Ασφάλεια Πληροφοριακών Συστημάτων

Τελική Εργασία Μαθήματος: Ανάλυση Επικινδυνότητας και Σχέδιο Πολιτικής Ασφάλειας

Ακαδημαϊκό Έτος: 2022 – 2023

Ομάδα:

Μπουμπλίνη Αναστασία (Π19117)

aboublini@gmail.com

ANASTASIA BOUBLINI (p19117@unipi.gr)

Μπριστογιάννης Ιωακείμ (Π19048)

ioakeim13@hotmail.gr

IOAKEIM EL-KHATTAB-BRISTOGIANNIS (p19048@unipi.gr)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Πίνακας Περιεχομένων

1. Ανάλυση Επικινδυνότητας

1.1. Αποτίμηση συνεπειών ή επιπτώσεων ασφάλειας

Στους παρακάτω πίνακες φαίνεται η αποτίμηση συνεπειών για κάθε υπηρεσία που περιγράφεται στην παράγραφο 2.1.

Όνομα Υπηρεσίας:	Κλείσιμο Ραντεβού		
	Τύπος Συνέπειας	Βαθμός Συνέπειας	Σύντομη Αιτιολόγηση
Συνέπειες για:			
Μη διαθεσιμότητα (Unavailability)	• Παρεμπόδιση λειτουργιών • Δυσφήμιση	Χαμηλή	Τα υπολογιστικά συστήματα που θα έφεραν την μεγαλύτερη ευθύνη θα ήταν ο Web Server και ο Application Server, διότι βρίσκονται στο κεντρικό κτήριο του πανεπιστημίου, χωρίς να έχουν την κατάλληλη φύλαξη, με αποτέλεσμα να είναι ευάλωτοι σε, φυσικής μορφής, καταστροφές.
Αποκάλυψη Δεδομένων (Disclosure)	• Δυσφήμιση	Χαμηλή	Το υπολογιστικό σύστημα που θα έφερε την μεγαλύτερη ευθύνη θα ήταν ο Database Server και συγκεκριμένα το λογισμικό PostgreSQL, διότι τα δεδομένα των ραντεβού δεν αποθηκεύονται στην βάση με κάποια μορφή κρυπτογράφησης, με αποτέλεσμα να μπορούν να τροποποιηθούν ή να αποκαλυφθούν με μια απλή παραβίαση του συστήματος.
Τροποποίηση Δεδομένων (Modification)	• Δυσφήμιση • Παρεμπόδιση λειτουργιών	Χαμηλή	

Η αποτίμηση συνεπειών και επιπτώσεων ασφαλείας για τις υπηρεσίες **αναζήτησης / εγγραφής φοιτητών** και **επεξεργασίας στοιχείων** γίνεται σε έναν πίνακα, καθώς και οι τρείς υπηρεσίες διαχειρίζονται τα ίδια δεδομένα (προσωπικά δεδομένα χρηστών).

Όνομα Υπηρεσίας:	Αναζήτηση / Εγγραφή Φοιτητών & Επεξεργασία Στοιχείων		
	Τύπος Συνέπειας	Βαθμός Συνέπειας	Σύντομη Αιτιολόγηση
Συνέπειες για:			
Μη διαθεσιμότητα (Unavailability)	• Παρεμπόδιση λειτουργιών • Δυσφήμιση	Χαμηλή	Τα υπολογιστικό σύστημα που θα έφερε την μεγαλύτερη ευθύνη θα ήταν ο Database Server και συγκεκριμένα το λογισμικό PostgreSQL, καθώς ένας κακόβουλος χρήστης μπορεί να έχει πρόσβαση στη βάση δεδομένων με μια απλή παραβίαση του συστήματος και κατ' επέκταση να

