Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ

Τμήμα Μηχανικών Πληροφορικής Τ.Ε.
Σχολή Τεχνολογικών Εφαρμογών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΑΠΟΤΙΜΗΣΗ ΤΟΥ ΚΙΝΔΥΝΟΥ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΕΝΟΣ ΤΜΗΜΑΤΟΣ ΠΛΗΡΟΦΟΡΙΚΗΣ Γ΄ΒΑΘΜΙΑΣ ΕΚΠΑΙΔΕΥΣΗΣ.

Επιβλέπων Καθηγητής: Καραμπάτσος Βασίλειος

Φοιτητής: Γαλάτουλας Ανδρέας *ΑΜ: 2008008*

Σπάρτη, Δεκέμβριος 2013

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ	ΥΠΟΓΡΑΦΕΣ
1.	
2.	
3.	

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Τ.Ε.Ι. Πελοποννήσου.

Ο συγγραφέας,

Γαλάτουλας Ανδρέας

Ευχαριστίες

Η παρούσα πτυχιακή εργασία με θέμα «Μελέτη της ασφάλειας και της διαχείρισης και αποτίμηση του κινδύνου των πληροφοριακών συστημάτων ενός τμήματος πληροφορικής Γ΄ βάθμιας εκπαίδευσης» πραγματοποιήθηκε, στο πλαίσιο της πτυχιακής εργασίας του τμήματος Μηχανικών Πληροφορικής Τ.Ε της σχολής Τεχνολογικών εφαρμογών (έδρα Σπάρτη) ΤΕΙ Πελοποννήσου. Στο σημείο αυτό αισθάνομαι την ανάγκη να εκφράσω τις ειλικρινείς και θερμές ευχαριστίες μου σε όσους συνέβαλαν στην ολοκλήρωση αυτής της προσπάθειας :

Και πρώτα απ' όλα, τον επιβλέπων καθηγητή Καραμπάτσο Βασίλειο εργαστηριακό συνεργάτη του τμήματος Μηχανικών Πληροφορικής Τ.Ε για τη συνεχή καθοδήγηση, την αμέριστη υποστήριξη, τις ουσιώδεις συμβουλές, καθώς και την αδιάκοπη συμπαράσταση και ενθάρρυνση που μου παρείχε σε όλο αυτό το διάστημα.

Τέλος, θέλω να ευχαριστήσω όλους εκείνους που με έμαθαν να «προσπερνώ» και βοήθησαν να γίνουν «ανεκτοί» οι συμβιβασμοί των τελευταίων χρόνων: την οικογένεια μου, τους φίλους μου, τους συναδέλφους μου.

Αφιερώνω λοιπόν την πτυχιακή μου εργασία στην οικογένεια μου Ξενοφών και Σταματία Γαλάτουλα οι οποίοι στήριξαν τις σπουδές μου με διάφορους τρόπους, φροντίζοντας για την καλύτερη δυνατή μόρφωση μου και τους στόχους μου σε όλα αυτά τα χρόνια. Υπήρξαν πάντα ένα ανεκτίμητο στήριγμα για μένα και στους οποίους οφείλω όλη την διαδρομή των σπουδών μου μέχρι και σήμερα.

Ανδρέας Ξ. Γαλάτουλας

Περιεχόμενα

Εισαγωγή

Γενικά

Το θέμα της παρούσας εργασίας είναι η μελέτη της ασφάλειας και της διαχείρισης και αποτίμηση του κινδύνου των Πληροφοριακών Συστημάτων του τμήματος Μηχανικών Πληροφορικής Τ.Ε. Το όλο σύστημα του τμήματος Μηχανικών Πληροφορικής Τ.Ε αποτελείται από επιμέρους συστήματα, όπως τους υπολογιστές στις αίθουσες των εργαστηρίων που είναι για φοιτητές, στα γραφεία των καθηγητών στην αίθουσα της γραμματείας του τμήματος και σε άλλους χώρους εργασίας. Ακόμη στο τμήμα Μηχανικών Πληροφορικής Τ.Ε υπάρχει μια αίθουσα ξεχωριστή από τις άλλες αίθουσες που εκεί μέσα είναι εγκατεστημένος ο SERVER του τμήματος όπου φιλοξενείται το site της σχολής.

Αντικείμενο εργασίας

Η μελέτη της ασφάλειας και της διαχείρισης και αποτίμηση του κινδύνου των Πληροφοριακών Συστημάτων του τμήματος Μηχανικών Πληροφορικής Τ.Ε. Μέσα από την εκπόνηση της συγκεκριμένης μεθοδολογίας πάνω στο σύστημα θα προσδιοριστούν τα κρίσιμα αγαθά του συστήματος, οι δυνητικές απειλές, τα αδύνατα σημεία του συστήματος και θα προταθούν κάποια αντίμετρα –μέτρα προστασίας τα οποία θα εξασφαλίζουν ασφαλέστερη λειτουργία του συστήματος.

1. Μεθοδολογική Προσέγγιση της Μελέτης

Η μεθοδολογία που επιλέχθηκε για την πραγματοποίηση της παρούσας μελέτης του πληροφοριακού συστήματος του τμήματος Μηχανικών Πληροφορικής Τ.Ε είναι η Octave–s. Ο λόγος που επιλέχθηκε η συγκεκριμένη έκδοση της Octave είναι ότι ανταποκρίνεται στο μέγεθός του πληροφοριακού συστήματος. Η συγκεκριμένη έκδοση της μεθοδολογίας χρησιμοποιείται ως τεχνική αξιολόγησης συστημάτων στον τομέα της ανάλυσης της επικινδυνότητας του συστήματος. Την παρούσα μελέτη παράγει μία ομάδα ανάλυσης όπου εξετάζει την επικινδυνότητα που διατρέχουν τα κρίσιμα αγαθά του Πληροφοριακού Συστήματος του τμήματος Μηχανικών Πληροφορικής Τ.Ε. σε συνδυασμό με την πλήρη λειτουργικότητα του συστήματος. Η ομάδα ανάλυσης επικινδυνότητας απαρτίζεται από τους ίδιους τους συγγραφείς. Με την εφαρμογή της συγκεκριμένης μεθοδολογία, το τμήμα Μηχανικών Πληροφορικής Τ.Ε μπορεί να προστατεύσει τα κρίσιμα αγαθά του και να προβεί στην παραγωγή της Πολιτικής Ασφάλειας.

Για την διεκπεραίωση της ανάλυσης επικινδυνότητας πρέπει να απαντηθούν κάποια ερωτηματολόγια από την ομάδα ανάλυσης. Η τελευταία, θα πρέπει να γνωρίζει πολύ καλά το σύστημα που εξετάζει για να παραχθεί μη πλασματικό αποτέλεσμα.

Τα ερωτηματολόγια της Octave-s αποτελούνται από τρεις φάσεις. Στην πρώτη φάση προσδιορίζονται τα κρίσιμα αγαθά του ιδρύματος και παρουσιάζεται/ αξιολογείται η παρούσα κατάσταση του συστήματος. Στη δεύτερη φάση λαμβάνει χώρα η ανασκόπηση του συστήματος του ιδρύματος. Δηλαδή η ομάδα ανάλυσης εξετάζει στα μέρη του πληροφοριακού συστήματος και ότι αυτό περιλαμβάνει. Τέλος στη τρίτη φάση αναπτύσσεται η στρατηγική και ο σχεδιασμός ασφάλειας. Μετά το πέρας των φάσεων της μεθοδολογίας έχουν πλέον αναγνωριστεί οι κίνδυνοι για τα αγαθά και λαμβάνονται κάποιες αποφάσεις για τον τρόπο αντιμετώπισης αυτών.

1.1. Εύρος Και Περιορισμοί

Το εύρος της συγκεκριμένης μελέτης ασφάλειας περιορίζεται μόνο από το Πληροφοριακό Σύστημα του τμήματος Μηχανικών Πληροφορικής Τ.Ε και ότι αυτό περιλαμβάνει (συλλογή, επεξεργασία, αποστολή δεδομένων). θεωρούμε ότι δεν

υπάρχουν οικονομικές κυρώσεις στο τμήμα Μηχανικών Πληροφορικής Τ.Ε και για αυτό το λόγο τοποθετούμε τις οικονομικές επιπτώσεις ως χαμηλές.

Επιπλέον πρέπει να ορίσουμε πως σε καμία περίπτωση δεν έχουμε ανθρώπινες απώλειες και σε περίπτωση αποκάλυψης προσωπικών δεδομένων χωρίς την έγκριση του νόμιμου ιδιοκτήτη προβλέπονται αυστηρές κυρώσεις από την νομοθεσία.

1.2. Αξιοποίηση Αποτελεσμάτων Μελέτης Ασφάλειας

Μετά την ολοκλήρωση του συστήματος, πάρθηκαν κάποια μέτρα προστασίας από τους σχεδιαστές ώστε να μειωθεί η πιθανότητα να τεθεί σε κίνδυνο το σύστημα. Είναι επιτακτική ανάγκη όμως να γίνονται συστηματικοί έλεγχοι της ασφάλειας του συστήματος. Πρέπει να αναφέρουμε ότι πριν από την παρούσα εργασία δεν υπήρχε πολιτική ασφάλειας.

Τα αποτελέσματα της μελέτης μπορούν να χρησιμοποιηθούν επικουρικά από την διοίκηση του τμήματος Μηχανικών Πληροφορικής Τ.Ε ώστε να πάρει τις κατάλληλες αποφάσεις για να περιορίσουν πιθανά κρούσματα ασφάλειας.

Τέλος, είναι σημαντικό να αναπτυχθεί υψηλός βαθμός κουλτούρας ασφάλειας στο προσωπικό που διαχειρίζεται σημαντικούς πόρους και αγαθά.

2. Περιγραφή Παρούσας Κατάστασης

2.1. Στοιχεία του Πληροφοριακού Συστήματος του τμήματος Μηχανικών Πληροφορικής Τ.Ε.

Το Πληροφοριακό Σύστημα του τμήματος Μηχανικών Πληροφορικής Τ.Ε «στεγάζεται» στο ΤΕΙ Πελοποννήσου με έδρα την Σπάρτη όπου εκεί βρίσκεται η Βάση Δεδομένων του συστήματος και ο server της ιστοσελίδας. Κατά την σχεδίαση του συστήματος πρωταρχικός στόχος των σχεδιαστών του, ήταν η όσο το δυνατόν μεγαλύτερη αυτονομία του συστήματος αλλά και η ανάπτυξη κάποιων αυτοματισμών του Πληροφοριακού Συστήματος του τμήματος Μηχανικών Πληροφορικής Τ.Ε ώστε να μπορούν εύκολα οι διαχειριστές του να το τροποποιούν και γενικότερα να είναι σχετικά εύκολη η επέκτασή του. Όπως ανάφερα παραπάνω, στην εισαγωγή το σύστημα αυτό του τμήματος Μηχανικών Πληροφορικής Τ.Ε αποτελείται από αίθουσες υπολογιστών που είναι για φοιτητές, από γραφεία καθηγητών που υπάρχουν υπολογιστές και στην αίθουσα της γραμματείας του τμήματος, που υπάρχουν και εκεί υπολογιστές, και σε άλλους χώρους εργασίας. Ακόμη στο τμήμα Μηχανικών Πληροφορικής Τ.Ε υπάρχει μια αίθουσα ξεχωριστή από τις άλλες αίθουσες που εκεί μέσα βρίσκεται ο SERVER του τμήματος που βρίσκετε το site της σχολής όπου υπάρχουν οι διαφορές ανακοινώσεις του ΤΕΙ Πελοποννήσου.

Αναλυτικά στις αίθουσες των φοιτητών υπάρχουν διάφορα λογισμικά όπου εκεί οι φοιτητές κάνουν τις εργασίες κατά την ώρα του μαθήματος. Κάθε εργαστήριο υπάρχει ένας προσωπικός υπολογιστής όπου είναι εγκατεστημένο τα Windows XP είναι ένα λειτουργικό σύστημα της οικογένειας Windows της Microsoft για προσωπικούς υπολογιστές. Κυκλοφόρησε στις 25 Οκτωβρίου 2001 σε δύο εκδόσεις: την Windows XP Home Edition που προορίζεται για οικιακούς χρήστες και την Windows XP Professional που περιλαμβάνει επιπλέον δυνατότητες όπως υποστήριξη για διπλό μικροεπεξεργαστή και την δυνατότητα σύνδεσης σε έναν τομέα (domain). Τα γράμματα XP προέρχονται από την λέξη "Experience" (εμπειρία). Ανάλογα με το κάθε μάθημα που υπάρχει στο εξάμηνο υπάρχει και το κατάλληλο λογισμικό όπου μπορεί να δουλέψει ο φοιτητής. Στην συνέχεια υπάρχει η αίθουσα της γραμματείας που έχει υπολογιστές και μπορούν να δουλέψουν το πληροφορικό σύστημα του τμήματος που προορίζονται για τη συλλογή, εγγραφή, ανάκτηση,

επεξεργασία, αποθήκευση και ανάλυση πληροφοριών. Τα συστήματα αυτά μπορούν να περιλαμβάνουν λογισμικό, υλικό και τηλεπικοινωνιακό σκέλος.

Στην συνέχεια υπάρχει το πρόγραμμα "Ηλεκτρονική Γραμματεία " εγκατεστημένο στο PC της γραμματείας όπου εκεί έχει πρόσβαση μόνο η γραμματεία του τμήματος ώστε έτσι να μπορεί να περνάει την βαθμολογία του φοιτητή να βλέπει ανακοινώσεις των φοιτητών ηλεκτρονικά και γενικά περιγράφει τα στοιχειά του φοιτητή «Εισάγετε όνομα χρήστη και κωδικό για να αποκτήσετε πρόσβαση στο σύστημα και να δείτε προσωπικές πληροφορίες για το πρόγραμμα σπουδών, διδασκαλίας, εξετάσεων, καθώς επίσης και να αποστείλετε αιτήσεις προς τη Γραμματεία του τμήματός σας, να δείτε την συνολική σας βαθμολογία και όλες τις εγγραφές σας στα εξάμηνα.»

Στην συνέχεια υπάρχει μια αίθουσα όπου βρίσκετε ο SERVER του ΤΕΙ όπου λειτουργεί η ιστοσελίδας του συστήματος Επίσης υφίσταται και site διαχείρισης του συστήματος όπου έχουν πρόσβαση μόνο οι διαχειριστές του συστήματος μόνο μέσω του συγκεκριμένου υπολογιστή. Με αυτό τον τρόπο οι διαχειριστές μπορούν να εποπτεύουν το σύστημα και να φροντίζουν για την ομαλή λειτουργία αυτού.

Για να είναι κάποιος χρήστης του συστήματος πρέπει να τηρεί την προϋπόθεση ότι είναι μέλος της ακαδημαϊκής κοινότητας του τμήματος Μηχανικών Πληροφορικής Τ.Ε είτε ως φοιτητής, είτε ως διδακτικό προσωπικό είτε ως διοικητικό προσωπικό. Με λίγα λόγια δικαίωμα εγγραφής στο σύστημα έχουν μόνο όσοι διαθέτουν λογαριασμό e-mail στο τμήμα Μηχανικών Πληροφορικής Τ.Ε.. Στην συνέχεια αφού ο χρήστης έχει συμπληρώσει τα στοιχεία του για την εγγραφή στο σύστημα είναι σε θέση να αλληλεπιδράσει με το πληροφοριακό σύστημα του τμήματος Μηχανικών Πληροφορικής Τ.Ε. Το σύστημα διαθέτει ένα υπολογιστή ώστε να αποστέλλει και να λαμβάνει τα δεδομένα από και προς τους χρήστες. Ο χρήστης με την εγγραφή του στο σύστημα δημιουργεί ένα λογαριασμό σε αυτό. Είναι αναγκαίο για την ύπαρξη επικοινωνίας μεταξύ του χρήστη και του συστήματος και σε αυτή την περίπτωση υπαρχή η τεχνική υποστήριξη του ΤΕΙ για οτιδήποτε πρόβλημα προκύψει το σύστημα.

2.2. Περιγραφή χρήσης του Πληροφοριακού Συστήματος του τμήματος Μηχανικών Πληροφορικής Τ.Ε.

Ο χρήστης από την στιγμή που έχει ολοκληρώσει την διαδικασία εγγραφής του στο σύστημα υπάρχουν κάποιες ενέργειες που πρέπει για να λειτούργει το πληροφοριακό σύστημα του τμήματος Μηχανικών Πληροφορικής Τ.Ε να υπάρχει τοποθέτηση του προβλήματος, διάφορες απαιτήσεις χρηστών ,απαιτήσεις σε αυτόματη επεξεργασία δεδομένων, λειτουργικές απαιτήσεις – λειτουργίες συστήματος και απαιτήσεις απόδοσης, προδιαγραφές υλικού, λογισμικού και διαδικασιών ,υλικό, λογισμικό. Επόμενος υπάρχει στενή σχέση μεταξύ πληροφοριακών συστημάτων και πραγματικού κόσμου.

