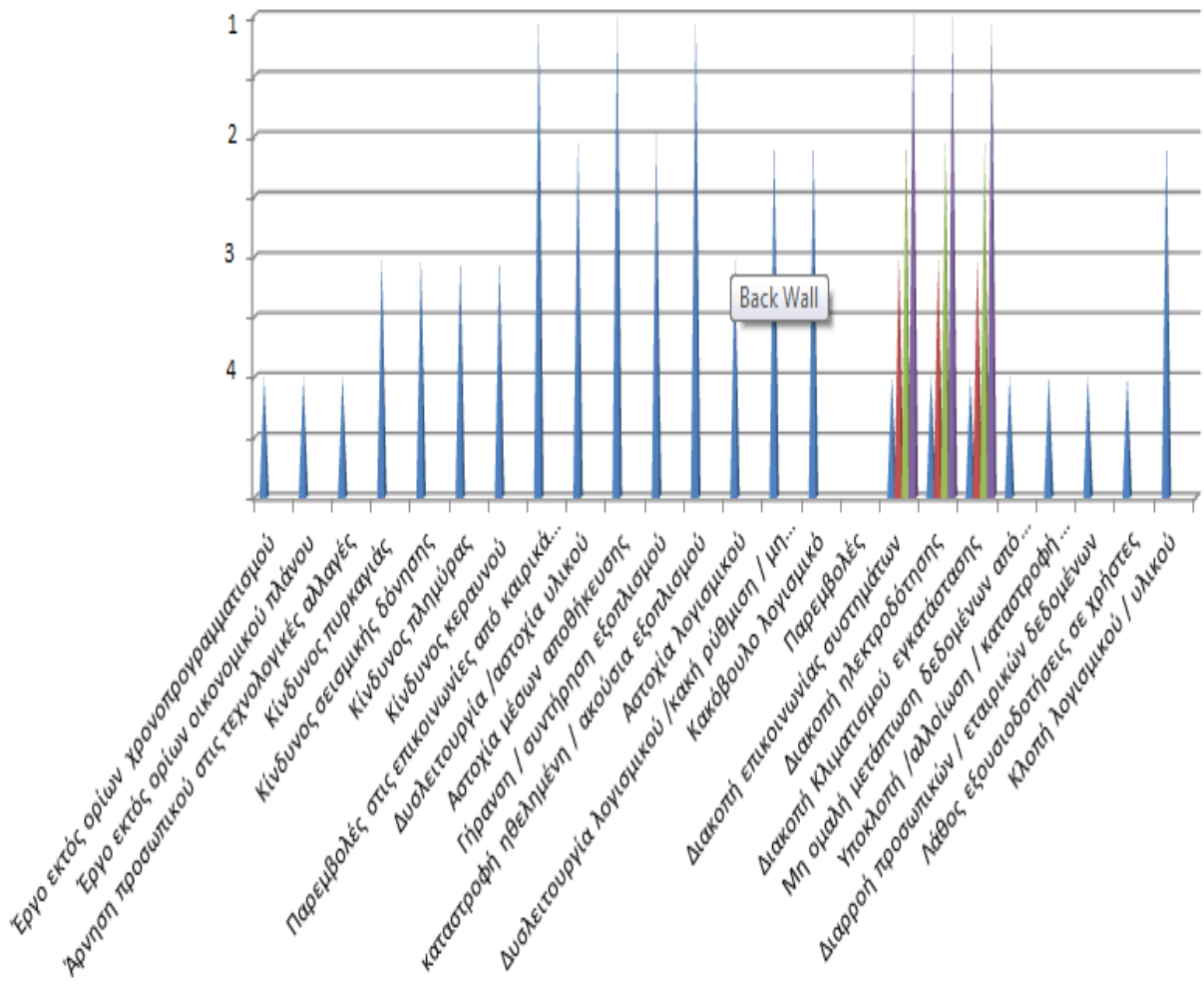
#24 Φύλλο κινδύνου: Κλοπή λογισμικού / υλικού