			καταστήσει τα δεδομένα μη διαθέσιμα.
Αποκάλυψη Δεδομένων (Disclosure)	• Νομικές Κυρώσεις • Άμεσες Οικονομικές Απώλειες • Δυσφήμιση	Υψηλή	Τα υπολογιστικό σύστημα που θα έφερε την μεγαλύτερη ευθύνη θα ήταν ο Database Server και συγκεκριμένα το λογισμικό PostgreSQL, καθώς τα προσωπικά δεδομένα των φοιτητών δεν αποθηκεύονται στη βάση δεδομένων με κάποια μορφή κρυπτογράφησης, επομένως η αποκάλυψη τους επιφέρει διάφορες συνέπειες, με την πιο σημαντική να είναι η παραβίαση του κανονισμού GDPR.
Τροποποίηση Δεδομένων (Modification)	• Νομικές Κυρώσεις • Δυσφήμιση • Παρεμπόδιση Λειτουργιών	Μέτρια	Τα υπολογιστικό σύστημα που θα έφερε την μεγαλύτερη ευθύνη θα ήταν ο Database Server και συγκεκριμένα το λογισμικό PostgreSQL, καθώς τα προσωπικά δεδομένα των φοιτητών δεν αποθηκεύονται στη βάση δεδομένων με κάποια μορφή κρυπτογράφησης, επομένως η τροποποίησή τους μπορεί να γίνει με μια απλή παραβίαση. Παρόλα αυτά, σε σχέση με την αποκάλυψη των δεδομένων, το κόστος της ζημιάς είναι μικρότερο.

Όνομα Υπηρεσίας:	**Βαθμολόγηση**		
	Τύπος Συνέπειας	**Βαθμός Συνέπειας**	**Σύντομη Αιτιολόγηση**
Συνέπειες για:			
Μη διαθεσιμότητα (Unavailability)	• Παρεμπόδιση λειτουργιών • Δυσφήμιση • Νομικές Κυρώσεις	Μέτρια	Τα υπολογιστικά συστήματα που θα έφεραν μεγαλύτερη ευθύνη θα ήταν ο Application Server και ο Database Server, διότι βρίσκονται στο κεντρικό κτήριο του πανεπιστημίου με αποτέλεσμα να είναι ευάλωτοι σε φυσικές καταστροφές. Επιπλέον οι βαθμολογίες δεν αποθηκεύονται με κάποια μορφή κρυπτογράφησης στην βάση δεδομένων, επομένως με μια απλή παραβίαση του συστήματος τα δεδομένα μπορεί να είναι μη διαθέσιμα.

Αποκάλυψη Δεδομένων (Disclosure)	• Νομικές Κυρώσεις • Άμεσες Οικονομικές Απώλειες • Δυσφήμιση	Μέτρια	Το υπολογιστικό σύστημα που θα έφερε την μεγαλύτερη ευθύνη θα ήταν ο Database Server και συγκεκριμένα το λογισμικό PostgreSQL, διότι τα δεδομένα βαθμολόγησης πτυχιακών δεν αποθηκεύονται στην βάση με κάποια μορφή κρυπτογράφησης, με αποτέλεσμα να μπορούν να τροποποιηθούν ή να αποκαλυφθούν με μια απλή παραβίαση του συστήματος. Ένα απλό παράδειγμα για την συγκεκριμένη περίπτωση είναι ένας δυσαρεστημένος φοιτητής, ο οποίος επιθυμεί να αλλάξει την βαθμολογία του.
Τροποποίηση Δεδομένων (Modification)	• Νομικές Κυρώσεις • Δυσφήμιση • Παρεμπόδιση Λειτουργιών	Υψηλή	

1.2. Αποτίμηση απειλών

Στους παρακάτω πίνακες φαίνεται η αποτίμηση απειλών για κάθε υπολογιστικό σύστημα που περιγράφεται στην παράγραφο 2.1.1.