2.3. Αποτίμηση Παρούσας Κατάστασης

Όπως ορίζει και η διαδικασία Πρακτικές Ασφάλειας (Security Practices Worksheet), διεθνώς, πρέπει να μελετηθεί η αποτελεσματικότητα και η αποδοτικότητα των πρακτικών ασφάλειας του χρήσης του Πληροφοριακού Συστήματος του τμήματος Μηχανικών Πληροφορικής Τ.Ε. στους παρακάτω ειδικούς τομείς ασφάλειας:

Εκπαίδευση και Ενημέρωση για θέματα ασφάλειας (Security Awareness and Training)

Είναι απαραίτητο οι διαχειριστές του συστήματος να ακολουθούν την πολιτική ασφαλείας που ορίζεται στη συνέχεια. Καθώς το σύστημα διαθέτει αποθηκευμένα τα προσωπικά στοιχεία των χρηστών του (όπως κινητό τηλέφωνο, βαθμολογίες σε μαθήματα) στη βάση δεδομένων του. Οι διαχειριστές έχουν πλήρη επίγνωση του ρόλου που παίζει η ασφάλεια στο σύστημα και φροντίζουν να ενημερώνουν σε περίπτωση που παρατηρήσου κάποιο περίεργο περιστατικό. Ακόμα υπάρχει περίπτωση για περαιτέρω ενημέρωση των διαχειριστών σε θέματα ασφάλειας καθώς στο τμήμα Μηχανικών Πληροφορικής Τ.Ε υφίσταται Σεμινάριο Ασφάλειας όπου μπορεί να προβεί σε κάποια ενημερωτικά σεμινάρια από το υπεύθυνο προσωπικό.

Πολιτική ασφάλειας

Η διαμόρφωση της πολιτικής ασφάλειας για τα πληροφοριακά συστήματα ενός οργανισμού έπεται της αξιολόγησης του επιπέδου ασφάλειας των συστημάτων

αυτών. Η αξιολόγηση της ασφάλειας μπορεί να γίνει με διάφορους τρόπους, οι πιο συνηθισμένοι από αυτούς είναι η εκπόνηση μιας μελέτης ανάλυσης επικινδυνότητας (Risk Analysis) και η χρήση κάποιων από τα πρότυπα (standards) διαχείρισης της ασφάλειας.

Για καλύτερη κατανόηση αρχικά δίνονται οι βασικοί ορισμοί που χρησιμοποιούνται ευρέως στην ανάλυση κινδύνων:

Απειλή: Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση μετατροπή των δεδομένων, καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.

Ευπάθεια: Είναι η αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, στην εφαρμογή ή στην υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος. Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

Ευπάθεια = Πιθανότητα να συμβεί μια απειλή x Πιθανότητα να είναι επιτυχής

Κίνδυνος: Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Ο κίνδυνος εκφράζει το ενδεχόμενο για απώλεια.

Αντίμετρο: Μέτρο που λαμβάνεται για την προστασία του πληροφοριακού συστήματος και την αντιμετώπιση των απειλών. Το μέτρο μπορεί να ενεργεί ανιχνεύοντας, προλαμβάνοντας ή μειώνοντας την απώλεια που σχετίζεται με την εμφάνιση μιας απειλής ή κατηγορίας απειλών.

Διαχείριση Ασφάλειας (Security Management)

Μέχρι πρότινος δεν υπήρχε Πολιτική Ασφάλειας και οι διαχειριστές έδρατταν μεμονωμένα και σύμφωνα με την δικιά τους κρίση απέναντι σε περιστατικά ασφάλειας, προχωρώντας αυτόβουλα στην λήψη κάποιων μέτρων ασφάλειας ώστε μετριαστούν οι εκάστοτε απειλές.

Οι διαχειριστές του συστήματος πρέπει να έχουν πλήρη γνώση των αρμοδιοτήτων τους που τους προσδίδει ο ρόλος τους. Αυτοί πρέπει να ελέγχουν τακτικά το σύστημα

για την τυχών ύπαρξη ύποπτων περιστατικών και να προβαίνουν στις αντίστοιχες ενέργειες που ορίζει η Πολιτική Ασφάλειας

Διαχείριση Ασφάλειας σε σχέση με τους εξωτερικούς συνεργάτες (Collaborative Security Management)

Η φύση της συνεργασίας των εξωτερικών παραγόντων του τμήματος Μηχανικών Πληροφορικής Τ.Ε. υπόκειται στη συμμόρφωση με τους ευρύτερους κανόνες της Πολιτικής Ασφάλειας και κανονισμών, που έχει αναπτύξει το τμήμα Μηχανικών Πληροφορικής Τ.Ε. για την συνεργασία του με τρίτους.

Σχέδιο Συνέχειας / Ανάκαμψη Μετά Από Καταστροφή (Contingency Planning / Disaster Recovery)

Σε αυτό το σημείο πρέπει να δώσουμε έμφαση στο γεγονός ότι δεν υφίσταται σχέδιο ανάκαμψης μετά από καταστροφή. Αναλυτικότερα ισχύουν τα εξής:

- Το πληροφοριακό σύστημα του τμήματος δημιουργεί εφεδρικά αντίγραφα της Β.Δ του στο τερματικό που λειτουργεί ήδη το σύστημα.

- Επίσης δεν υπάρχει κάποιο εφεδρικό τερματικό όπου είναι εγκατεστημένο το πληροφοριακό σύστημα του τμήματος ώστε να υπάρχει η δυνατότητα παροχής των υπηρεσιών ανά πάσα στιγμή.

Έλεγχος Φυσικής Πρόσβασης (Physical Access Control)

Όσων αφορά τον έλεγχο της φυσικής πρόσβασης, θα πρέπει να αναφέρουμε ότι δεν υπάρχουν συγκεκριμένοι κανονισμοί και πολιτικές ασφάλειας για την πρόσβαση στο χώρο όπου βρίσκεται το σύστημα στεγάζεται σε χώρο ο οποίος αποτελεί γραφεία διδακτικού προσωπικού Εκτός των προαναφερθέντων, φυσική πρόσβαση στο χώρο έχουν και άλλα μέλη του προσωπικού του τμήματος Μηχανικών Πληροφορικής Τ.Ε. (συνεργείο καθαρισμού, τεχνική υπηρεσία κ.α.).

Παρακολούθηση και Έλεγχος της Ασφάλειας των Πληροφοριακών Συστημάτων (Monitoring and Auditing IT Security)

Οι διαχειριστές του συστήματος εποπτεύουν την λειτουργία του πληροφοριακού συστήματος του τμήματος μέσω της ιστοσελίδας διαχείρισης για την πιθανή ύπαρξη ύποπτων ενεργειών ή δοσοληψιών προς το σύστημα. Επίσης καταγράφεται η όποια

απόπειρα πρόσβασης στην ιστοσελίδα διαχείρισης του συστήματος από τρίτους (πέραν των διαχειριστών).

Κρυπτογράφηση (Encryption)

Η Β.Δ περιέχει κάποια προσωπικά στοιχεία των χρηστών (όπως αριθμός κινητού τηλεφώνου, βαθμολογίες σε μαθήματα) όπου αυτά υπόκεινται σε κρυπτογράφηση κατά την αποθήκευσή τους.

Σχεδιασμός και Αρχιτεκτονική Ασφάλειας (Security Architecture and Design)

Ο σχεδιασμός και η αρχιτεκτονική του συστήματος δημιουργήθηκε από μηδενική βάση και δεν βασίστηκε σε προϋπάρχουσες διαδικασίες και πολιτικές ασφάλειας. Πιθανή επέκταση του συστήματος, πλέον μπορεί να αναπτυχθεί πάνω στους νέους κανόνες που περιγράφονται στη παρούσα μελέτη.

Παρακολούθηση και Καταγραφή Φυσικής Ασφάλειας (Monitoring and Auditing Physical Security)

Σύμφωνα με το άρθρο 2 του Ν. 1268/82 όπου ορίζονται οι ακαδημαϊκές ελευθερίες και το πανεπιστημιακό άσυλο δεν επιτρέπεται η χρήση συστημάτων παρακολούθησης και καταγραφής συμβάντων.

Διαχείριση Συστημάτων και Δικτύου (System and Network Management)

Η τεχνική υπηρεσία πληροφορικής του ΤΕΙ Πελοποννήσου είναι υπεύθυνο για τον έλεγχο της ακεραιότητας του εγκατεστημένου λογισμικού, την ενημέρωση και την αναβάθμιση του σύμφωνα με τις τρέχουσες νέες τεχνολογίες κατόπιν σχετικού αιτήματος από την μεριά των διαχειριστών του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε. Ακόμα η τεχνική υπηρεσία πληροφορικής του ΤΕΙ Πελοποννήσου είναι υπεύθυνο για τη διαχείριση του δικτύου όπου και το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε αποτελεί ένα από τους κόμβους αυτού.

Αυθεντικοποίηση και Εξουσιοδότηση (Authentication and Authorization)

Οι χρήστες του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε αυθεντικοποιούνται για να εισέλθουν στο προσωπικό τους λογαριασμό στο σύστημα και να προβούν ίσως στην διαχείριση αυτού. Οι διαχειριστές αυθεντικοποιούνται στο τερματικό που είναι εγκατεστημένο το λογισμικό του συστήματος και στη συνέχεια έχουν πρόσβαση σε όλα τα κρίσιμα δεδομένα του

συστήματος (π.χ. ιστοσελίδα διαχείρισης, Β.Δ, δεδομένα του συστήματος). Επιπρόσθετα οι διαχειριστές έχουν την δυνατότητα για απομακρυσμένη πρόσβαση με Secure Shell (ssh) στο σύστημα.

Διαχείριση Ευπαθειών (Vulnerability Management)

Οι διαχειριστές του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε έχουν προβεί σε έλεγχο στο σύστημα για την εύρεση πιθανών ευπαθειών με την χρήση των κατάλληλων εργαλείων εκτίμησης ευπαθειών (π.χ. Nessus). Στη συνέχεια προχώρησαν στην λήψη μέτρων για τον περιορισμό αυτών (π.χ. φραγή θυρών). Ακόμα είναι υπεύθυνοι για τη διαχείριση νέων ευπαθειών που προκύπτουν και την αντιμετώπιση αυτών με νέες μεθόδους.

Διαχείριση Συμβάντων (Incident Management)

Για συμβάντα εξωτερικής φύσεως όπως εσωτερικό δίκτυο, εξωτερικό δίκτυο, παροχή ρεύματος, χαμηλή ισχύ σήματος οι διαχειριστές του συστήματος δεν είναι σε θέση να διαχειριστούν τέτοιες περιπτώσεις. Μέχρι τώρα η διαχείριση εσωτερικών συμβάντων από τους διαχειριστές του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε πραγματοποιούνταν εμπειρικά.

3. Αποτελέσματα Ανάλυσης Επικινδυνότητας

Σκοπός

Βασικός σκοπός της μελέτης αυτής είναι η ανάλυση επικινδυνότητας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε μέσα από την τυποποιημένη μέθοδο της OCTAVE – s. Έχει ήδη παρουσιαστεί η παρούσα κατάσταση και τα κρίσιμα αγαθά του συστήματος. Στη συνέχεια, ακολουθεί η εκτίμηση των αδύναμων σημείων των κρίσιμων αγαθών, οι παράγοντες που απειλούν τα αδύναμα σημεία και τέλος οι επιπτώσεις που θα υπάρξουν αν αυτοί εμφανιστούν.

Η κατηγοριοποίηση που ακολουθείται από την OCTAVE – s για τις απειλές των κρίσιμων αγαθών που πιθανόν υπάρξουν είναι οι εξής:

- Ανθρώπινοι Παράγοντες που χρησιμοποιούν το δίκτυο
- Ανθρώπινοι Παράγοντες που έχουν φυσική πρόσβαση
- Προβλήματα Συστημάτων
- Λοιπά προβλήματα
- Προβλήματα που σχετίζονται με το ανθρώπινο προσωπικό.

Η ομάδα ανάλυσης του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε λόγω του γεγονότος ότι κάποιες κατηγορίες απειλών ταυτίζονται χρησιμοποιεί την κατηγοριοποίηση:

- Απειλές Μέσω Δικτυακής Πρόσβασης
- Απειλές Μέσω Φυσικής Πρόσβασης
- Απειλές Μέσω Άλλων Προβλημάτων.

Για κάθε κρίσιμο αγαθό, στην παρακάτω ανάλυση, παρουσιάζονται στον πρώτο πίνακα οι πιθανότητες να εμφανιστούν οι απειλές, με βάση την αποκάλυψη, την τροποποίηση, την απώλεια ή καταστροφή και την διακοπή λειτουργίας, καθώς και ο βαθμός βεβαιότητάς τους. Στο δεύτερο πίνακα παρουσιάζονται τα κόστη των

επιπτώσεων στους τομείς της φήμης, των οικονομικών, της παραγωγικότητας και της επιβολής χρηματικών ποινών. Ο βαθμός βεβαιότητας και τα κόστη των επιπτώσεων χαρακτηρίζονται ως Χαμηλά, Μέτρια, Υψηλά.

3.1 Προσδιορισμός Κρίσιμων Αγαθών

Μετά από την αποτίμηση της παρούσας κατάστασης το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε επεξεργάζεται τα ερωτηματολόγια , που χρησιμοποιεί η μέθοδος OCTAVE – s, τα κρίσιμα αγαθά που προσδιορίστηκαν είναι:

- η ιστοσελίδα του συστήματος, η οποία είναι η εικόνα του και μέσω της οποίας μπορεί ο χρήστης να εγγραφεί, να αλλάξει το προσωπικό του menu κ.α.
- η βάση δεδομένων, στην οποία αποθηκεύονται τα προσωπικά δεδομένα των χρηστών (όπως για παράδειγμα, το ονοματεπώνυμο, e-mail ή αριθμό κινητού τηλεφώνου, κ.ά.) αλλά και άλλες πληροφορίες (οι βαθμολογίες των χρηστών στα μαθήματα που έχουν εξεταστεί κλπ).
- τα δεδομένα (ιστοσελίδα διαχείρισης), τα οποία αποθηκεύονται στον ηλεκτρονικό υπολογιστή του. Επίσης λαμβάνεται σε αυτά και η ιστοσελίδα διαχείρισης η οποία είναι ζωτικής σημασίας για το σύστημα.

Για κάθε ένα από τα υπάρχοντα κρίσιμα αγαθά θα αναλυθούν παρακάτω οι απειλές που μπορούν να εμφανιστούν όσον αφορά την πρόσβαση μέσω δικτύου, τη φυσική πρόσβαση και άλλα προβλήματα που πιθανώς εμφανιστούν.

3.2 Η Ιστοσελίδα του τμήματος του ΤΕΙ Πελοποννήσου.

Η ιστοσελίδα του ΤΕΙ Πελοποννήσου αποτελεί ένα σύστημα παροχής υπηρεσιών και προσφέρει φοιτητικές υπηρεσίες στα πλαίσια του τμήματος Μηχανικών πληροφορικής με Έδρα την Σπάρτη καθώς και υπηρεσίες ενημέρωσης γενικού ενδιαφέροντος όπως αποστολή του Τμήματος δηλαδή αναφέρει την επιστημονική και τεχνολογική ανάπτυξη στους τομείς της Πληροφορικής και των Τηλεπικοινωνιών είναι απαραίτητη για την κάλυψη των αναγκών που προκύπτουν σε

όλους τους τομείς της παραγωγικής διαδικασίας. Οι εφαρμογές της πληροφορικής και των τηλεπικοινωνιών συνεχώς αναπτύσσονται και δημιουργούν καινούργιες ανάγκες σε επιστημονικό προσωπικό με αυξημένα προσόντα. Η αποστολή του τμήματος είναι η κάλυψη αυτών των αναγκών με την παροχή υψηλού επιπέδου γνώσεων στους σπουδαστές του, οι οποίοι θα αποτελέσουν μελλοντικά στελέχη εταιρειών και φορέων τόσο του δημοσίου όσο και του ιδιωτικού τομέα. Οι χρήστες μόνο μέσω της ιστοσελίδας μπορούν να εγγραφούν στο σύστημα και μπορούν να κατανοήσουν τον τρόπο αλληλεπίδρασης του συστήματος με τον χρήστη. Μέσω της ιστοσελίδας μπορούν να αιτηθούν διάφορα έγγραφα από την γραμματεία του τμήματος που ανήκει ο χρήστης, όπως έκδοση αναλυτικής βαθμολογίας, βεβαίωσης σπουδών είτε για αναβολή στράτευσης (για τους άνδρες φοιτητές), είτε για την εφορία είτε για οποιαδήποτε νόμιμη χρήση, και άλλα έγγραφα ακόμα περιλαμβάνει τις

- Εξελίξεις στους τομείς της πληροφορικής και των τηλεπικοινωνιών τόσο σε Εθνικό όσο και Διεθνές επίπεδο και να διασφαλίζει τη παροχή σύγχρονης γνώσης μέσα από ένα ποιοτικό και σύγχρονο πρόγραμμα σπουδών.
- Να χρησιμοποιεί και να προάγει τη σύγχρονη τεχνολογία στα θεματικά του αντικείμενα κυρίως με τη συμμετοχή και αξιοποίηση του ανθρώπινου δυναμικού του (Ε.Π ,Ε.Ε.Π, φοιτητές) σε χώρους εφαρμογής
- Να συνεργάζεται με φορείς, υπηρεσίες και παραγωγικές μονάδες του δημόσιου και ιδιωτικού τομέα σε θέματα σχετικά με τα γνωστικά του αντικείμενα
- Να συμμετέχει και να προάγει ερευνητικά θέματα στα θεματικά πεδία των νέων τεχνολογιών μέσα από συνεργασίες με άλλα Ανώτατα εκπαιδευτικά Ιδρύματα της χώρας και του εξωτερικού και να συμμετέχει σε ερευνητικά, αναπτυξιακά και καινοτομικά προγράμματα σε Περιφερειακό, Εθνικό και Διεθνές επίπεδο

Τέλος να παράσχει στους σπουδαστές του δυνατότητες και διευκολύνσεις για τη συμμετοχή τους σε άλλα ακαδημαϊκά προγράμματα μέσα από συνεργασίες και στα πλαίσια της κινητικότητας του προσωπικού και των φοιτητών. Λαμβάνοντας υπόψη λοιπόν, ότι η ιστοσελίδα του ΤΕΙ Πελοποννήσου αποτελεί την εικόνα της και λόγω του γεγονότος ότι μπορεί να τροποποιηθεί χωρίς εξουσιοδότηση και να διακοπεί ή

τερματιστεί η πρόσβαση / λειτουργία της, αυτή αποτελεί κρίσιμο αγαθό του συστήματος.