Συγκεντρωτικός πίνακας προτεραιοτήτων

Όνομα κινδύνου	Προτεραιότητα				Σχόλια
	1	2	3	4	
	Υψηλός κίνδυνος	Σημαντικός κίνδυνος	Μέτριος κίνδυνος	Μικρός κίνδυνος	
Έργο εκτός ορίων χρονοπρογραμματισμού	X				Οργανωτικός κίνδυνος
Έργο εκτός ορίων οικονομικού πλάνου	X				Οργανωτικός κίνδυνος
Άρνηση προσωπικού στις τεχνολογικές αλλαγές	X				Οργανωτικός κίνδυνος
Κίνδυνος πυρκαγιάς		X			Φυσικός κίνδυνος
Κίνδυνος σεισμικής δόνησης		X			Φυσικός κίνδυνος
Κίνδυνος πλημύρας		X			Φυσικός κίνδυνος
Κίνδυνος κεραυνού		X			Φυσικός κίνδυνος
Παρεμβολές στις επικοινωνίες από καιρικά φαινόμενα				X	Φυσικός κίνδυνος
Δυσλειτουργία /αστοχία υλικού			X		Τεχνολογικός κίνδυνος
Αστοχία μέσων αποθήκευσης				X	Τεχνολογικός κίνδυνος
Γήρανση / συντήρηση εξοπλισμού			X		Τεχνολογικός κίνδυνος
καταστροφή ηθελημένη / ακούσια εξοπλισμού				X	Ανθρώπινος κίνδυνος
Αστοχία λογισμικού		X			Τεχνολογικός κίνδυνος
Δυσλειτουργία λογισμικού /κακή ρύθμιση / μη συμβατότητα			X		Τεχνολογικός κίνδυνος
Κακόβουλο λογισμικό			X		Ανθρώπινος κίνδυνος /

					τεχνολογικός κίνδυνος
Παρεμβολές	**-**	**-**	**-**	**-**	**Τεχνολογικός κίνδυνος**
Διακοπή επικοινωνίας συστημάτων	**X (1η ώρα)**	**X (2η ώρα)**	**X (3η &4η ώρα)**	**X (5η ώρα)**	**Τεχνολογικός κίνδυνος**
Διακοπή ηλεκτροδότησης	**X (1η ώρα)**	**X (2η ώρα)**	**X (3η &4η ώρα)**	**X (5η ώρα)**	**Τεχνολογικός κίνδυνος**
Διακοπή Κλιματισμού εγκατάστασης	**X (1η ώρα)**	**X (2η ώρα)**	**X (3η &4η ώρα)**	**X (5η ώρα)**	**Τεχνολογικός κίνδυνος**
Μη ομαλή μετάπτωση δεδομένων από παλαιότερο σύστημα	**X**				**Τεχνολογικός κίνδυνος**
Υποκλοπή /αλλοίωση / καταστροφή πληροφοριών	**X**				**Θεσμικός κίνδυνος**
Διαρροή προσωπικών / εταιρικών δεδομένων	**X**				**Θεσμικός κίνδυνος**
Λάθος εξουσιοδοτήσεις σε χρήστες	**X**				**Ανθρώπινος κίνδυνος / οργανωτικός κίνδυνος**
Κλοπή λογισμικού / υλικού			**X**		**Ανθρώπινος κίνδυνος**

Πίνακας 19: Συγκεντρωτικός πίνακας προτεραιοτήτων



Εικόνα 5: Γράφημα αναγνώρισης κινδύνων

Συμπεράσματα

Με την ανάλυση της διαδικασίας διαχείρισης κινδύνων στο ολοκληρωμένο πληροφοριακό σύστημα της εταιρίας ανοξείδωτου χάλυβα που εξετάσαμε παραπάνω, μας έδωσε χρήσιμες πληροφορίες και εξάχθηκαν χρήσιμα συμπεράσματα για τον εντοπισμό και ανάλυσης των κινδύνων του έργου .Εξετάζοντας τους κινδύνους που επηρεάζουν αρνητικά τους στόχους του έργου μας δίνεται η δυνατότητα λήψης ενεργειών τόσο στην αρχή-σχεδιασμό του έργου όσο και κατά την διάρκειά του.