Όνομα υπολογιστικού συστήματος : Web Server

Απειλή	Αποτίμηση	Αιτιολόγηση
Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access)	2	Ο web server χρησιμοποιεί τεχνική authorization.
Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware)	3	Ο web server επικοινωνεί απευθείας με την βάση δεδομένων.
Παραποίηση ιστοσελίδας (Web Defacement)	1	Ο κώδικας του ΠΣ βρίσκεται στον application server, οπότε για να γίνει παραποίηση της σελίδας πρέπει, πρώτα, να υπάρχει πρόσβαση στον application server.
Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection)	0	-
Άρνηση υπηρεσίας (Denial of Service)	4	Ο web server δεν χρησιμοποιεί κάποια τεχνική αντιμετώπισης απειλών DoS.

Όνομα υπολογιστικού συστήματος : Application Server

Απειλή	Αποτίμηση	Αιτιολόγηση
Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access)	1	Για να αποκτηθεί Μη εξουσιοδοτημένη πρόσβαση στο application server πρέπει να υπάρχει πρόσβαση στο hardware.
Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware)	2	Εφόσον ο επιτιθέμενος αποκτήσει πρόσβαση στο σύστημα δεν υπάρχει τρόπος αντιμετώπισης.
Παραποίηση ιστοσελίδας (Web Defacement)	2	Εφόσον ο επιτιθέμενος αποκτήσει πρόσβαση στο σύστημα δεν υπάρχει τρόπος αντιμετώπισης.
Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection)	2	Εφόσον ο επιτιθέμενος αποκτήσει πρόσβαση στο σύστημα δεν υπάρχει τρόπος αντιμετώπισης.
Άρνηση υπηρεσίας (Denial of Service)	0	-

Όνομα υπολογιστικού συστήματος : Database Server

Απειλή	Αποτίμηση	Αιτιολόγηση
Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access)	1	Για να αποκτηθεί Μη εξουσιοδοτημένη πρόσβαση στον database server πρέπει να υπάρχει πρόσβαση στο hardware.
Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware)	2	Εφόσον ο επιτιθέμενος αποκτήσει πρόσβαση στο σύστημα δεν υπάρχει τρόπος αντιμετώπισης.
Παραποίηση ιστοσελίδας (Web Defacement)	0	-
Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection)	0	-
Άρνηση υπηρεσίας	2	Εφόσον ο επιτιθέμενος αποκτήσει πρόσβαση στο

(Denial of Service)		σύστημα δεν υπάρχει τρόπος αντιμετώπισης.

1.3. Αποτίμηση αδυναμιών

Στους παρακάτω πίνακες φαίνεται η αποτίμηση των βασικότερων αδυναμιών ασφάλειας που υπάρχουν για τις συγκεκριμένες εκδόσεις λογισμικού που περιλαμβάνονται στα, υπο μελέτη, υπολογιστικά συστήματα.

Όνομα υπολογιστικού συστήματος : Web Server		
Αδυναμία	Περιγραφή NIST (από https://www.nist.gov/)	Σοβαρότητα
CVE-2002-0862	*The (1) CertGetCertificateChain, (2) CertVerifyCertificateChainPolicy, and (3) WinVerifyTrust APIs within the CryptoAPI for Microsoft products including Microsoft Windows 98 through XP, Office for Mac, Internet Explorer for Mac, and Outlook Express for Mac, do not properly verify the Basic Constraints of intermediate CA-signed X.509 certificates, which allows remote attackers to spoof the certificates of trusted sites via a man-in-the-middle attack for SSL sessions, as originally reported for Internet Explorer and IIS.*	Severity: HIGH
CVE-2000-0115	*IIS allows local users to cause a denial of service via invalid regular expressions in a Visual Basic script in an ASP page.*	Severity: MEDIUM