Οι απαιτήσεις ασφάλειας για την ιστοσελίδα είναι οι εξής:

Ακεραιότητα (Integrity): Δυνατότητα τροποποίησης της ιστοσελίδας αλλά και του τρόπου λειτουργίας της θα πρέπει να έχουν μόνο οι διαχειριστές της και όχι εξωτερικές οντότητες.

Διαθεσιμότητα (Availability): Η ιστοσελίδα θα πρέπει να είναι διαθέσιμη επί εικοσιτετραώρου βάσεως και να λειτουργεί σωστά.

Σύμφωνα με την μελέτη ασφάλειας, η ιστοσελίδα του ΤΕΙ Πελοποννήσου μπορεί να απειληθεί, αν δεν ικανοποιούνται οι δύο παραπάνω απαιτήσεις, με δύο τρόπους, είτε μέσω δικτυακής πρόσβασης είτε μέσω φυσικής πρόσβασης.

3.2.1 Απειλές Μέσω Δικτυακής Πρόσβασης

Στην περίπτωση της δικτυακής πρόσβασης, οι πιθανές απειλές μπορεί να προέλθουν είτε από εξωτερικούς παράγοντες, είτε από το εσωτερικό του τμήματος Μηχανικών πληροφορικής Τ.Ε συμφώνα με την ιστοσελίδα του ΤΕΙ Πελοποννήσου. Στις δύο παραπάνω περιπτώσεις, οι απειλές μπορεί να είναι σκόπιμες ή μη. Έτσι λοιπόν:

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Οι διαχειριστές της ιστοσελίδας, δηλαδή οι υπεύθυνοι του συστήματος, μπορεί από απροσεξία κατά την διαδικασία ανανέωσής της να την τροποποιήσουν με λανθασμένο τρόπο ή να διακόψουν την λειτουργία της ή να την καταστρέψουν. Έτσι λοιπόν, οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Υψηλός

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Τροποποίηση	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή
Ασφάλεια	Υψηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Ο χρηματισμός και η διαφθορά των διαχειριστών της ιστοσελίδας είναι η κύρια απειλή για το σύστημα, δεδομένου ότι η ηθελημένη τροποποίηση της ιστοσελίδας ή η διακοπή της λειτουργίας της για κάποιο χρονικό διάστημα για λόγους κέρδους ή κακόβουλης πρόθεσης προκαλεί την μη σωστή λειτουργία ή τη μη διαθεσιμότητά της και επομένως την δυσφήμιση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε. Οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Τροποποίηση	Υψηλός
Απώλεια ή καταστροφή	Υψηλός
Διακοπή Λειτουργίας	Υψηλός

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Τροποποίηση	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή
Ασφάλεια	Υψηλή	Χαμηλή	Χαμηλή

Μη σκόπιμες απειλές από εξωτερικούς παράγοντες:

Η ακούσια πρόκληση της μη διαθεσιμότητας της ιστοσελίδας του συστήματος από εξωτερικούς παράγοντες είναι μέτρια απειλή γιατί δεν μπορούν να εγγραφούν νέοι χρήστες και οι υπάρχοντες χρήστες δεν μπορούν να ενημερωθούν για την κατάσταση του λογαριασμού τους. Η παραπάνω απειλή μπορεί να προέλθει από πολύ μεγάλο αριθμό ταυτόχρονων επισκέψεων στην ιστοσελίδα. Οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Απώλεια ή καταστροφή	Μέτριος
Διακοπή στο σύστημα	Μέτριος

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Απώλεια / Καταστροφή	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή

Παραγωγικότητα	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από εξωτερικούς παράγοντες:

Η ύπαρξη κακόβουλων προθέσεων εξωτερικών παραγόντων μπορεί να αποτελέσει απειλή. Η παραπάνω απειλή μπορεί να προέλθει και σε αυτήν την περίπτωση από μεγάλο αριθμό επισκέψεων στην ιστοσελίδα, αλλά με οργανωμένους τρόπους και διαδικασίες. Οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Απώλεια ή καταστροφή	Μέτριος
Διακοπή Λειτουργίας	Μέτριος

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Απώλεια / Καταστροφή	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Χαμηλή
Οικονομικά	Χαμηλή	Χαμηλή
Παραγωγικότητα	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή

3.2.2 Απειλές Μέσω Φυσικής Πρόσβασης

Στην περίπτωση της φυσικής πρόσβασης, οι πιθανές απειλές μπορεί να προέλθουν μόνο από το εσωτερικό πληροφοριακού συστήματος του τμήματος Μηχανικών

πληροφορικής Τ.Ε. Στην παραπάνω περίπτωση, οι απειλές μπορεί να είναι σκόπιμες ή μη. Έτσι λοιπόν:

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Οι επιπτώσεις τέτοιων απειλών μπορεί να επιφέρουν τροποποίηση, διακοπή λειτουργίας στην εν λόγω ιστοσελίδα λόγω απροσεξίας του ανθρώπινου δυναμικού που είναι υπεύθυνο για την διαχείρισή της. Σε αυτό το σημείο καλό θα ήταν να οριστούν οι πιθανότητες των παραπάνω γεγονότων. Έτσι με απόλυτη βεβαιότητα:

Γεγονός	Βαθμός Βεβαιότητας
Τροποποίηση	Υψηλός
Διακοπή Λειτουργίας	Μέτριος

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Τροποποίηση	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Ο ανθρώπινος παράγοντας είναι απρόβλεπτος και πιθανόν οι ίδιοι οι διαχειριστές του συστήματος να του δημιουργήσουν ζημία. Λόγω της μη ύπαρξης διαφορετικών συνθηματικών μεταξύ των διαχειριστών δυσχεραίνει την αναγνώριση ποιος από

αυτούς προξένησε την ζημιά στην ιστοσελίδα. Έτσι ορίζοντας την πιθανότητα του παραπάνω γεγονότος, με απόλυτη βεβαιότητα:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Υψηλός
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Μέτριος

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Χαμηλή	Υψηλή	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Χαμηλή	Υψηλή	Μέτρια
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Ασφάλεια	Υψηλή	Υψηλή	Υψηλή	Υψηλή

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Οι διαχειριστές του συστήματος, μπορεί από απροσεξία κατά την διαδικασία τροποποίηση του συστήματος να εκθέσουν το σύστημα σε απειλές του διαδικτύου, να αποκαλύψουν την βάση δεδομένων και εν τέλει τη μη διαθεσιμότητα του συστήματος. Έτσι λοιπόν, οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Υψηλός

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Τροποποίηση	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή
Ασφάλεια	Υψηλή	Χαμηλή	Χαμηλή

Ως αποτίμηση των παραγόντων αυτών συνιστάται οι διαχειριστές να λάβουν εξειδικευμένα μέτρα προστασίας από κακόβουλο λογισμικό.

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Ο χρηματισμός και η διαφθορά των διαχειριστών της ιστοσελίδας είναι η κύρια απειλή για το σύστημα, δεδομένου ότι η ηθελημένη τροποποίηση του συστήματος ή η διακοπή της λειτουργίας του για κάποιο χρονικό διάστημα για λόγους κέρδους ή κακόβουλης πρόθεσης μπορεί να προκαλέσει την μη σωστή λειτουργία ή τη μη διαθεσιμότητά του και επομένως την δυσφήμιση του πληροφοριακού συστήματος του

τμήματος Μηχανικών πληροφορικής Τ.Ε . Οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Τροποποίηση	Υψηλός
Απώλεια ή καταστροφή	Υψηλός
Διακοπή Λειτουργίας	Υψηλός

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Τροποποίηση	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή
Ασφάλεια	Υψηλή	Υψηλή	Υψηλή

Μη σκόπιμες απειλές από εξωτερικούς παράγοντες:

Η ακούσια πρόκληση της μη διαθεσιμότητας του συστήματος από εξωτερικούς παράγοντες είναι πολύ υψηλή απειλή γιατί δεν θα μπορούν οι χρήστες να διαχειριστούν τις λειτουργίες του συστήματος. Η παραπάνω απειλή μπορεί να προέλθει είτε από την απροσεξία άλλων ατόμων που παραβρίσκονται στον ίδιο χώρο όπου βρίσκεται ο υπολογιστής, είτε από την διακοπή ρεύματος στην περιοχή όπου βρίσκεται ο υπολογιστής που παράλληλα παίζει το ρόλο του server, είτε από άλλους

φυσικούς παράγοντες. Οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Απώλεια ή καταστροφή	Μέτριος
Διακοπή στο σύστημα	Μέτριος

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Απώλεια / Καταστροφή	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή
Παραγωγικότητα	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από εξωτερικούς παράγοντες:

Η ύπαρξη κακόβουλων προθέσεων εξωτερικών παραγόντων μπορεί να αποτελέσει απειλή. Η παραπάνω απειλή μπορεί να προέλθει είτε από τις κακόβουλες προθέσεις άλλων ατόμων που έχουν την δυνατότητα να παραβρίσκονται στον ίδιο χώρο όπου βρίσκεται ο υπολογιστής, είτε από την ηθελημένη διακοπή ρεύματος στον χώρο όπου βρίσκεται ο υπολογιστής - server, είτε από την πρόκληση άλλων αιτιών καταστροφής με οργανωμένους τρόπους και διαδικασίες. Οι πιθανότητες των παραπάνω γεγονότων, με απόλυτη βεβαιότητα, είναι:

Γεγονός	Βαθμός Βεβαιότητας
Απώλεια ή καταστροφή	Μέτριος
Διακοπή Λειτουργίας	Μέτριος

Το καθένα από τα παραπάνω γεγονότα θα επιφέρει ζημιά στους εξής τομείς:

	Απώλεια / Καταστροφή	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή
Παραγωγικότητα	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή

3.2.3. Απειλές Μέσω Άλλων Προβλημάτων

Άλλα είδη προβλημάτων που μπορεί να αποτελέσουν απειλή για την ιστοσελίδα του ΤΕΙ Πελοποννήσου σύμφωνα με το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε έχει προβλήματα τροφοδοσίας, προβλήματα στο επικοινωνιακό δίκτυο προβλήματα από τους εξωτερικούς συνεργάτες και προβλήματα από την εκδήλωση φυσικών καταστροφών. Στην περίπτωση των φυσικών καταστροφών, η αποκατάσταση γίνεται με αργούς ρυθμούς καθώς δεν υπάρχει backup του web server. Η επίπτωση όλων των παραπάνω προβλημάτων είναι σημαντική για το συγκεκριμένο σύστημα.

Για τα προβλήματα στο επικοινωνιακό δίκτυο ισχύει ότι μπορούν να οδηγήσουν σε απώλεια / καταστροφή ή διακοπή συστήματος όμως η πιθανότητα εμφάνισής τους ιδιαίτερα χαμηλή.

Η εκδήλωση φυσικών καταστροφών ως αυτή του σεισμού ή της πλημμύρας μπορεί να οδηγήσει σε απώλεια / καταστροφή ή διακοπή του εν λόγω συστήματος. Η πιθανότητα να συμβούν οι επιπτώσεις αυτές είναι μάλλον χαμηλή, αλλά χωρίς καμία βεβαιότητα. Το κόστος της υπόληψης είναι χαμηλό και για τις δύο επιπτώσεις. Επίσης το οικονομικό κόστος και το κόστος παραγωγής είναι πολύ μικρό για το σύστημα, και έτσι δεν κρίνεται αναγκαίο να λάβει μέτρα για την προστασία της από φυσικές καταστροφές .Για κάθε κατηγορία περιουσιακών στοιχείων υπάρχουν και μια σειρά από απειλές. Στο βήμα αυτό αναγνωρίζονται οι απειλές για κάθε περιουσιακό στοιχείο, ο τρόπος με τον οποίο το απειλούν και οι επιπτώσεις που θα επιφέρει η κάθε απειλή.

Ανάλυση των ευπαθειών:

Ένα περιουσιακό στοιχείο μπορεί να είναι λιγότερο ευπαθής προς μια απειλή και περισσότερο προς μια άλλη. Στο βήμα αυτό διευκρινίζεται η ευπάθεια του κάθε περιουσιακού στοιχείου προς κάθε απειλή ξεχωριστά. Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

Ευπάθεια = Πιθανότητα να συμβεί μια απειλή x Πιθανότητα να είναι επιτυχής

Υπολογισμός του κινδύνου:

Ο βαθμός του κινδύνου υπολογίζεται ξεχωριστά για κάθε απειλή προς κάθε περιουσιακό στοιχείο. Είναι συνάρτηση όλων των παραπάνω, δηλαδή:

- Των επιπτώσεων μιας απειλής (που έχουν σχέση με την αξία του περιουσιακού στοιχείου)
- Της ευπάθειας του περιουσιακού στοιχείου ως προς την απειλή

Επιλογή τρόπων αντιμετώπισης των κινδύνων:

Υπάρχουν 3 τρόποι αντιμετώπισης του κινδύνου:

α) Αποφυγή του κινδύνου με πλήρη απόσυρση από μια συγκεκριμένη δραστηριότητα

β) Αποδοχή του κινδύνου

γ) Μείωση του κινδύνου με χρήση αντιμέτρων (μέτρων ασφαλείας)

Με τα αντίμετρα μπορούν να επιτευχθούν τα εξής:

- Μεταφορά κινδύνου, πχ. αγορά ασφάλειας

- Μείωση ευπάθειας:

• Μείωση πιθανότητας να συμβεί μια απειλή

- πχ. απαγορεύοντας το κάπνισμα σε μια ευαίσθητη περιοχή

• Μείωση πιθανότητας μια απειλή να είναι επιτυχής

- πχ. χρήση κρυπτογράφησης, χρήση firewall

- Μείωση αντίκτυπου, πχ. σύστημα πυρόσβεσης

- Μέτρα ανάνηψης (επαναφοράς), πχ. backup

Κατά το βήμα αυτό αναγνωρίζονται τα πιθανά αντίμετρα που μπορούν να εφαρμοστούν και επιλέγονται αυτά που συμφέρουν περισσότερο στον οργανισμό. Η ανάλυση κινδύνων και η ασφάλεια των πληροφοριακών συστημάτων για το τμήμα Μηχανικών πληροφορικής Τ.Ε είναι μια συνεχόμενη διαδικασία. Μετά την επιλογή των τρόπων αντιμετώπισης και την εφαρμογή τους στον οργανισμό πρέπει να υπάρχει μια συνεχής παρακολούθηση των κινδύνων. Τα δεδομένα σε ένα πληροφοριακό σύστημα αλλάζουν συνεχώς, εισάγονται νέες απειλές, νέες ευπάθειες, νέες επιπτώσεις κτλ. Τα αντίμετρα που έχουν επιλεχθεί ελέγχονται συνεχώς για την αποτελεσματικότητα τους. Πολλά από αυτά με τον καιρό σταματούν να συμφέρουν στον οργανισμό και πρέπει να καταργηθούν ή να αντικατασταθούν από νέα αντίμετρα.

3.3. Βάση δεδομένων

Σύμφωνα με τη διαδικασία Critical Asset Selection Worksheet της OCTAVE-s, η βάση δεδομένων αποτελεί σημαντικό αγαθό του συστήματος εφόσον η αποκάλυψή της σε μη εξουσιοδοτημένες οντότητες, η τροποποίησή της χωρίς εξουσιοδότηση, η καταστροφή της, καθώς και η διακοπή πρόσβασης – λειτουργίας της οδηγούν στη δυσλειτουργία και στη δυσφήμισή της. Η βάση δεδομένων διαθέτει ιστορικό προσπέλασης κάτι που είναι πάρα πολύ χρήσιμο όχι μόνο για την διατήρηση της ακεραιότητας της, αλλά και για την προστασία των δεδομένων που αποθηκεύονται. Οι απαιτήσεις ασφάλειας που μπορεί να παραβιαστούν είναι:

- Εμπιστευτικότητα: Η πρόσβαση στη βάση δεδομένων, που έχουν μόνο οι διαχειριστές, διαβαθμίζεται με στόχο να προστατεύεται από κακόβουλες ενέργειες και να διασφαλίζεται η σωστή λειτουργία της.
- Ακεραιότητα: Δυνατότητα τροποποίησης έχουν μόνο οι διαχειριστές.
- Διαθεσιμότητα: Βασικό πλεονέκτημα της βάσης δεδομένων είναι η διαθεσιμότητα της και η διαμοιρασμένη και ταυτόχρονη προσπέλαση των δεδομένων της.