Με την βοήθεια των φύλλων κινδύνου έχουμε μια πλήρη εικόνα του κινδύνου που αντιμετωπίζουμε ή πρόκειται να αντιμετωπίσουμε και έτσι έχουμε το πλεονέκτημα της πρόβλεψης και γρήγορης αντιμετώπισης. Ακόμα με τις διαδικασίες καταγραφής των κινδύνων , έχουμε και πλήρη εικόνα για το ποιος είναι υπεύθυνος για την ενδεχόμενη καταστροφή , όπως και μια γρήγορη λύση για την αντιμετώπιση του προβλήματος.

Μερικά από τα σημαντικά συμπεράσματα είναι πόσο σημαντική είναι η συνεχής εκτίμηση και ο προγραμματισμός του κινδύνου σε όλες τις φάσεις ενός έργου. Άλλο ένα σημείο που πρέπει να αναλογιστούν οι επιχειρήσεις είναι πόσο σημαντικό ρόλο παίζει η συνεχής εκπαίδευση και ενημέρωση του προσωπικού σε έναν οργανισμό για να έχει τα εφόδια να αντιμετωπίσει πιθανούς κινδύνους στην καθημερινότητα τους. Επίσης ένα σημαντικό συμπέρασμα είναι ότι δεν πρέπει να σταματήσει ο έλεγχος των συστημάτων και οι συνθήκες πρόσβασης και αυθεντικότητας των χρηστών.

Τέλος η προσωπική μου άποψη είναι ότι η άριστη γνώση του συστήματος και των λειτουργιών του θα αποφέρουν τα επιθυμητά αποτελέσματα για ένα ασφαλές ολοκληρωμένο πληροφοριακό σύστημα κατά ένα μεγάλο ποσοστό επιτυχίας. «Σίγουρα : Δεν υπάρχει έργο χωρίς κίνδυνο και δεν υπάρχει managementχωρίς ρίσκο.»

Βιβλιογραφία

1. http://el.wikipedia.org/wiki/

2. http://www.oracle.com/

*3. QNR - Quality and Reliability S.A(*www.qnr.com.gr)

*4. Pc systems(*www.pcsystems.gr)

5. Computer related risks (peter G.Neuman)

6. http://www.fdic.gov/

7. computer Solutions SA.

8.http://www.theirm.org/publications/documents/Risk_Management_Standard_Greek_000.pdf

9.IRM (institute of risk management)

10.http://www.skatelescope.org/

11.http://www.theirm.org/publications/documents/Risk_Management_Standard_Greek_000.pdf

12.http://en.wikipedia.org/wiki/CRAMM

13.http://www.theirm.org/publications/documents/Risk_Management_Standard_Greek_000.pdf

14. http://www.riskmanagement-solutions.net/project-risk-management

15.http://www.riskmanagement-solutions.net/?s=Risk%20management%20framework&ac=2&slt=8&slr=1&lpt=1&gdt=AG06ipB-Lxqk5pDBS1HkkXVtUuiwdOQboQoTCKqY4qXhuLcCFeWNwgod_VUAYhgBIABQ0ZKhAVDk2sQJUL_v4g5Q8v7iDlCgxI0PUMH7mA9Q7_6YD1Dz_pgPUNn_mA9Qme7OD1Cn9NsPUMy63A9QwYH3D1DGgfcPUN6p-Q9QhoyvEFDEu7URUPe7tRFQvLzlEVDGvOURUMH8pxNQo-

3_E1C_5ekVUJWQ7hVQn665HVCgupEhUMLZkSFQ967fJVDTsa0pUOqv_0NQtYKmUVCKkJOPAVD7u5SVAVD63sqjAVCa-aanAVCJmPPAAVC6xODCAVCx58iaA1DthdidA1CWi9idA1CproqNBWjRkqEBcTEVYhrFGDMRggETCI_u4qXhuLcCFaGRwgodvSsAvI0BFUMfIJEBxusVZBqFgSU

16.http://el.wikiversity.org/wiki/%CE%95%CE%B9%CF%83%CE%B1%CE%B3%CF%89%CE%B3%CE%AE_%CF%83%CF%84%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%AC_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1

17. http://aetos.it.teithe.gr/~dranidis/IS_Notes_1.pdf