Όνομα υπολογιστικού συστήματος : Application Server		
Αδυναμία	Περιγραφή NIST (από https://www.nist.gov/)	Σοβαρότητα
CVE-2021-41609	*SQL injection in the ID parameter of the UploadedImageDisplay.aspx endpoint of SelectSurvey.NET before 5.052.000 allows a remote, unauthenticated attacker to retrieve data from the application's backend database via boolean-based blind and UNION injection.*	Severity: CRITICAL
CVE-2021-44029	*An issue was discovered in Quest KACE Desktop Authority before 11.2. This vulnerability allows attackers to execute remote code through a deserialization exploitation in the RadAsyncUpload function of ASP.NET AJAX. An attacker can leverage this vulnerability when the encryption keys are known (due to the presence of CVE-2017-11317, CVE-2017-11357, or other means). A default setting for the type whitelisting feature in more current versions of ASP.NET AJAX prevents exploitation.*	Severity: CRITICAL
CVE-2021-43877	*ASP.NET Core and Visual Studio Elevation of Privilege Vulnerability*	Severity: HIGH

Όνομα υπολογιστικού συστήματος : Database Server		
Αδυναμία	Περιγραφή NIST (από https://www.nist.gov/)	Σοβαρότητα
CVE-2022-35942	*Improper input validation on the `contains` LoopBack filter may allow for arbitrary SQL injection. When the extended filter property `contains` is permitted to be interpreted by the Postgres connector, it is possible to inject arbitrary SQL which may affect the confidentiality and integrity of data stored on the connected database. A patch was released in version 5.5.1. This affects users who does any of the following: - Connect to the database via the DataSource with `allowExtendedProperties: true` setting OR - Uses the connector's CRUD methods directly OR - Uses the connector's other methods to interpret the LoopBack filter. Users who are unable to upgrade should do the following if applicable: - Remove `allowExtendedProperties: true` DataSource setting - Add `allowExtendedProperties: false` DataSource setting - When passing directly to the connector functions, manually sanitize the user input for the `contains` LoopBack filter beforehand.*	Severity: CRITICAL
CVE-2022-1552	*A flaw was found in PostgreSQL. There is an issue with incomplete efforts to operate safely when a privileged user is maintaining another user's objects. The Autovacuum, REINDEX, CREATE INDEX, REFRESH MATERIALIZED VIEW, CLUSTER, and pg_amcheck commands activated relevant protections too late or not at all during the process. This flaw allows an attacker with permission to create non-temporary objects in at least one schema to execute arbitrary SQL functions under a superuser identity.*	Severity: HIGH
CVE-2022-2625	*A vulnerability was found in PostgreSQL. This attack requires permission to create non-temporary objects in at least one schema, the ability to lure or wait for an administrator to create or update an affected extension in that schema, and the ability to lure or wait for a victim to use the object targeted in CREATE OR REPLACE or CREATE IF NOT EXISTS. Given all three prerequisites, this flaw allows an attacker to run arbitrary code as the victim role, which may be a superuser.*	Severity: HIGH

2. Σχέδιο Πολιτικής Ασφάλειας

2.1. Καταγραφή του υπο μελέτη συστήματος

Η μελέτη περίπτωσης ανάγεται σε ένα ηλεκτρονικό σύστημα διαχείρισης και επίβλεψης πτυχιακών εργασιών του πανεπιστημίου. Η, εν λόγω, διαδικτυακή εφαρμογή κατηγοριοποιεί τους χρήστες ανάλογα με την ιδιότητα τους, δηλαδή για το αν πρόκειται για φοιτητή ή καθηγητή του πανεπιστημίου. Επιπλέον οι υπηρεσίες που παρέχονται, όπως επίσης και οι δυνατότητες των χρηστών μέσα στην εφαρμογή διαφοροποιούνται ανάλογα με την κατηγορία τους.