Η βάση δεδομένων του συστήματος μπορεί να απειληθεί μόνο τόσο μέσω πρόσβασης από το δίκτυο όσο και από φυσική πρόσβαση. Περισσότερος όμως κίνδυνος υπάρχει από τους ίδιους τους διαχειριστές του συστήματος, δηλαδή μόνο εσωτερικά, στην περίπτωση της φυσικής πρόσβασης. Οι απειλές αυτές γίνονται είτε σκόπιμα είτε μη.

3.3.1. Απειλές Μέσω Δικτυακής Πρόσβασης

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Μία από τις πιο επίφοβες μη σκόπιμες απειλές που προέρχεται από το εσωτερικό του συστήματος είναι οι διαχειριστές του συστήματος, που είναι οι ίδιοι αρμόδιοι για τη βάση δεδομένων. Και αυτό γιατί μπορούν είτε από απροσεξία ή είτε από αμέλεια να τροποποιήσουν, να αποκαλύψουν ή και να διαγράψουν τα δεδομένα της. Έτσι με απόλυτη βεβαιότητα έχουμε:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός (χωρίς απόλυτη βεβαιότητα)
Διακοπή Λειτουργίας	Χαμηλός

Αυτές οι απειλές μπορούν να έχουν τα ακόλουθα κόστη:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Χαμηλή	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Τα παραπάνω φέρουν τις ακόλουθες αρνητικές συνέπειες.

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εξωτερικούς παράγοντες:

Ως σκόπιμη απειλή από εξωτερικούς παράγοντες μπορεί να θεωρηθεί όταν ένας κακόβουλος χρήστης προσπαθεί με διάφορα queries και χρησιμοποιώντας παραδείγματος χάρη Blind XPath Injection ή SQL Injection. Κατά τη σχεδίαση του συστήματος για να αποφευχθούν πιθανές επιθέσεις στη βάση δεδομένων, αποφασίστηκε και πραγματοποιήθηκε να μην μπορεί ο χρήστης να εισάγει μεταχαρακτήρες όπου χρησιμοποιούνται κατά κόρον σε τέτοιου είδους επιθέσεις. Έτσι με απόλυτη βεβαιότητα έχουμε:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Αυτά θα επιφέρουν ζημίες στα παρακάτω:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

3.3.2. Απειλές Μέσω Φυσικής Πρόσβασης

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Όπως και στην περίπτωση της πρόσβασης μέσω δικτύου, έτσι και σε αυτή την περίπτωση ισχύουν οι ίδιες απειλές.

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Μέτριος
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Ο χρηματισμός κάποιων εκ των διαχειριστών του συστήματος για την πρόσβαση στη βάση δεδομένων αποτελεί πάντα μια απειλή για το σύστημα. Παρόλα αυτά η συγκεκριμένη απειλή έχει πολύ μικρή πιθανότητα να πραγματοποιηθεί αφού πρόκειται για ένα σύστημα που πρόκειται να υλοποιηθεί στα πλαίσια διπλωματικής εργασίας στο τμήμα Μηχανικών πληροφορικής Τ.Ε. από προπτυχιακούς φοιτητές.

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός

Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Τα κόστη των επιπτώσεων παρατίθενται παρακάτω:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Χαμηλή	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Απειλές Μέσω Άλλων Προβλημάτων

Άλλες πιθανές απειλές μπορεί να προκύψουν είναι πιθανό να οφείλονται σε κατάρρευση του συστήματος, ατέλειες υλικού, κακόβουλο λογισμικό, προβλήματα τροφοδοσίας.

3.4. Τα Δεδομένα του πληροφορικού συστήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου με έδρα την Σπάρτη

Σύμφωνα με τη διαδικασία Critical Asset Selection Worksheet της OCTAVE-s, τα δεδομένα αποτελούν εξαιρετικά ουσιαστικό αγαθό του συστήματος εφόσον η αποκάλυψή τους σε μη εξουσιοδοτημένες οντότητες, η τροποποίησή τους χωρίς

εξουσιοδότηση, η καταστροφή τους, καθώς και η διακοπή πρόσβασης σε αυτά οδηγούν στη δυσλειτουργία και στη δυσφήμισή του.

Γενικότερα, ως δεδομένα θεωρούνται τα δεδομένα που ανταλλάσσονται μέσω ηλεκτρονικών μηνυμάτων, τα δεδομένα που βρίσκονται αποθηκευμένα σε ηλεκτρονική ή άλλη μορφή. Τα δεδομένα αυτά είναι προσβάσιμα από όλα τα συστήματα μέσω του εσωτερικού δικτύου ή μέσω Remote Desktop με χρήση Secure Shell (SSH), όπου χρειάζεται αυθεντικοποίηση του διαχειριστή. Οι διαδικασίες κατά τις οποίες εμπλέκεται μεταφορά και αποθήκευση δεδομένων είναι πάρα πολλές και για αυτό το λόγο τα δεδομένα θεωρήθηκαν από την ομάδα ανάλυσης κρίσιμο αγαθό.

Το σύστημα είναι υπεύθυνο για την ομαλή μεταφορά των δεδομένων και οι βασικές συνιστώσες της ασφάλειας που οφείλει να ακολουθεί είναι οι εξής:

- Εμπιστευτικότητα: Η πρόσβαση στα δεδομένα που έχει ο διαχειριστής διαβαθμίζεται με στόχο να προστατεύονται από κακόβουλες ενέργειες.
- Ακεραιότητα: Δυνατότητα τροποποίησης έχουν μόνο οι διαχειριστές.
- Διαθεσιμότητα: Όλα τα δεδομένα πρέπει να είναι διαθέσιμα ανά πάσα ώρα και στιγμή, καθώς από τις σωστές πληροφορίες κρίνεται η εύρυθμη λειτουργία του συστήματος.

3.4.1. Απειλές Μέσω Δικτυακής Πρόσβασης

Όσον αφορά στην πρόσβαση μέσω του δικτύου, οι απειλές μπορούν να προέρχονται, τόσο από το εσωτερικό, όσο και από το εξωτερικό του συστήματος, με ή χωρίς σκοπό. Οι επιπτώσεις των απειλών αυτών είναι στην φήμη του συστήματος και στις παραγωγικές διαδικασίες.

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Όσον αφορά στις εσωτερικές μη σκόπιμες απειλές, παρατηρείται ότι η αποκάλυψη, η τροποποίηση, η απώλεια / καταστροφή ή η μη διαθεσιμότητα των δεδομένων μπορούν να έχουν αρνητικές επιπτώσεις για το σύστημα. Για παράδειγμα, αν κάποιος χρήστης άθελα του μπορέσει να έχει πρόσβαση στο σύστημα ως διαχειριστής, τότε μπορεί εξαιτίας της αμέλειας του και της άγνοιας του να επέμβει στις ρυθμίσεις των διαφόρων προγραμμάτων του συστήματος. Αυτό μπορεί να έχει ως αποτέλεσμα να

μην είναι δυνατόν να συλλεχθούν οι πληροφορίες είτε από την βάση δεδομένων είτε από το διαδίκτυο, ή να μην μπορεί να αποκριθεί στα αιτήματα που δέχεται Αξίζουμε να αναφέρουμε ότι μια άλλη περίπτωση όπου ενδεχομένως μπορεί να έχουμε κάποιο πρόβλημα στο σύστημα, είναι κατά τον απομακρυσμένο έλεγχο από έναν εκ των διαχειριστών, να πραγματοποιηθεί κάποια λάθος κίνηση. Σε αυτό το σημείο καλό θα ήταν να οριστούν οι πιθανότητες των παραπάνω γεγονότων. Έτσι με απόλυτη βεβαιότητα:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Μέτριος
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Μέτριος

Και αυτό θα επιφέρει ζημίες στους παρακάτω τομείς:

	Αποκαλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Χαμηλή	Υψηλή	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Χαμηλή	Υψηλή	Μέτρια
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Η τελική απόφαση που λαμβάνεται μετά από τον συμψηφισμό των αποτελεσμάτων είναι ότι πρέπει να ληφθούν από τους διαχειριστές του συστήματος μέτρα, ώστε να προστατευθούν τα δεδομένα από όλες τις εσωτερικές μη σκόπιμες απειλές μέσω δικτύου.

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Όπως με τις μη σκόπιμες απειλές έτσι και οι σκόπιμες εξετάζονται για τις συνέπειες που αποφέρουν στην περίπτωση αποκάλυψης, τροποποίησης, απώλειας ή καταστροφής και διακοπής του συστήματος. Καθώς οι διαχειριστές είναι ενήμεροι για την πολιτική ασφάλειας που εφαρμόζεται, η πιθανότητα να συμβεί κάτι σκόπιμα είναι χαμηλή. Ο ανθρώπινος παράγοντας είναι αστάθμητος και για αυτό γίνεται όλη αυτή η διαδικασία.

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Χαμηλή	Υψηλή	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Χαμηλή	Υψηλή	Μέτρια
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Καθώς πρόκειται σε γενικές γραμμές για ένα σύστημα με περιορισμένο αριθμό ανθρώπινου δυναμικού, υπάρχει χαμηλό κίνητρο για οποιονδήποτε δράστη. Ως αποτίμηση αυτών των παραγόντων συνιστάται το σύστημα να μην αλλάξει την λειτουργία της, ώστε να αντιμετωπίσει τέτοιου είδους απειλές.

Μη σκόπιμες απειλές από εξωτερικούς παράγοντες:

Οι χρήστες του συστήματος, μπορούν να προκαλέσουν δυσλειτουργίες στο σύστημα, και το επιτυγχάνουν αυτό με τη ταυτόχρονη μαζική αποστολή μηνυμάτων με αιτήματα στο σύστημα. Βέβαια για να προκληθεί αυτή η δυσλειτουργία, είναι απαραίτητο το σύνολο των μηνυμάτων να ξεπερνά των αριθμό των 50.000 (πενήντα χιλιάδων) ανά δευτερόλεπτο. Αυτό θα έχει ως αποτέλεσμα να μην μπορεί το σύστημα να αποκριθεί σε όλα τα αιτήματα και έτσι να βρεθεί σε κατάσταση άρνησης εξυπηρέτησης (Denial of Service).

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Χαμηλή	Χαμηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Χαμηλή	Χαμηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από εξωτερικούς παράγοντες:

Ενδεχομένως κάποιος κακόβουλος χρήστης επιθυμεί να βλάψει την υπόληψη του συστήματος. Ωστόσο λόγω του μεγέθους του, μπορεί να είναι λιγότερο δύσκολο να συμβεί, αλλά αν πράγματι συμβεί κρύβει πολλές ζημίες.

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Όπως έχει ήδη θεωρηθεί, το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε είναι ένα σύστημα με περιορισμένο αριθμό εργαζομένων, που είναι μόνο οι διαχειριστές του συστήματος, γεγονός το οποίο αποτελεί, όπως εκτιμήθηκε, μέτριο κίνητρο για κάποιο επίβουλο χρήστη. Ο συγκεκριμένος επίβουλος χρήστης είναι δυνατό είτε να εκμεταλλευτεί αδυναμία συστημάτων τέτοιου είδους είτε να εκτελεί εντολές για προσωπική ικανοποίηση. Για αυτό και οι διαχειριστές του συστήματος θα πρέπει να δώσουν μεγαλύτερη έμφαση στην διαφύλαξη των δεδομένων.

3.4.2. Απειλές Μέσω Φυσικής Πρόσβασης

Στην περίπτωση της φυσικής πρόσβασης, οι απειλές μπορούν να προέρχονται, μόνο από το εσωτερικό του συστήματος και μπορούν να είναι, είτε σκόπιμες, είτε μη σκόπιμες. Το σύστημα μπορεί να έχει συνέπειες από τις επιπτώσεις των απειλών αυτών στην υπόληψή του και στην παραγωγική του διαδικασία.

Μη σκόπιμες απειλές από το εσωτερικό του συστήματος:

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Μέτριος
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Μέτριος

Οι διαχειριστές του συστήματος, μπορούν να προκαλέσουν δυσλειτουργίες στο σύστημα, εάν κάποιος εκ των διαχειριστών, πραγματοποιήσει κάποια λάθος κίνηση. Αυτό μπορεί να έχει ως αποτέλεσμα να μην μπορεί το σύστημα να αποκριθεί σε όλα τα αιτήματα που δέχεται και έτσι να βρεθεί σε κατάσταση άρνησης εξυπηρέτησης (Denial of Service).

Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Μέτρισ	Υψηλή	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Μέτρια	Υψηλή	Μέτρια
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από το εσωτερικό του συστήματος:

Οι διαχειριστές του συστήματος, μπορούν να προκαλέσουν δυσλειτουργίες στο σύστημα, και το επιτυγχάνουν αυτό με τροποποίηση των πληροφοριών, τις οποίες διαχειρίζεται το σύστημα ή ακόμα να το υπερφορτώσουν, ώστε να βρεθεί σε κατάσταση άρνησης εξυπηρέτησης (Denial of Service).

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Μη σκόπιμες απειλές από εξωτερικούς παράγοντες:

Οι εξωτερικοί παράγοντες μπορούν να προκαλέσουν δυσλειτουργίες στο σύστημα, και το επιτυγχάνουν αυτό, για παράδειγμα εάν κάποιος εισέλθει στο χώρο όπου βρίσκεται εγκατεστημένο το πληροφοριακό σύστημα του τμήματος Μηχανικών

πληροφορικής, και χωρίς την θέλησή του προκαλέσει βλάβη στο σύστημα, όπως να χυθεί υγρά στο τερματικό.

Επίσης εάν με οποιοδήποτε τρόπο έχει πρόσβαση στο τερματικό και από περιέργεια επεξεργαστεί το σύστημα, τότε μπορεί να προκαλέσει τροποποίηση των δεδομένων, ακόμη και απώλεια ή καταστροφή αυτών.

Αυτό θα έχει ως αποτέλεσμα να μην μπορεί το σύστημα να αποκριθεί σε όλα τα αιτήματα και έτσι να βρεθεί σε κατάσταση άρνησης εξυπηρέτησης (Denial of Service).

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Μέτριος
Τροποποίηση	Μέτριος
Απώλεια ή καταστροφή	Υψηλός
Διακοπή Λειτουργίας	Υψηλός

Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Οικονομικά	Χαμηλή	Χαμηλή	Μέτρια	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

Σκόπιμες απειλές από εξωτερικούς παράγοντες:

Αυτή η περίπτωση περιλαμβάνει κατασκοπεία και χρηματισμό εξωτερικών παραγόντων. Μπορεί να συμβεί κάτι τέτοιο, αλλά είναι δύσκολο λόγω του ότι το σύστημα αποτελεί υλοποίηση διπλωματικής εργασίας προπτυχιακών φοιτητών και έτσι είναι φύση αδύνατον να συμβεί. Οπότε αν συμβεί κάποια παρατυπία είναι πολύ εύκολο να διαπιστωθεί.

Γεγονός	Βαθμός Βεβαιότητας
Αποκάλυψη	Χαμηλός
Τροποποίηση	Χαμηλός
Απώλεια ή καταστροφή	Χαμηλός
Διακοπή Λειτουργίας	Χαμηλός

Αυτά θα επιφέρουν ζημίες στους παρακάτω τομείς:

	Αποκάλυψη	*Τροποποίηση*	*Απώλεια / Καταστροφή*	*Διακοπή λειτουργίας*
Φήμη	Μέτρια	Υψηλή	Υψηλή	Μέτρια
Οικονομικά	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή
Παραγωγικότητα	Μέτρια	Υψηλή	Υψηλή	Μέτρια
Πρόστιμα	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή

3.4.3. Απειλές Μέσω Άλλων Προβλημάτων

Ένα από τα προβλήματα που μπορεί να προκύψουν και δεν μπορούν να ελεχθούν από τη μεριά του συστήματος είναι προβλήματα από κατάρρευση του δικτύου του ΤΕΙ Πελοποννήσου στο τμήμα Μηχανικών πληροφορικής στο σύστημα του

πληροφοριακού συστήματος από τη χαμηλή εκπομπή σήματος καταστροφή του ηλεκτρολογικού εξοπλισμού και εκδήλωση φυσικών καταστροφών, όπως είναι ο σεισμός και η πυρκαγιά. Τέλος, θα πρέπει να υπάρχει μια μακροπρόθεσμη απόδοση επένδυσης γι' αυτό το σύστημα, γεγονός που οικονομικά δαπανούνται αρκετά χρήματα.