Το DTM (Dissertation Thesis Management) σύστημα παρέχει τις παρακάτω online υπηρεσίες:

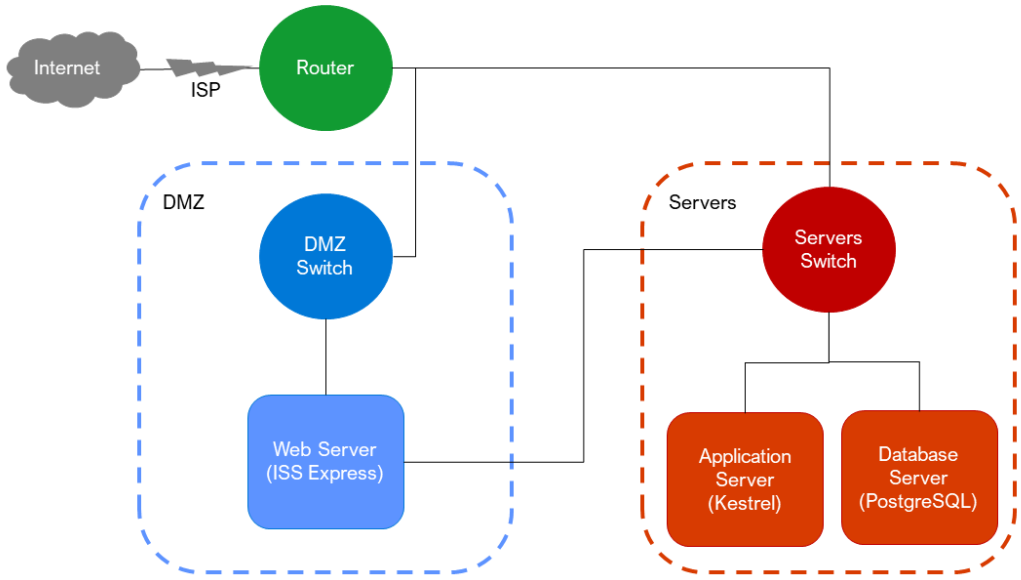
- Κλείσιμο ραντεβού: Παρέχεται η δυνατότητα προγραμματισμού συναντήσεων. Συγκεκριμένα οι καθηγητές μπορούν να προγραμματίζουν επόμενες συναντήσεις με τους φοιτητές που επιβλέπουν, μέσα από την σελίδα του ημερολογίου (επιλογή “Appointments). Οι φοιτητές μπορούν μόνο να δουν τα προγραμματισμένα ραντεβού τους, χωρίς να τους παρέχεται η δυνατότητα επεξεργασίας ή δημιουργίας τους.
- Αναζήτηση φοιτητών: Οι χρήστες με την ιδιότητα καθηγητή μπορούν να αναζητούν, στο σύστημα, τους φοιτητές που επιβλέπουν, μέσα από την σελίδα αναζήτησης (επιλογή “Students”) με βάση τον αριθμό μητρώου ή το ονοματεπώνυμο του φοιτητή.
- Εγγραφή φοιτητών: Οι χρήστες με την ιδιότητα καθηγητή μπορούν να εγγράψουν νέους φοιτητές στο σύστημα μέσω web φόρμας (επιλογή “Students > Add Student”), παρέχοντας τα απαραίτητα στοιχεία του φοιτητή όπως ονοματεπώνυμο, τηλέφωνο, ένα προσωρινό password κ.α. Όταν ένας φοιτητής συνδεθεί για πρώτη φορά στο σύστημα καλείται να αλλάξει τον προσωρινό κωδικό του. Οι καθηγητές μπορούν να προστεθούν στο σύστημα αποκλειστικά και μόνο από τους δημιουργούς της εφαρμογής. Το DTM έχει, αυτή τη στιγμή, περίπου 1000 εγγεγραμμένους χρήστες, οι οποίοι είναι αποθηκευμένοι στη βάση δεδομένων.
- Επεξεργασία στοιχείων: Οι εγγεγραμμένοι χρήστες της εφαρμογής έχουν την δυνατότητα να επεξεργαστούν κάποια προσωπικά στοιχεία τους, όπως ο αριθμός τηλεφώνου και ο κωδικός πρόσβασης στην εφαρμογή, μέσω της σελίδας στοιχείων προφίλ (επιλογή “Profile”). Οι νέες αλλαγές αποθηκεύονται στη βάση δεδομένων.
- Βαθμολόγηση: Οι χρήστες με την ιδιότητα καθηγητή έχουν την δυνατότητα να βαθμολογήσουν τις πτυχιακές εργασίες των φοιτητών που έχει αναλάβει (επιλογή “Profile > Grade a Thesis”). Ο βαθμός αποθηκεύεται στη βάση δεδομένων χωρίς κάποια μορφή κρυπτογράφησης.

Οι τεχνολογίες στις οποίες έχει υλοποιηθεί η παραπάνω υπηρεσία είναι οι ακόλουθες:

- Λειτουργικό Σύστημα: Windows 11
- Εξυπηρετητής Ιστού: Kestrel
- Εξυπηρετητής Εφαρμογής: Kestrel
- Εξυπηρετητής Βάσης Δεδομένων: PostgreSQL 14.2
- Πλαίσιο Υλοποίησης (framework): ASP.NET MVC Server-Side Web Application Framework

- Κλειδί εξυπηρετητή: PKCS #1 RSA Encryption
- Πρωτόκολλο Ασφαλείας: PKCS #1 SHA-256 With RSA Encryption

Η αρχιτεκτονική του δικτύου φαίνεται στο παρακάτω σχήμα:



2.1.1. Δημιουργία μοντέλου αγαθών

Όνομα υπολογιστικού συστήματος : Web Server

HW	Server	AMD RYZEN 5, 16GB
	Τοποθεσία	Κεντρικό κτήριο , Server Room
SW	Λειτουργικό σύστημα	Windows 10
	Λογισμικό Εφαρμογών	Visual Studio
	Άλλο Λογισμικό	
Network	Περιοχή Δικτύου (Network Zone)	http://localhost:26888
	Σημείο σύνδεσης (Gateway)	44339
Data	Δεδομένα διαμόρφωσης (Configuration data)	"windowsAuthentication": false, "anonymousAuthentication": true
	Δεδομένα λειτουργίας υπηρεσιών (Operation data)	
	Άλλα δεδομένα	

Όνομα υπολογιστικού συστήματος : Application Server

HW	Server	AMD RYZEN 5, 16GB
	Τοποθεσία	Κεντρικό κτήριο, Server room
SW	Λειτουργικό σύστημα	Windows 10
	Λογισμικό Εφαρμογών	Visual Studio
	Άλλο Λογισμικό	
Network	Περιοχή Δικτύου (Network Zone)	https://localhost:7120
	Σημείο σύνδεσης (Gateway)	
Data	Δεδομένα διαμόρφωσης (Configuration data)	"Logging": { "LogLevel": { "Default": "Information", "Microsoft.AspNetCore": "Warning" }
	Δεδομένα λειτουργίας υπηρεσιών (Operation data)	
	Άλλα δεδομένα	

Όνομα υπολογιστικού συστήματος : Database Server

HW	Server	AMD RYZEN 5, 16GB
	Τοποθεσία	Κεντρικό κτήριο , Server room
SW	Λειτουργικό σύστημα	Windows 10
	Λογισμικό Εφαρμογών	PostgreSQL
	Άλλο Λογισμικό	PgAdmin
Network	Περιοχή Δικτύου (network zone)	https://localhost: 5432
	Σημείο σύνδεσης (Gateway)	5432
Data	Δεδομένα διαμόρφωσης (Configuration data)	Encoding : UTF8 Connection limit : -1 Template : No
	Δεδομένα λειτουργίας υπηρεσιών (Operation data)	
	Άλλα δεδομένα	

2.1.2. Αντιστοίχιση υπηρεσιών και υπολογιστικών συστημάτων

Η αντιστοίχιση υπηρεσιών και υπολογιστικών συστημάτων φαίνεται στον παρακάτω πίνακα.