Δεν είναι λίγες οι φορές που εξωτερικοί παράγοντες επηρεάζουν το περιβάλλον ενός συστήματος ακούσια. Χαρακτηριστική και ιδιαίτερα καταστροφική είναι η περίπτωση υπερβολικής τροφοδοσίας ηλεκτρικού ρεύματος, η οποία αντιμετωπίζεται με την ύπαρξη UPS, ή η διακοπή παροχής ηλεκτρικού ρεύματος από τη ΔΕΗ στο εσωτερικό δίκτυο του συστήματος. για να πληροφορήσει τους διαχειριστές ότι δεν υπάρχει παροχή δικτύου. Έτσι, οι διαχειριστές του συστήματος έχουν την δυνατότητα να επισκεφθούν τον χώρο όπου είναι εγκατεστημένο το σύστημα και να ελέγξουν για ποιο λόγο δεν είναι διαθέσιμο το δίκτυο (π.χ. απόσπαση του καλωδίου από τη θύρα του υπολογιστή του συστήματος). Επίσης, το σύστημα είναι προγραμματισμένο αν υπάρχει πρόβλημα να ενημερώσει αυτόματα το τεχνικό προσωπικό και να πληροφορήσει ότι το δίκτυο έχει επανέλθει και λειτουργεί κανονικά. Η διακοπή του ηλεκτρικού ρεύματος ελλοχεύει την πιθανότητα να έχει σαν αποτέλεσμα την ολική καταστροφή του server ή / και των ηλεκτρονικών υπολογιστών ή μερών αυτών. Επομένως, το γεγονός ότι δεν έχουν ληφθεί μέτρα ώστε να υπάρχει τροφοδότηση ρεύματος στο δίκτυο, μέσω γεννήτριας παραγωγής ηλεκτρικού ρεύματος, όταν γίνεται διακοπή ρεύματος από τη ΔΕΗ, είναι βασικό μειονέκτημα του συστήματος. Το εσωτερικό δίκτυο του συστήματος απειλείται από φυσικές καταστροφές, όπως κεραυνό ή σεισμό.

Άρα, τα προβλήματα του συστήματος για το εσωτερικό της δίκτυο έχουν:

Γεγονός	Βαθμός Βεβαιότητας
Απώλεια ή καταστροφή	Υψηλός
Διακοπή Λειτουργίας	Υψηλός

Αυτά επιφέρουν ζημιές στους παρακάτω τομείς:

	Απώλεια / Καταστροφή	*Διακοπή λειτουργίας*
Φήμη	Υψηλή	Υψηλή
Οικονομικά	Μέτρια	Μέτρια
Παραγωγικότητα	Υψηλή	Υψηλή
Πρόστιμα	Χαμηλή	Χαμηλή

Ο βαθμός βεβαιότητας είναι υψηλός, αφού γίνεται αναφορά σε φυσικά φαινόμενα και σε περιπτώσεις που μπορούν να επηρεάσουν την λειτουργία του συστήματος.

4. Τεκμηρίωση της Ασφάλειας

4.1. Πολιτική Ασφάλειας του ΤΕΙ Πελοποννήσου

Εισαγωγή

Η πολιτική ασφάλειας περιέχει το σύνολο των κανόνων που καθορίζουν τον τρόπο που η Διοίκηση του ΤΕΙ Πελοποννήσου στο τμήμα Μηχανικών πληροφορικής Τ.Ε με έδρα την Σπάρτη πρέπει να διαχειρίζεται και να προστατεύει τους πόρους του το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε ώστε να επιτυγχάνονται συγκεκριμένοι στόχοι ασφάλειας. Στόχος της Πολιτικής Ασφάλειας είναι η καθοδήγηση των διαχειριστών του συστήματος όσο αφορά την προστασία του συγκεκριμένου πληροφοριακού συστήματος. Η Πολιτική Ασφάλειας πρέπει να είναι δυναμική και προσαρμόσιμη ακολουθώντας τις εκάστοτε αλλαγές της πληροφοριακής υποδομής.

Η παρούσα Πολιτική Ασφάλειας βασίστηκε στα αποτελέσματα της ανάλυσης επικινδυνότητας, στις απαιτήσεις της **Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** και στις απαιτήσεις της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε).

4.2. Σκοπός & χρησιμότητα της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας δρομολογεί την λήψη αποφάσεων σε όλες τις βαθμίδες της διοίκησης. Επίσης με την βοήθεια της Πολιτικής Ασφάλειας επιτυγχάνονται οι παρακάτω στόχοι:

- Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων και τη διασφάλιση του απορρήτου των επικοινωνιών.
- Διασφάλιση της επιχειρησιακής της ικανότητας, στο βαθμό που εξαρτάται από την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα πληροφοριών και επικοινωνιών.
- Προστασία της επένδυσης που απαιτεί η λειτουργία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου με έδρα την Σπάρτη.

4.2.1 Εμβέλεια της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας όσο αφορά το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου Καλύπτει το σύνολο των πληροφοριών που διακινούνται, τυγχάνουν επεξεργασίας ή αποθηκεύονται σε ηλεκτρονική μορφή, επεκτείνεται, όμως και στις περιπτώσεις όπου οι ανωτέρω πληροφορίες μετατρέπονται σε άλλες μορφές. Να υπάρχει εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή. Για παράδειγμα: με την κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα του ΤΕΙ Πελοποννήσου, να υπάρχει διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση

Η ανάπτυξη της πολιτικής ασφάλειας όσο αφορά το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής βασίζεται στην καταγραφή των απαιτήσεων ασφάλειας, με βάση τις οποίες διαμορφώνονται οι στόχοι της ασφάλειας, και στον προσδιορισμό των τρόπων για την επίτευξη των στόχων αυτών. Οι απαιτήσεις ασφάλειας μπορεί να προέρχονται από διαφορετικές πηγές, όπως:

Οι χρήστες των πληροφοριακών συστημάτων.

- Η διοίκηση του οργανισμού που επιθυμεί την απρόσκοπτη χρήση των πληροφοριακών συστημάτων στις λειτουργίες του οργανισμού.
- Οι πελάτες του οργανισμού, εφόσον δεδομένα που τους αφορούν αποτελούν συνιστώσα του πληροφοριακού συστήματος.
- Το νομικό και ρυθμιστικό πλαίσιο στο οποίο λειτουργεί το ΤΕΙ Πελοποννήσου

Η πολιτική ασφάλειας θα πρέπει να ικανοποιεί όλες τις απαιτήσεις ασφάλειας που προκύπτουν για το πληροφοριακό σύστημα στο τμήμα Μηχανικών πληροφορικής ,

και μάλιστα με αναλογικό τρόπο, δηλαδή τα μέτρα και οι οδηγίες που περιλαμβάνει να εξασφαλίζουν το επιθυμητό επίπεδο ασφάλειας.

4.2.2. Περιορισμοί

Η Πολιτική Ασφάλεια περιορίζεται στο εν λόγω σύστημα του ΤΕΙ Πελοποννήσου καθώς η ανάλυση επικινδυνότητας που πραγματοποιήθηκε αφορούσε αυτό το σύστημα. Η διαμόρφωση της παρούσας πολιτικής έχει ως αφετηρία τα προβλεπόμενα στο πρότυπο ISO / IEC 17799 και η εφαρμογή της οδηγεί σε συμμόρφωση με το πρότυπο αυτό. Επίσης, καλύπτει τις σχετικές απαιτήσεις της **Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** και της σχετικής νομοθεσίας.

Η παρούσα πολιτική δεν αναφέρεται στο φυσικό επικοινωνιακό δίκτυο.

4.2.3. Αξιοποίηση της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας βασίστηκε στις εκτιμήσεις των μελετητών του έργου σχετικά με τις απαιτήσεις ασφάλειας της οργάνωσης, λειτουργίας και τεχνικής υποδομής του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε. Εντούτοις, η Πολιτική Ασφάλειας είναι άμεσα εξαρτημένη από τη φύση των δραστηριοτήτων του ιδρύματος, τις κατευθύνσεις της διοίκησης και το περιβάλλον λειτουργίας του ιδρύματος.

Για την κατανόηση και αξιοποίηση της Πολιτικής Ασφαλείας παρατίθενται οι παρακάτω κανόνες:

- Η Πολιτική Ασφάλειας αποτελεί γενικά διαθέσιμο υπηρεσιακό κείμενο και πρέπει να ληφθεί μέριμνα, ώστε όλα τα μέλη του προσωπικού που έχουν ρόλο στη λειτουργία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε είτε ως χρήστες, είτε ως διαχειριστές, είτε ως διοικητικά στελέχη, να λάβουν γνώση της.
- Η Πολιτική Ασφάλειας είναι δυναμική. Βασίστηκε στη μελέτη επικινδυνότητας.

4.2.4. Δομή της Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας αποτελείται από επιμέρους εξειδικευμένες πολιτικές. Αναλυτικά παρατίθεται παρακάτω η δομή της Πολιτικής Ασφάλειας:

1. Πολιτική Διαχείρισης Ασφάλειας του πληροφοριακού συστήματος του

τμήματος Μηχανικών πληροφορικής Τ.Ε

2. Πολιτική Προσωπικού (Διαχειριστών)
3. Πολιτική Πρακτικών Θεμιτής Χρήσης
4. Πολιτική Προστασίας Προσωπικών Δεδομένων και Επικοινωνιών
5. Πολιτική Συνεργατών
6. Πολιτική Προστασίας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Η καθεμία από τις παραπάνω Πολιτικές αναπτύσσονται στη συνέχεια. Επίσης η δομή της κάθε Πολιτικής είναι η ακόλουθη:

a) Σκοπός,
b) Εμβέλεια,
c) Γενικές αρχές &
d) Οδηγίες και κανόνες ασφάλειας.

4.3. Πολιτική Διαχείρισης Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Εισαγωγή

Η συγκεκριμένη πολιτική του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε εκφράζει την πρόθεση του ιδρύματος να προστατέψει την πληροφοριακή του υποδομή. Επιπρόσθετα παρέχονται οι κατευθύνσεις για την διαχείριση της ασφάλειας τους έτσι ώστε να δύναται να αντεπεξέλθει το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε σε μεγάλο αριθμό χρηστών.

Σκοπός

Ο σκοπός της Πολιτικής Διαχείρισης Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε φαίνεται παρακάτω:

- Το ΤΕΙ Πελοποννήσου να διασφαλίσει την λειτουργία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

- Η καθοδήγηση του διοικητικού προσωπικού ΤΕΙ Πελοποννήσου για τον τρόπο με τον οποίο πρέπει να αντιμετωπίζονται τα ζητήματα ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Η προδιαγραφή ενός Συστήματος Διαχείρισης της Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Εμβέλεια

Η πολιτική καλύπτει το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε να είναι υποχρεωτική και να αποτελεί αναπόσπαστο κομμάτι της Πολιτικής Ασφάλειας. Ακόμη η Πολιτική απευθύνεται στο διοικητικό προσωπικό του ΤΕΙ Πελοποννήσου που υποστηρίζει την λειτουργία το πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Γενικές Αρχές

- Βούληση της διοίκησης

Το ΤΕΙ Πελοποννήσου δίνει υψηλή προτεραιότητα στην ασφάλεια που υποστηρίζει την λειτουργία το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε

- Η Πολιτική Ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε.

Το ΤΕΙ Πελοποννήσου θέτει σε ισχύ την Πολιτική Ασφάλεια του η οποία αποτελείται από την παρούσα Πολιτική Διαχείρισης Ασφάλειας και από ένα σύνολο θεματικών Πολιτικών Ασφάλειας.

- Υποστήριξη εφαρμογής της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Η διοίκηση ΤΕΙ Πελοποννήσου υποστηρίζει την εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε εξασφαλίζοντας τους απαραίτητους πόρους και μέσα.

- Διοικητική και οργανωτική υποστήριξη διαχείρισης της ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε Με στόχο την αποτελεσματικότερη εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε αναπτύσσεται η κατάλληλη διοικητική δομή, ορίζονται οι ρόλοι που είναι απαραίτητοι για τη διαχείριση της ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε καθορίζονται οι αρμοδιότητες για κάθε ρόλο και ανατίθενται οι ρόλοι στα κατάλληλα άτομα.

- Συμμόρφωση με νομικό πλαίσιο

Η διοίκηση ΤΕΙ Πελοποννήσου προβαίνει σε όλες τις ενέργειες που απαιτούνται για να γίνεται σεβαστή η νομοθεσία που αφορά στην προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά η νομοθεσία που αφορά τη χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Οδηγίες και κανόνες ασφάλειας

Α. Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

1. Η Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε πρέπει να είναι έγγραφη και επικυρωμένη από τη διοίκηση του ΤΕΙ Πελοποννήσου
2. Το ΤΕΙ Πελοποννήσου οφείλει να προβαίνει σε όλες τις απαραίτητες ενέργειες, ώστε να ενημερώνει το προσωπικό για την Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε και να εξασφαλίζει άμεση και εύκολη πρόσβαση του προσωπικού στο πλήρες κείμενο της Πολιτικής Ασφάλειας.
3. Η Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε καθορίζεται με βάση την επικινδυνότητα που ενέχεται στη λειτουργία, του πληροφοριακού συστήματος του τμήματος

Μηχανικών πληροφορικής Τ.Ε όπως αυτή αποτιμάται με την εκπόνηση μελέτης ανάλυσης επικινδυνότητας

4. Η Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε πρέπει να τυγχάνει τακτικής ενημέρωσης και να αναθεωρείται και επικαιροποιείται σε περίπτωση μειζόνων αλλαγών στο πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε καθώς και σε περιπτώσεις σημαντικών μεταβολών του κοινωνικού και τεχνολογικού περιβάλλοντος, από τις οποίες προκύπτουν νέες απειλές, ευπάθειες, ή νέες ευκαιρίες βελτίωσης της ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε. Οι διαδικασίες αναθεώρησης της Πολιτικής περιλαμβάνονται στο Σχέδιο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
5. Το προσωπικό ΤΕΙ Πελοποννήσου και οι διαχειριστές του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε πρέπει να συμβουλεύονται την Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε σε κάθε απόφασή τους, που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα, την ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
6. Η εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε είναι υποχρεωτική. Σε περίπτωση παραβίασης της Πολιτικής, το ΤΕΙ Πελοποννήσου έχει το δικαίωμα να επιβάλλει κυρώσεις.

Β. Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο

1. Το ΤΕΙ Πελοποννήσου δεσμεύεται για την τήρηση της νομοθεσίας που αφορά την προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά τη νομοθεσία που αφορά τη χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε καθώς και για την εφαρμογή των σχετικών αποφάσεων της Αρχής Προστασίας Προσωπικών Δεδομένων.

2. Το ΤΕΙ Πελοποννήσου διαμορφώνει μία Πολιτική Αποδεκτής Χρήσης που απευθύνεται στους χρήστες των υπηρεσιών της και περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες. Η πολιτική αυτή πρέπει να είναι συνοπτική και να δημοσιοποιείται.

3. Το ΤΕΙ Πελοποννήσου καταρτίζει και εφαρμόζει διαδικασίες που διασφαλίζουν τη διατήρηση των δεδομένων των επικοινωνιών για το χρονικό διάστημα που ορίζει η νομοθεσία.

4. Το ΤΕΙ Πελοποννήσου προβαίνει σε όλες τις ενέργειες που απαιτούνται, ώστε να παρέχει στις Αρχές διευκολύνσεις και πληροφορίες, όπως προβλέπει η σχετική νομοθεσία. Το ΤΕΙ Πελοποννήσου διασφαλίζει ότι οι σχετικές διευκολύνσεις και πληροφορίες παρέχονται μόνο στις περιπτώσεις που προβλέπονται από τη νομοθεσία, ακολουθώντας νόμιμες διαδικασίες.

5. Η Διοίκηση του ΤΕΙ Πελοποννήσου μεριμνά ώστε όλα τα μέλη του προσωπικού να γνωρίζουν τις υποχρεώσεις τους που απορρέουν από τη νομοθεσία σχετικά με την επεξεργασία προσωπικών πληροφοριών και τη διασφάλιση του απορρήτου των επικοινωνιών.

6. Η Διοίκηση μεριμνά για την ανάπτυξη οργανωτικών δομών και διαδικασιών με στόχο την προστασία του ΤΕΙ Πελοποννήσου από νομικές ενέργειες που στρέφονται εναντίον του.

7. Το ΤΕΙ Πελοποννήσου μεριμνά για την προστασία του προσωπικού από νομικές συνέπειες που μπορεί να προκύψουν από ενέργειές τους στα πλαίσια της άσκησης των καθηκόντων τους και εφόσον τηρούν πιστά τις πολιτικές και τους κανονισμούς του ΤΕΙ Πελοποννήσου.

Γ. Οργανωτική υποδομή

Το ΤΕΙ Πελοποννήσου αναπτύσσει κατάλληλες οργανωτικές δομές για την αποτελεσματική διαχείριση ασφάλειας του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε. Η ευθύνη για την διαχείριση ανατίθεται σε ξεχωριστό άτομο, τον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε.

Δ. Εκπαίδευση και ενημέρωση

1. Η Διοίκηση μεριμνά, ώστε χρήστες, διαχειριστές, στελέχη που αναλαμβάνουν ρόλους σχετικούς με την ασφάλεια του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε και γενικότερα το προσωπικό του ΤΕΙ Πελοποννήσου που σχετίζεται με την λειτουργία του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε να λαμβάνει την απαραίτητη εκπαίδευση, ευαισθητοποίηση και κατάρτιση σε θέματα ασφάλειας του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε.

2. Η Διοίκηση μεριμνά ώστε να είναι διαθέσιμη πηγή πληροφόρησης για ζητήματα ασφάλειας, καθώς και εκπαιδευτικό υλικό σε όλο το προσωπικό του ΤΕΙ Πελοποννήσου

3. Περίληψη της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε χορηγείται στο προσωπικό του ΤΕΙ Πελοποννήσου (μόνιμο ή προσωρινό), καθώς και στους προμηθευτές υπηρεσιών ή στους αναδόχους έργων που μπορεί να επηρεάσουν την ασφάλεια του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε

4. Όλα τα νέα μέλη του προσωπικού να ακολουθούν ένα βασικό πρόγραμμα εκπαίδευσης, το οποίο περιλαμβάνει και ζητήματα ασφάλειας του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε

5. Τα διοικητικά στελέχη ΤΕΙ Πελοποννήσου οφείλουν να εφαρμόζουν υποδειγματικά την Πολιτική Ασφάλειας του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε και τις διαδικασίες ασφάλειας που απορρέουν από αυτήν, αποδεικνύοντας με τον τρόπο αυτό την αυξημένη σημασία που έχει στην ασφάλεια του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε

Ε. Έλεγχος Εφαρμογής της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικός Τ.Ε

1. Πραγματοποιούνται τακτικοί και έκτακτοι έλεγχοι από τον Υπεύθυνο Ασφάλειας (ή κάποιος από τους διαχειριστές) του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε

2. Ο Υπεύθυνος Ασφάλειας του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε λειτουργεί κατά κύριο λόγο συμβουλευτικά και κατά δεύτερο λόγο ελεγκτικά, έχοντας ως στόχο των ελέγχων τη βελτίωση του επιπέδου ασφάλειας του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε.

4.4. Πολιτική Προσωπικού -Διαχειριστών

Εισαγωγή

Όπως δείχνουν σχετικές μελέτες, ο σημαντικότερος παράγοντας στην ασφάλεια του πληροφοριακού συστήματος Μηχανικών πληροφορικής Τ.Ε είναι η συμπεριφορά και η δράση των ανθρώπων που μετέχουν της λειτουργίας του συστήματος ως χρήστες ή ως διαχειριστές των συστήματος ή ασκώντας διοικητικά καθήκοντα.

Το ΤΕΙ Πελοποννήσου, αναγνωρίζοντας το σημαντικό ρόλο που διαδραματίζουν τα μέλη του προσωπικού στην προσπάθεια διασφάλισης της πληροφοριακής και επικοινωνιακής υποδομής του, ανέπτυξε και θέτει σε εφαρμογή την παρούσα Πολιτική Προσωπικού.

Σκοπός

Σκοπός της Πολιτικής Προσωπικού είναι:

- Η μείωση της επικινδυνότητας που συνδέεται με ανθρώπινα λάθη, με την πιθανή κατάχρηση του συστήματος, καθώς και με κάθε εκούσια ή ακούσια ενέργεια που μπορεί να θέσει σε κίνδυνο το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Η ενίσχυση της ενεργούς συμμετοχής του προσωπικού στη συλλογική προσπάθεια ενδυνάμωσης της ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Εμβέλεια

Η Πολιτική Προσωπικού απευθύνεται στο σύνολο του προσωπικού του ΤΕΙ Πελοποννήσου που κατά την άσκηση των καθηκόντων του επηρεάζει τη λειτουργία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε , είτε ως χρήστης, είτε ως διαχειριστής, είτε ασκώντας διοικητικά καθήκοντα. Η Πολιτική

Προσωπικού αφορά ιδιαίτερα τα στελέχη του ΤΕΙ Πελοποννήσου. που έχουν ως αρμοδιότητα τη διαχείριση του ανθρώπινου δυναμικού.

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Γενικές αρχές

- Ρόλος του ανθρώπινου δυναμικού.

Το ΤΕΙ Πελοποννήσου. αποδίδει ιδιαίτερη βαρύτητα στο ρόλο που διαδραματίζει το ανθρώπινο δυναμικό στην προσπάθεια διασφάλισης του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

- Ενίσχυση του ανθρώπινου δυναμικού.

Το ΤΕΙ Πελοποννήσου προβαίνει σε όλες τις απαιτούμενες ενέργειες για την ενίσχυση του προσωπικού του με μέσα, κατευθυντήριες οδηγίες, πληροφόρηση και γνώση, ώστε να συμβάλλει με τον πλέον αποτελεσματικό τρόπο στην ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

- Υποχρέωση ενεργούς συμμετοχής.

Όλα τα μέλη του προσωπικού έχουν την υποχρέωση να συμβάλλουν ενεργά στην ασφάλεια της πληροφορικής και επικοινωνιακής υποδομής του ΤΕΙ Πελοποννήσου και να απέχουν από κάθε ενέργεια που μπορεί να θέσει σε κίνδυνο την ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Οδηγίες και κανόνες ασφάλειας

Α. Διαχείριση ανθρώπινου δυναμικού

1. Το ΤΕΙ Πελοποννήσου στελεχώνει θέσεις που είναι σημαντικές για την ασφαλή και αποτελεσματική λειτουργία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε επιλέγοντας προσωπικό με κατάλληλα τυπικά και ουσιαστικά προσόντα.

2. Το ΤΕΙ Πελοποννήσου. διατηρεί το δικαίωμα πρόσβασης στα δεδομένα που δημιουργούνται και αποθηκεύονται στο πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε με τέτοιο τρόπο, ώστε να μην παραβιάζονται τα έννομα δικαιώματα των χρηστών του.

Β. Γενικές υποχρεώσεις προσωπικού

1. Όλα τα μέλη του προσωπικού έχουν την υποχρέωση να συμβάλλουν θετικά στην ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου.

2. Όλα τα μέλη του προσωπικού οφείλουν να σέβονται την ιδιωτικότητα (privacy) των συναδέλφων τους.

3. Το προσωπικό έχει την υποχρέωση να αποφεύγει τα δημόσια δυσφημιστικά σχόλια για φοιτητές ή συνεργάτες του ΤΕΙ Πελοποννήσου.

4. Τα μέλη του προσωπικού έχουν την υποχρέωση να αναφέρουν οποιοδήποτε γεγονός ή ενέργεια θεωρούν ότι περιορίζει την ασφάλεια του τμήματος Μηχανικών πληροφορικής Τ.Ε. Η Διοίκηση οφείλει να χρησιμοποιεί αυτές τις πληροφορίες με διακριτικό τρόπο.

4.4. Πολιτική Θεμιτών Πρακτικών Χρήσης του πληροφοριακού συστήματος του τιμήματος Μηχανικών πληροφορικής Τ.Ε

Εισαγωγή

Η Πολιτική Θεμιτών Πρακτικών Χρήσης του τιμήματος Μηχανικών πληροφορικής Τ.Ε ρυθμίζει τα ζητήματα που αφορούν στη χρήση του τιμήματος Μηχανικών πληροφορικής Τ.Ε που υποστηρίζει τις δραστηριότητες του ΤΕΙ Πελοποννήσου.. Με την έκδοση της πολιτικής αυτής δίνεται η δυνατότητα στους χρήστες του τμήματος Μηχανικών πληροφορικής Τ.Ε να γνωρίζουν ποιες ενέργειές τους θεωρούνται επιτρεπτές και ποιες απαγορεύονται.

Σκοπός

Σκοπός της Πολιτικής Θεμιτών Πρακτικών Χρήσης του τμήματος Μηχανικών πληροφορικής Τ.Ε είναι:

- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από

κακή χρήση του τιμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου

- Η προστασία των χρηστών του τμήματος Μηχανικών πληροφορικής Τ.Ε από τις συνέπειες που μπορεί να υποστούν από την εσφαλμένη χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε.
- Η διασφάλιση ότι οι χρήστες δεν θα καταχραστούν τις δυνατότητες χρήσης του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε που τους παρέχονται προκειμένου να προβούν σε παράνομες ενέργειες.

Εμβέλεια

- Η πολιτική αυτή απευθύνεται στα μέλη του προσωπικού του ΤΕΙ Πελοποννήσου. και στους συνεργάτες του ΤΕΙ Πελοποννήσου που χρησιμοποιούν το πληροφοριακό σύστημα του τιμήματος Μηχανικών πληροφορικής Τ.Ε
- Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε.

Γενικές αρχές

- Το πληροφοριακό σύστημα του τιμήματος Μηχανικών πληροφορικής Τ.Ε ως περιουσιακό στοιχείο
- Το πληροφοριακό σύστημα του τιμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου αποτελεί περιουσιακό του στοιχείο και η χρήση του πρέπει να γίνεται αποκλειστικά για τους σκοπούς ΤΕΙ Πελοποννήσου
- Υποχρεώσεις συνδεόμενες με τη χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε.
- Η χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε. συνεπάγεται την ανάληψη ευθυνών και υποχρεώσεων που περιγράφονται στην Πολιτική Θεμιτών Πρακτικών Χρήσης του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε.

Οδηγίες και κανόνες ασφάλειας

Α. Δικαιώματα και υποχρεώσεις χρηστών

1. Το προσωπικό δικαιούται να χρησιμοποιεί πληροφοριακό σύστημα του τιμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου σύμφωνα με τα όσα προβλέπονται στην παρούσα Πολιτική Θεμιτών Πρακτικών Χρήσης του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε.
2. Το προσωπικό πρέπει να χρησιμοποιεί σωστά το πληροφοριακό σύστημα του τιμήματος και να μην αρκείται στην κατά γράμμα εφαρμογή της Πολιτικής Θεμιτών Πρακτικών Χρήσης του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε., ενώ σε κάθε περίπτωση που κάποιο μέλος του προσωπικού αμφιβάλλει αν κάποια ενέργειά του είναι συμβατή με την πολιτική, θα πρέπει να απευθύνεται στον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε.
3. Οι χρήστες έχουν το δικαίωμα της ενημέρωσης σχετικά με τα δεδομένα που συλλέγονται από το ΤΕΙ Πελοποννήσου. και αφορούν τη χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε. από αυτούς.
4. Τα δεδομένα που δημιουργούνται με τη χρήση του τμήματος Μηχανικών πληροφορικής Τ.Ε. από αυτούς του ΤΕΙ Πελοποννήσου αποτελούν ιδιοκτησία του.
5. Οι χρήστες οφείλουν να σέβονται τους ελέγχους πρόσβασης (access controls).
6. Οι χρήστες υποχρεούνται να συμμορφώνονται με την νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας.
7. Απαγορεύεται η χρήση λογισμικού που έχει αποκτηθεί με μη νόμιμο τρόπο.
8. Οι εργαζόμενοι στο ΤΕΙ Πελοποννήσου απαγορεύεται να αποκαλύπτουν πληροφορίες σχετικές με τα προσωπικά στοιχεία χρηστών.

Β. Παρακολούθηση και έλεγχος εφαρμογής της πολιτικής

1. Τα δεδομένα που δημιουργούνται με τη χρήση του πληροφοριακού συστήματος του τιμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου αποτελούν ιδιοκτησία του ΤΕΙ.

2. Η χρήση του πληροφοριακού συστήματος του τιμήματος Μηχανικών πληροφορικής Τ.Ε μπορεί να καταγράφεται και να παρακολουθείται από εξουσιοδοτημένα άτομα. Οι χρήστες ενημερώνονται εφάπαξ ότι οι ενέργειές τους καταγράφονται.

Το ΤΕΙ Πελοποννήσου για να διαπιστώσει την τήρηση της Πολιτικής Θεμιτών Πρακτικών Χρήσης χρήση του πληροφοριακού συστήματος του τιμήματος Μηχανικών πληροφορικής Τ.Ε και την τήρηση των πολιτικών που συμπεριλαμβάνονται στην Πολιτική Ασφάλειας χρήση του πληροφοριακού συστήματος του τιμήματος Μηχανικών πληροφορικής Τ.Ε διατηρεί το δικαίωμα να διενεργεί προγραμματισμένους ή έκτακτους ελέγχους. Τους ελέγχους πραγματοποιεί ο Υπεύθυνος Ασφάλειας και τα μέλη του προσωπικού οφείλουν να συνεργαστούν με αυτόν.

Γ. Χρήση Ηλεκτρονικού Ταχυδρομείου και Παγκόσμιου Ιστού

1. Απαγορεύεται η χρήση του ηλεκτρονικού ταχυδρομείου για την αποστολή αυτόκλητων μηνυμάτων (unsolicited mail - spam).

2. Οι χρήστες πρέπει να γνωρίζουν ότι μόνο στην περίπτωση εφαρμογής ειδικών τεχνικών κρυπτογράφησης μπορεί να διασφαλιστεί η εμπιστευτικότητα των ηλεκτρονικών μηνυμάτων.

3. Οι χρήστες πρέπει να γνωρίζουν ότι ο παραλήπτης ενός μηνύματος μπορεί να το διατηρήσει για απροσδιόριστο χρόνο, να το προωθήσει σε τρίτους ή ακόμα να αλλοιώσει το περιεχόμενό του και έπειτα να το προωθήσει σε τρίτους.

4. Οι χρήστες πρέπει να γνωρίζουν ότι η πραγματική ταυτότητα του αποστολέα ενός μηνύματος μπορεί να είναι διαφορετική από την αναγραφόμενη στο μήνυμα.

5. Δεν επιτρέπεται στους χρήστες να χρησιμοποιούν τους λογαριασμούς ηλεκτρονικού ταχυδρομείου συναδέλφων τους.

6. Δεν πρέπει να αποστέλλονται εμπιστευτικές πληροφορίες εκτός του ΤΕΙ Πελοποννήσου με το ηλεκτρονικό ταχυδρομείο.

Δ. Επιλογή και Διαχείριση Συνθηματικών

1. Οι χρήστες δεν πρέπει να αποκαλύπτουν τα συνθηματικά τους σε τρίτους, έστω και εάν αυτοί είναι στενά συγγενικά πρόσωπα, ανώτερα διοικητικά στελέχη ή ακόμα και οι διαχειριστές του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου..

2. Απαγορεύεται η αποκάλυψη της μεθόδου με την οποία ο χρήστης έχει επιλέξει το συνθηματικό του.

3. Απαγορεύεται οποιοδήποτε σχόλιο για την ανθεκτικότητα του συνθηματικού και οποιοσδήποτε υπαινιγμός για τη σύνθεσή του.

4. Απαγορεύεται στους χρήστες να γνωστοποιούν το συνθηματικό τους σε συναδέλφους τους, όταν πρόκειται να απουσιάσουν (π.χ. λόγω αδείας ή ασθενείας).

5. Οι χρήστες πρέπει να αλλάζουν το συνθηματικό τους σε κάθε περίπτωση που θεωρούν ότι μπορεί ή έχει ήδη αποκαλυφθεί.

6. Τα συνθηματικά των χρηστών πρέπει να αλλάζουν τουλάχιστον κάθε τρεις μήνες.

7. Τα συνθηματικά δεν πρέπει να καταγράφονται ή να αναφέρονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, επιστολές κλπ. Εξαιρείται η αποστολή νέου συνθηματικού (στη περίπτωση που ο χρήστης έχει ξεχάσει το συνθηματικό του) από το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε το οποίο συνιστά την εκ νέου αλλαγή του συνθηματικού.

8. Απαγορεύεται η χρήση λειτουργιών αυτόματης συμπλήρωσης συνθηματικού, όπως η λειτουργία "remember password", καθώς και η αποθήκευση των συνθηματικών σε υπολογιστές ή συσκευές

9. Απαγορεύεται η χρήση συνθηματικών όπου:

   a) με λιγότερους από τρεις χαρακτήρες,

   b) που περιέχουν μέρος ή ολόκληρο το αναγνωριστικό χρήστη (username),

   c) που είναι δυνατόν να περιλαμβάνονται σε κάποιο λεξικό,

d) είναι κοινές λέξεις, όπως ονόματα κλπ.,

e) είναι πληροφορίες που αφορούν το χρήστη, όπως η ημερομηνία γέννησης κλπ.,

f) επαναλαμβάνουν τον ίδιο χαρακτήρα πολλές φορές ή έχουν ακολουθίες αριθμών ή γραμμάτων,

g) οποιαδήποτε από τα ανωτέρω συλλαβισμένο ανάποδα ή με ένα χαρακτήρα εμπρός ή πίσω,

h) η χρήση μεταχαρακτήρων.

4.5. Πολιτική Προστασίας Προσωπικών Δεδομένων και Επικοινωνιών

Εισαγωγή

Το ΤΕΙ Πελοποννήσου. έχει την υποχρέωση να προστατεύει τα προσωπικά δεδομένα των φοιτητών του, καθώς κάθε άλλου προσώπου για το οποίο επεξεργάζεται πληροφορίες, και να διαφυλάσσει το απόρρητο των επικοινωνιών στο βαθμό που αυτό εξαρτάται από το πληροφοριακό σύστημα του τιμήματος Μηχανικών πληροφορικής Τ.Ε

Σκοπός

Σκοπός της Πολιτικής Προστασίας Προσωπικών Δεδομένων και Επικοινωνιών είναι:

- Η συμμόρφωση του ΤΕΙ Πελοποννήσου με τις νομικές και κανονιστικές υποχρεώσεις προστασίας προσωπικών δεδομένων.
- Η προστασία της ιδιωτικότητας των φοιτητών του ΤΕΙ Πελοποννήσου.

Εμβέλεια

Η πολιτική αφορά τα μέλη του προσωπικού και τους συνεργάτες του ΤΕΙ Πελοποννήσου. που έχουν ή μπορεί να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα, καθώς και όσους μπορεί να έχουν πρόσβαση ή εμπλέκονται με οποιοδήποτε τρόπο στις επικοινωνίες των φοιτητών του.

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τιμήματος Μηχανικών Τ.Ε

Γενικές αρχές

- Συμμόρφωση με νομικές απαιτήσεις για προστασία προσωπικών δεδομένων

  Το ΤΕΙ Πελοποννήσου προβαίνει σε όλες τις ενέργειες που απαιτούνται για τη τήρηση των υποχρεώσεών του που απορρέουν από το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων.

- Υποχρέωση νομικής συμμόρφωσης προσωπικού

  Όλοι όσοι εργάζονται για το ΤΕΙ Πελοποννήσου ή συνεργάζονται με αυτό έχουν την υποχρέωση να συμβάλλουν στην προστασία των προσωπικών δεδομένων.

Οδηγίες και κανόνες ασφάλειας

Α. Προστασία Προσωπικών Δεδομένων

1. Το ΤΕΙ Πελοποννήσου τηρεί το Ν. 2472/97 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και το Ν. 2225/94 περί προστασίας της ελευθερίας ανταπόκρισης και επικοινωνίας.
2. Το ΤΕΙ Πελοποννήσου γνωστοποιεί στην Αρχή Προστασίας Προσωπικών Δεδομένων την τήρηση οποιουδήποτε αρχείου προσωπικών δεδομένων.
3. Το ΤΕΙ Πελοποννήσου επεξεργάζεται προσωπικά δεδομένα φοιτητών του μόνο μετά την ενημέρωσή τους και εφόσον έχει τη συγκατάθεση τους, όπως ο Νόμος ορίζει.
4. Το ΤΕΙ Πελοποννήσου ενημερώνει τους φοιτητές του για την επεξεργασία των προσωπικών τους δεδομένων, όπως ορίζει η σχετική νομοθεσία.
5. Το ΤΕΙ Πελοποννήσου επεξεργάζεται προσωπικά δεδομένα των υπαλλήλων του μόνο για λόγους που συνδέονται με την άσκηση της εργασίας τους.
6. Το ΤΕΙ Πελοποννήσου δεν μεταβιβάζει, ούτε αποκαλύπτει στοιχεία των φοιτητών του σε τρίτους, παρά μόνο κατόπιν δικαστικής ή εισαγγελικής εντολής ή όταν επιβάλλεται από το νόμο. Σε κάθε άλλη περίπτωση απαιτείται η ρητή συγκατάθεση του υποκειμένου.
7. Η επεξεργασία δεδομένων που αφορούν φοιτητές του ΤΕΙ Πελοποννήσου γίνεται μόνο για τους σκοπούς που σχετίζονται με την παροχή υπηρεσιών σε αυτούς.

8. Η συλλογή προσωπικών δεδομένων περιορίζεται μόνο στα δεδομένα που είναι απαραίτητα για την εκπλήρωση συμβατικών και νομικών υποχρεώσεων του ΤΕΙ Πελοποννήσου
9. Η πρόσβαση του προσωπικού ΤΕΙ Πελοποννήσου. στα προσωπικά δεδομένα των φοιτητών του περιορίζεται με βάση την αρχή ανάγκης γνώσης (need-to-know).
10. Οι φοιτητές έχουν το δικαίωμα να ζητήσουν τη διόρθωση προσωπικών τους στοιχείων που είναι αναληθή ή ανακριβή.

Πολιτική Συνεργατών του ΤΕΙ Πελοποννήσου

Η φύση της συνεργασίας των εξωτερικών παραγόντων με το ΤΕΙ Πελοποννήσου υπόκειται στη συμμόρφωση με τους ευρύτερους κανόνες της Πολιτικής Ασφάλειας και κανονισμών, που έχει αναπτύξει το ΤΕΙ Πελοποννήσου για την συνεργασία του με τρίτους.

4.6. Πολιτική Προστασίας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Εισαγωγή

Η Πολιτική Προστασίας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε προδιαγράφει τα μέσα και τις διαδικασίες με τα οποία διασφαλίζεται αυτό. Η Πολιτική αναφέρεται κυρίως στα τεχνικά μέσα και στις διαδικασίες που εφαρμόζουν οι διαχειριστές του.

Με την πολιτική αυτή διασφαλίζεται ότι υφίσταται και λειτουργεί ένα επαρκές σύστημα ασφάλειας, ικανό να επιτύχει τους σχετικούς με την ασφάλεια στόχους, όπως αυτοί περιγράφονται στην Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Σκοπός

Σκοπός της Πολιτικής Προστασίας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

είναι:

- Η προδιαγραφή των απαιτούμενων μέσων και των κατάλληλων ενεργειών για την προστασία του συστήματος από εκούσιες ή ακούσιες απειλές.

Η διασφάλιση επαρκούμενων τεχνικών μέτρων προστασίας για την εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

- Η διασφάλιση ότι το ΤΕΙ Πελοποννήσου . έχει αποκτήσει τα τεχνικά μέσα που απαιτούνται για να ανταποκριθεί στις νομικές, κανονιστικές και συμβατικές υποχρεώσεις του.

Εμβέλεια

Η Πολιτική Προστασίας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε αφορά το σύστημα που υποστηρίζει κάποιες από τις δραστηριότητες ΤΕΙ Πελοποννήσου

Η πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε.

Γενικές αρχές

- Τεχνική επάρκεια μέσων προστασίας

Το ΤΕΙ Πελοποννήσου εγκαθιστά ένα σύνολο μέσων προστασίας και εφαρμόζει διαδικασίες ικανές να διασφαλίσουν, από τεχνική άποψη, την εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

- Προσανατολισμός μέσων προστασίας

Τα μέσα προστασίας έχουν ως στόχο την προστασία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε τόσο από εξωτερικές όσο και από εσωτερικές απειλές.

- Εύρος απειλών

Τα μέσα προστασίας αποσκοπούν στην προστασία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε τόσο από κακόβουλες όσο και από ακούσιες ενέργειες, όπως επίσης και από απειλές που προέρχονται από τεχνικούς και

περιβαλλοντικούς παράγοντες.

Οδηγίες και κανόνες ασφάλειας

Α. Ανάπτυξη ή προμήθεια συστημάτων και εγκατάστασή τους

1. Όλες οι προμήθειες συστημάτων βασίζονται σε προδιαγραφές, οι οποίες λαμβάνουν υπόψη και τα ζητήματα ασφάλειας.

2. Οι προδιαγραφές ασφάλειας ελέγχονται από τον Υπεύθυνο Ασφάλειας (ένας εκ των διαχειριστών) του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε καθώς και από τη διεύθυνση που θα αναλάβει τη διαχείριση των συστημάτων έπειτα από την εγκατάστασή τους.

3. Όλα τα συστήματα, ανεξαρτήτως μεγέθους και πολυπλοκότητας, ενσωματώνουν επαρκείς μηχανισμούς ασφάλειας. Ιδιαίτερη προσοχή αποδίδεται στην αυθεντικοποίηση (authentication) και τον έλεγχο πρόσβασης των χρηστών.

Β. Έλεγχος πρόσβασης

1. Η απονομή δικαιωμάτων πρόσβασης στο πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου . ακολουθεί την αρχή ανάγκης γνώσης (need-to-know).

2. Η πρόσβαση στο πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε ελέγχεται από κατάλληλους μηχανισμούς ελέγχου πρόσβασης.

3. Το ΤΕΙ Πελοποννήσου τηρεί σαφείς διαδικασίες για τη προσθήκη νέων χρηστών, τις μεταβολές στα επίπεδα πρόσβασης των χρηστών κλπ.

4. Οι μηχανισμοί ελέγχου πρόσβασης διασφαλίζουν ότι υπάρχει δυνατότητα ταυτοποίησης του ατόμου που πραγματοποίησε μία ενέργεια. Η αρχή αυτή ισχύει τόσο για τους χρήστες, όσο και για τους διαχειριστές (μηχανικούς, τεχνικούς κλπ.).

5. Οι χρήστες λαμβάνουν οδηγίες για την επιλογή και διαχείριση των συνθηματικών τους.

6. Η αυστηρότητα των μηχανισμών ελέγχου πρόσβασης είναι αντίστοιχη της διαβάθμισης των δεδομένων.

Γ. Αντιμετώπιση Περιστατικών και Διασφάλιση Συνέχειας Λειτουργίας

1. Όλα τα ύποπτα περιστατικά αναφέρονται στον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε και στην συνέχεια διερευνώνται. Για αυτόν το σκοπό αναπτύσσονται διαδικασίες που διευκολύνουν την αναφορά τους.

2. Το προσωπικό ενθαρρύνεται να αναφέρει ύποπτα περιστατικά, έστω και εάν υπάρχουν περιορισμένες πιθανότητες να αφορούν πραγματική απειλή για το πληροφοριακό σύστημα του τμήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου.

3. Το ΤΕΙ Πελοποννήσου. αναπτύσσει και εφαρμόζει σχέδιο συνέχειας λειτουργίας (business continuity plan).

4. Το σχέδιο συνέχειας λειτουργίας βασίζεται στις απαιτήσεις διαθεσιμότητας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε και ακεραιότητας των πληροφοριών.

5. Το σχέδιο συνέχειας λειτουργίας λαμβάνει υπόψη την πιθανότητα καταστροφικών γεγονότων που μπορεί να θέσουν εκτός λειτουργίας ολόκληρες εγκαταστάσεις (π.χ. σεισμός, πυρκαγιά, πλημμύρα κλπ.).

Δ. Χρήση κρυπτογραφικών μεθόδων

1. Χρησιμοποιούνται κρυπτογραφικές μέθοδοι που ακολουθούν διεθνή πρότυπα.
2. Επιλέγονται κρυπτογραφικές μέθοδοι ανάλογα με την εφαρμογή για την οποία χρησιμοποιούνται.
3. Το μήκος του κλειδιού έχει επαρκές μέγεθος και έχει εγκριθεί από τον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
4. Δεν χρησιμοποιούνται κρυπτογραφικές μέθοδοι που δεν έχουν τεθεί σε δημόσιο έλεγχο.

Ε. Ασφάλεια εγκαταστάσεων

5. Χρησιμοποιείται έλεγχος πρόσβασης, προκειμένου να διασφαλίζεται ο επαρκής έλεγχος σε συνδυασμό με την ευκολία πρόσβασης και διακίνησης των εξουσιοδοτημένων προσώπων.

ΣΤ. Προστασία συστήματος

1. Εγκαθίστανται αποτελεσματικοί μηχανισμοί για την προστασία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου από ιομορφικό λογισμικό.

2. Η ανεπιθύμητη ηλεκτρονική αλληλογραφία (spam) περιορίζεται.

3. Ο βασικός εξοπλισμός προστατεύεται, τόσο φυσικά, όσο και λογικά.

4.7. Σύνοψη Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου

Η Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε είναι ένα εκτενές κείμενο, το οποίο, αν και γραμμένο σε απλή γλώσσα, δύσκολα εντυπώνεται στην μνήμη αυτών που θα επιχειρήσουν να το μελετήσουν. Για αυτόν ακριβώς το λόγο κρίνεται σκόπιμο να συνταχτούν περιλήψεις των πολιτικών για κάθε κατηγορία.

Οι παρακάτω περιλήψεις απευθύνονται σε όλο το ανθρώπινο δυναμικό του ΤΕΙ Πελοποννήσου .. Στις παραγράφους που ακολουθούν προτείνονται τρεις περιλήψεις, οι οποίες απευθύνονται στους χρήστες του συστήματος, στα διοικητικά στελέχη και τους διαχειριστές του συστήματος.

4.7.1. Σύνοψη Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου

Το ΤΕΙ Πελοποννήσου αποδίδει υψηλή προτεραιότητα στην ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε που υποστηρίζει κάποιες από τις δραστηριότητές του. Είναι υποχρέωση της διοίκησης του Π.Α να υποστηρίζουν ενεργά την προσπάθεια διασφάλισης του συστήματος αυτού. Η προσοχή αυτής θα πρέπει να επικεντρωθεί στα παρακάτω:

- Όλες οι δραστηριότητες που αφορούν την ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε βασίζονται σε ρητές πολιτικές και διαδικασίες του ΤΕΙ Πελοποννήσου

- Το ΤΕΙ Πελοποννήσου δεσμεύεται για την τήρηση της νομοθεσίας όσον αφορά στην προστασία προσωπικών δεδομένων, το απόρρητο των επικοινωνιών, τα πνευματικά δικαιώματα, το ηλεκτρονικό έγκλημα και γενικά τη νομοθεσία που αφορά τη χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Η Διοίκηση του ΤΕΙ Πελοποννήσου μεριμνά ώστε όλα τα μέλη του προσωπικού να γνωρίζουν τις υποχρεώσεις τους που απορρέουν από τη Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Το ΤΕΙ Πελοποννήσου είναι υπεύθυνο απέναντι στο νόμο για την τήρηση των νομικών και κανονιστικών προβλέψεων που αφορούν την προστασία προσωπικών δεδομένων και τη διασφάλιση του απόρρητου των επικοινωνιών, έστω και εάν η παραβίαση προέλθει από εξωτερικούς συνεργάτες ή αναδόχους εργασιών.

4.7.2. Σύνοψη Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε για τους διαχειριστές του συστήματος

Τι πρέπει να προσέχετε:

Το ΤΕΙ Πελοποννήσου αποδίδει υψηλή προτεραιότητα στην ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε που υποστηρίζει κάποιες από τις δραστηριότητές του. Είναι υποχρέωση όλων των στελεχών που υποστηρίζουν τεχνικά το σύστημα να καταβάλλουν κάθε προσπάθεια για την προστασία του. Ιδιαίτερη προσοχή οφείλεται στα παρακάτω:

- Η εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε είναι υποχρεωτική για όλα τα μέλη του προσωπικού ΤΕΙ Πελοποννήσου, χωρίς εξαιρέσεις.
- Η ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου στηρίζεται τόσο στην πιστή τήρηση των πολιτικών και των διαδικασιών, όσο και στη συνεχή προσοχή και μέριμνα, καθώς και στην κριτική ικανότητα των ανθρώπων που διαχειρίζονται το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Το ΤΕΙ Πελοποννήσου δεσμεύεται για την τήρηση της νομοθεσίας που

αφορά την προστασία των προσωπικών δεδομένων και του απορρήτου των επικοινωνιών. Η συμβολή των διαχειριστών του συστήματος στην προσπάθεια ανταπόκρισης του ΤΕΙ Πελοποννήσου στις υποχρεώσεις του είναι απαραίτητη.

Δεν επιτρέπεται να:

- Παραβιάζετε τη νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας, όπως και να προβαίνετε σε οποιαδήποτε παράνομη ενέργεια χρησιμοποιώντας εξοπλισμό του ΤΕΙ Πελοποννήσου Σε αντίθετη περίπτωση το ΤΕΙ Πελοποννήσου επιφυλάσσεται να επιβάλλει και διοικητικές κυρώσεις, πέρα από τις όποιες ποινικές συνέπειες.
- Αποκαλύπτετε σε τρίτους οποιεσδήποτε πληροφορίες αφορούν τους φοιτητές του ΤΕΙ Πελοποννήσου
- Κάνετε χρήση κοινών λογαριασμών και συνθηματικών.
- Παραβιάζετε ή παρακάμπτετε τους μηχανισμούς ελέγχου πρόσβασης με τρόπο που να καθιστά αδύνατη την ταυτοποίηση των ατόμων που εκτέλεσαν την κάθε ενέργεια.

Πρέπει να:

- Συμβουλεύεστε την Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε σε κάθε απόφασή σας που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα, την ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Αναφέρετε κάθε ύποπτο περιστατικό στον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Σέβεστε τα δικαιώματα των συναδέλφων σας και να μην παρακολουθείτε ή επεμβαίνετε στις δραστηριότητές τους εάν δεν έχετε σχετική εξουσιοδότηση και μόνο εάν είναι απαραίτητο για την εργασία που έχετε αναλάβει.
- Συνεργάζεστε με τον Υπεύθυνο Ασφάλειας Συνεργάζεστε με τον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου παρέχοντάς του τις πληροφορίες

που χρειάζονται και όποιες άλλες διευκολύνσεις του είναι απαραίτητες.

- Ακολουθείτε αυστηρές πρακτικές για την ορθή επιλογή και διαχείριση των συνθηματικών που χρησιμοποιείτε.
- Τηρείτε την αρχή ανάγκης γνώσης (need-to-know) για την πρόσβασή σας σε συστήματα και δεδομένα.
- Εποπτεύετε τους αναδόχους έργων, εξωτερικούς συνεργάτες και παρόχους υπηρεσιών που μπορεί να επηρεάσουν τη λειτουργία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου
- Συμβάλλετε στη βελτίωση των διαδικασιών ασφάλειας υποβάλλοντας προτάσεις βελτίωσης και να μεριμνάτε για τη διάδοση της γνώσης που αποκτούν κατά την άσκηση των καθηκόντων τους.
- Θέτετε σε δοκιμαστική λειτουργία και να ελέγχετε κάθε νέο σύστημα πριν τεθεί σε παραγωγική λειτουργία, καθώς και κάθε παλαιό σύστημα στο οποίο γίνονται σημαντικές αλλαγές.
- Μεριμνάτε ώστε οι εφαρμογές που αναπτύσσουν, ανεξάρτητα του μεγέθους τους, να ενσωματώνουν επαρκείς και αποτελεσματικούς μηχανισμούς ασφάλειας. του ΤΕΙ Πελοποννήσου παρέχοντάς του τις πληροφορίες που χρειάζονται και όποιες άλλες διευκολύνσεις του είναι απαραίτητες.

- Ακολουθείτε αυστηρές πρακτικές για την ορθή επιλογή και διαχείριση των συνθηματικών που χρησιμοποιείτε.
- Τηρείτε την αρχή ανάγκης γνώσης (need-to-know) για την πρόσβασή σας σε συστήματα και δεδομένα.
- Εποπτεύετε τους αναδόχους έργων, εξωτερικούς συνεργάτες και παρόχους υπηρεσιών που μπορεί να επηρεάσουν τη λειτουργία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του ΤΕΙ Πελοποννήσου
- Συμβάλλετε στη βελτίωση των διαδικασιών ασφάλειας υποβάλλοντας προτάσεις βελτίωσης και να μεριμνάτε για τη διάδοση της γνώσης που αποκτούν κατά την άσκηση των καθηκόντων τους.

- Θέτετε σε δοκιμαστική λειτουργία και να ελέγχετε κάθε νέο σύστημα πριν τεθεί σε παραγωγική λειτουργία, καθώς και κάθε παλαιό σύστημα στο οποίο γίνονται σημαντικές αλλαγές.
- Μεριμνάτε ώστε οι εφαρμογές που αναπτύσσουν, ανεξάρτητα του μεγέθους τους, να ενσωματώνουν επαρκείς και αποτελεσματικούς μηχανισμούς ασφάλειας.

4.7.3. Σύνοψη Πολιτικής Ασφάλειας για τους χρήστες του συστήματος

Τι πρέπει να προσέχετε:

Είναι υποχρέωση όλων των εργαζομένων να συμβάλλουν ενεργά στην προσπάθεια αυτή. Ιδιαίτερη προσοχή οφείλεται στα παρακάτω:

- Η εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε είναι υποχρεωτική. Όλα τα μέλη του προσωπικού έχουν την υποχρέωση να μελετήσουν τα κείμενα όπου περιγράφεται.
- Το ΤΕΙ Πελοποννήσου θα πραγματοποιεί ελέγχους τήρησης της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε και διατηρεί το δικαίωμα να επιβάλλει κυρώσεις σε περιπτώσεις παραβίασης.
- Η χρήση του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε μπορεί να εποπτεύεται από ειδικά εξουσιοδοτημένα για αυτόν το σκοπό άτομα.
- Το ΤΕΙ Πελοποννήσου διατηρεί το δικαίωμα πρόσβασης σε όλα τα δεδομένα που δημιουργούνται και αποθηκεύονται στο πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε Οι χρήστες πρέπει να γνωρίζουν ότι η εμπιστευτικότητα των μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails) και των πληροφοριών που διακινούνται μέσω του Διαδικτύου δεν διασφαλίζεται επαρκώς.

Δεν επιτρέπεται να:

- Χρησιμοποιείτε το σύστημα του ΤΕΙ Πελοποννήσου. για παράνομες

δραστηριότητες.

- Αποκαλύπτετε οποιαδήποτε δεδομένα που αφορούν το ΤΕΙ Πελοποννήσου. ή φοιτητές του σε τρίτους.
- Χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο για την αποστολή εμπιστευτικών πληροφοριών.
- Αποκαλύπτετε τα συνθηματικά σας σε τρίτους, έστω και εάν αυτοί είναι συγγενικά πρόσωπα, ανώτερα διοικητικά στελέχη ή ακόμα και διαχειριστές του συστήματος του ΤΕΙ Πελοποννήσου
- Γνωστοποιείτε το συνθηματικό σας σε συναδέλφους όταν πρόκειται να απουσιάσετε (π.χ. λόγω αδείας ή ασθενείας).
- Καταγράφετε τα συνθηματικά σας σε οποιοδήποτε μέσο.
- Χρησιμοποιείτε συνθηματικά:
  - με λιγότερους από 3 χαρακτήρες,
  - που περιέχουν μέρος ή ολόκληρο το αναγνωριστικό χρήστη
  - που είναι δυνατόν να περιλαμβάνονται σε κάποιο λεξικό,
  - που είναι κοινές λέξεις, όπως ονόματα κλπ.,
  - που είναι πληροφορίες που αφορούν το χρήστη, όπως η ημερομηνία γέννησης του κλπ.,
  - που επαναλαμβάνουν τον ίδιο χαρακτήρα πολλές φορές ή έχουν ακολουθίες αριθμών ή γραμμάτων,
- οποιαδήποτε από τα ανωτέρω συλλαβισμένο ανάποδα ή με ένα χαρακτήρα
- εμπρός ή πίσω.
- με μεταχαρακτήρες.
- Χρησιμοποιείτε συνθηματικά για το σύστημα του ΤΕΙ Πελοποννήσου . και για συστήματα ή υπηρεσίες εκτός ΤΕΙ Πελοποννήσου (π.χ. οικιακοί υπολογιστές).

Πρέπει να:

- Αναφέρετε στον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του

τμήματος Μηχανικών πληροφορικής Τ.Ε οποιαδήποτε θεωρείτε ότι περιορίζει την ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

- Συμβουλεύεστε τον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε για κάθε απορία που έχετε σε σχέση με την ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε, την εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε και τους τρόπους που μπορείτε να συμβάλλετε στη βελτίωση της ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Επιλέγετε συνθηματικά που σας είναι εύκολο να θυμόσαστε, αλλά δύσκολο για οποιονδήποτε άλλον να μαντέψει. Αν χρειάζεστε βοήθεια συμβουλευτείτε τον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Σέβεστε τους μηχανισμούς ελέγχου πρόσβασης (access control), ακόμα και αν αυτοί είναι ανεπαρκείς.
- Αλλάζετε το συνθηματικό σας σε κάθε περίπτωση που θεωρείτε ότι μπορεί να έχει αποκαλυφθεί.

Δεν επιτρέπεται να :

- Μεταβιβάζετε στοιχεία των φοιτητών του ΤΕΙ Πελοποννήσου σε τρίτους, παρά μόνο κατόπιν δικαστικής ή εισαγγελικής εντολής ή όταν επιβάλλεται από το νόμο.
- Παρακάμπτετε την Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε να εξουσιοδοτείτε ενέργειες που παραβιάζουν την Πολιτική ή να δείχνετε ανοχή σε τέτοιες ενέργειες.

Πρέπει να:

- Αποδεικνύετε τη σημασία που έχει η ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε εφαρμόζοντας υποδειγματικά την Πολιτική Ασφάλειάς του και τις διαδικασίες ασφάλειας που απορρέουν από αυτήν.

- Συμβουλεύεστε την Πολιτική Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε σε κάθε απόφασή σας που αφορά ή μπορεί να επηρεάσει, άμεσα ή έμμεσα, την ασφάλεια του.
- Παρέχετε τα απαραίτητα μέσα για την αποτελεσματική εφαρμογή της Πολιτικής Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε Έχει πρόσβαση το προσωπικό σε πηγές πληροφόρησης για ζητήματα ασφάλειας, καθώς και σε σχετικό εκπαιδευτικό υλικό, όπως μαθήματα εξ' αποστάσεως, εκπαιδευτικά videos κλπ.
- Μεριμνάτε για την εκπαίδευση και ευαισθητοποίηση σε θέματα ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε του προσωπικού του ΤΕΙ Πελοποννήσου. που σχετίζεται με τη λειτουργία του.
- Επιλέγετε προσωπικό με κατάλληλα τυπικά και ουσιαστικά προσόντα για την πλήρωση θέσεων που είναι σημαντικές για την ασφαλή λειτουργία του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Συνεργάζεστε με τον Υπεύθυνο Ασφάλειας του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε και τους ελεγκτές του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε για ζητήματα που αφορούν την Ασφάλεια του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε
- Ενημερώνεστε για το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων και τη διασφάλιση του απόρρητου των επικοινωνιών.

5. Μέτρα Προστασίας

Σε αυτή την ενότητα θα παραθέσουμε κάποια μέτρα που πρέπει να ληφθούν από τους διαχειριστές του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε για να περιοριστούν οι αδυναμίες του συστήματος.

Β.Δ

Πρόβλημα 1

Η Β.Δ αποτελεί είναι ένα από τα πιο κρίσιμα αγαθά και για αυτό πρέπει οι διαχειριστές να του δώσουν ιδιαίτερη έμφαση. Επίσης πρέπει να τονίσουμε ότι οι Β.Δ αποτελούν συνήθη στόχο των επιτιθέμενων. Έτσι πρέπει να διασφαλιστεί ότι δεν θα υπάρχει αποκάλυψη των στοιχείων της σε περίπτωση που το λάβει κάποιος μη εξουσιοδοτημένος χρήστης.

Αντίμετρο

Οι διαχειριστές μπορούν να αντιμετωπίσουν την κατάσταση αυτή κρυπτογραφώντας την Β.Δ με ισχυρές κρυπτογραφικές μεθόδους.

Πρόβλημα 2

Ακόμα η Β.Δ κρατείται αυτοματοποιημένα αντίγραφο ασφάλειας καθημερινά, αλλά στο ίδιο τερματικό και ενίοτε μεταφέρεται σε διαφορετικό τερματικό και σε διαφορετικό κτίριο από αυτό που στεγάζεται το σύστημα.

Αντίμετρο

Οι διαχειριστές πρέπει να προγραμματίσουν το σύστημα έτσι ώστε να αποστέλλεται καθημερινά και αυτοματοποιημένα backup σε διαφορετικό τερματικό και φυσικά σε άλλο κτίριο του ΤΕΙ Πελοποννήσου

Πληροφοριακό Σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε.

Πρόβλημα 1

Το σημαντικότερο μειονέκτημα του συστήματος είναι ότι σε περίπτωση καταστροφής του συστήματος (πυρκαγιά, σεισμός) δεν θα υπάρχει άμεση διαθεσιμότητα όλου του

συστήματος καθώς δεν υφίσταται κάποιο εφεδρικό τερματικό που να αντικαθιστά το πρωτότυπο σύστημα.

Αντίμετρο

Είναι επιτακτική ανάγκη για την ομαλή λειτουργία του συστήματος να υπάρχει κάποιος εφεδρικός server σε διαφορετικό κτίριο του ΤΕΙ Πελοποννήσου όπου θα είναι πλήρως λειτουργικός σε περίπτωση που καταστραφεί το αρχικό σύστημα.

Πρόβλημα 2

Σε περίπτωση πρόσβασης στο πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε από κάποιο μη εξουσιοδοτημένο χρήστη υπάρχει περίπτωση να τροποποιήσει τα δεδομένα του συστήματος και να το θέσει εκτός λειτουργίας.

Αντίμετρο

Προτείνεται στους διαχειριστές του συστήματος να χρησιμοποιήσουν ειδικό λογισμικό όπου κρυπτογραφεί τον κώδικα (π.χ. php) του συστήματος και παράγει κάποιο εκτελέσιμο όπου είναι δύσκολο να επέμβει κάποιος εξωτερικός παράγοντας. Έτσι διαφυλάσσεται και ο κώδικας αλλά και η λειτουργικότητα του συστήματος.

Επιθέσεις

Πρόβλημα

Υπάρχει η πιθανότητα το σύστημα να δεχτεί κατά την διάρκεια λειτουργίας του κάποιες επιθέσεις από κακόβουλους χρήστες.

Αντίμετρο

Πρέπει να γίνονται συχνοί έλεγχοι από τους διαχειριστές του συστήματος με τα κατάλληλα εργαλεία εύρεσης ευπαθειών ή απειλών (nessus, acunetix κ.α.) για να αντιμετωπιστεί άμεσα οποιαδήποτε απόπειρα κατά του συστήματος.

Κρυπτογράφηση

Πρόβλημα

Όπως αναφέραμε παραπάνω γίνεται χρήση κρυπτογραφικών μεθόδων (π.χ. MD5) που είναι αναξιόπιστες πλέον και δεν παρέχουν καμία προστασία στα δεδομένα που κρυπτογραφούνται.

Αντίμετρο

Προτείνεται η χρήση συνδυασμένων ισχυρών κρυπτογραφικών μεθόδων.

Παροχή ρεύματος

Πρόβλημα

Υπάρχει μεγάλη πιθανότητα να μην υφίσταται παροχή ηλεκτρικού ρεύματος ανά τακτές χρονικές περιόδους. Παρόλο που υπάρχει κάποια προσωρινή λύση (UPS) για την αντιμετώπιση αυτού του φαινομένου κρίνεται ανεπαρκής.

Αντίμετρο

Για να είναι το σύστημα πλήρως λειτουργικό κατά την περίοδο αυτών των διακοπών παροχής ρεύματος προτείνεται η αγορά και η εγκατάσταση γεννήτριας παραγωγής ηλεκτρικού ρεύματος.

Φυσική Πρόσβαση στο χώρο του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε

Πρόβλημα

Στο χώρο όπου στεγάζεται το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε έχουν φυσική πρόσβαση χωρίς έλεγχο τουλάχιστον δέκα άτομα. Έτσι είναι πιθανό να υπάρξει κάποιο πρόβλημα σκοπίμως ή μη, μελλοντικά στο σύστημα.

Αντίμετρο

Μία προτεινόμενη λύση είναι να εγκατασταθεί το τερματικό του συστήματος σε ένα χώρο όπου θα έχουν πρόσβαση μόνο οι διαχειριστές του.

6. Συμπεράσματα

Η μέθοδος OCTAVE-s ήταν κατατοπιστική όσων αφορά την διεξαγωγή όλων των βημάτων διαμόρφωσης ενός σχεδίου ασφάλειας. Βασιζόμενοι σε αυτή καταφέραμε να εντοπίσουμε τις αδυναμίες του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε και των κινδύνων που ελλοχεύουν.

Επειδή το πληροφοριακό σύστημα του τμήματος Μηχανικών πληροφορικής Τ.Ε διαχειρίζεται και προσωπικά δεδομένα, η ασφάλεια αυτών είναι το κύριο μέλημα του ΤΕΙ Πελοποννήσου σε συνάρτηση με την λειτουργικότητα του συστήματος. Το προσωπικό του ΤΕΙ Πελοποννήσου είναι ενημερωμένο σε θέματα διαχείρισης και στρατηγικής της ασφάλειας. Επίσης πρέπει να τονιστεί ότι δεν υπήρχε κάποιος κανόνας ή πολιτική ασφάλειας. Επιπλέον, ο ανθρώπινος παράγοντας είναι ζωτικής σημασίας για την σωστή και αποτελεσματική λειτουργία του συστήματος, που όμως δεν μπορεί να προβλεφθεί. Τα μέτρα που προτείναμε παραπάνω έχουν σαν σκοπό κυρίως τον εκσυγχρονισμό του πληροφοριακού συστήματος του τμήματος Μηχανικών πληροφορικής Τ.Ε την βελτίωση οργάνωσης σε θέματα ασφαλείας, την εκπαίδευση του προσωπικού και την ενημέρωσή του για νέες εξελίξεις στον τομέα απασχόλησή του.

Εν τέλει είναι σημαντικό το προσωπικό που διαχειρίζεται τέτοιου είδους συστήματα να διαθέτει αρκετά ευαισθητοποιημένη κουλτούρα σε θέματα ασφάλειας.

Βιβλιογραφία

1. Πολιτικής Ασφάλειας NewTelS.A,
   http://www.icsd.aegean.gr/lecturers/sak/index_files/SampleSecPol NewTel_SA.pdf

2. OCTAVE, http://www.cert.org/octave/

3. Η Ιστοσελίδα του ΤΕΙ Πελοποννήσου

   Σχολή: Τεχνολογικών εφαρμογών (Εδρα Σπάρτη)

   Τμήμα: Μηχανικών Πληροφορικής Τ.Ε http://www.cs.teikal.gr/

4. Εισαγωγή στα Πληροφοριακά Συστήματα
   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

5. Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων
   http://www.cs.ucy.ac.cy/courses/EPL674/lectures/Politikes-Asfaleias-Pliroforiakwn-Systimatwn.pdf

6. Διπλωματική Εργασία του Πανεπιστήμιου Δυτικής Μακεδονίας του τμήματος Μηχανικών πληροφορικής και τηλεπικοινωνιών με τίτλο: Μελέτη ασφάλειας πληροφοριών και πληροφοριακών συστημάτων.