Υπολογιστικό Σύστημα	Υπηρεσία	Αιτιολόγηση Αντιστοίχισης
Web Server	Κλείσιμο Ραντεβού	Όλες οι υπηρεσίες αντιστοιχίζονται στον Web Server, διότι σε όλες πρέπει να φορτωθεί στατικό περιεχόμενο.
	Αναζήτηση Φοιτητών	
	Εγγραφή Φοιτητών	
	Επεξεργασία Στοιχείων	
	Βαθμολόγηση	
Application Server	Κλείσιμο Ραντεβού	Όλες οι υπηρεσίες αντιστοιχίζονται στον Application Server, διότι σε όλες πρέπει να φορτωθεί δυναμικό περιεχόμενο, με το οποίο αλληλεπιδρά ο χρήστης.
	Αναζήτηση Φοιτητών	
	Εγγραφή Φοιτητών	
	Επεξεργασία Στοιχείων	
	Βαθμολόγηση	
Database Server	Κλείσιμο Ραντεβού	Όλες οι υπηρεσίες αντιστοιχίζονται στον Application Server, διότι για τις λειτουργίες που παρέχονται από τις υπηρεσίες εκτελούνται διάφορα queries στην βάση δεδομένων.
	Αναζήτηση Φοιτητών	
	Εγγραφή Φοιτητών	
	Επεξεργασία Στοιχείων	
	Βαθμολόγηση	

2.2. Μέτρα Ασφάλειας

Τα μέτρα που ακολουθούνται από το Πανεπιστήμιο Πειραιώς εντάσσονται στις παρακάτω κατηγορίες.

2.2.1. Οργανωτικά Μέτρα Ασφάλειας

- Υπεύθυνος Ασφάλειας
  - **Ορισμός υπεύθυνου ασφάλειας:** Προβλέπεται ο ορισμός διακριτής θέσης υπεύθυνου ασφαλείας, εντός του πανεπιστημίου, με αρμοδιότητες την ανάπτυξη και τη διαμόρφωση των πολιτικών και διαδικασιών ασφαλείας δεδομένων του πανεπιστημίου, την επανεξέταση της αποτελεσματικότητας όσων έχουν ήδη υλοποιηθεί και τη βελτίωση της γενικής συνείδησης της ασφάλειας.
- Οργάνωση και Διαχείριση Προσωπικού
  - **Ορισμός ρόλων προσωπικού:** Το προσωπικό του πανεπιστημίου έχει δικαίωμα πρόσβασης μόνο στα απολύτως απαραίτητα δεδομένα προσωπικού χαρακτήρα, βάσει των αρμοδιοτήτων και καθηκόντων που τους έχουν ανατεθεί.
  - **Δέσμευση προσωπικού ως προς την εμπιστευτικότητα:** Το προσωπικό του πανεπιστημίου πρέπει να ενημερώνεται και να δεσμεύεται για τις υποχρεώσεις του σε σχέση με την τήρηση των όρων εμπιστευτικότητας και εχεμύθειας, όταν αλλάζουν θέση εργασίας ή και κατά το πέρας της συνεργασίας τους με το Πανεπιστήμιο.
  - **Αποχώρηση μέλους:** Κατά την αποχώρηση μέλους του προσωπικού ακολουθείται διαδικασία προστασίας των πληροφοριών και των προσωπικών δεδομένων με ευθύνη του υπεύθυνου ασφάλειας.

- Οργάνωση και Διαχείριση Δεδομένων
    - **Φυσικά πληροφοριακά αγαθά:** Κάθε οργανωτική μονάδα του πανεπιστημίου, η οποία διαθέτει φυσικό τεχνολογικό εξοπλισμό διαχείρισης δεδομένων, θα πρέπει να καταγράφει τα παρακάτω με τη συνεργασία του υπεύθυνου της μονάδας και του υπεύθυνου ασφαλείας:
        - Υπολογιστικός εξοπλισμός
        - Δικτυακός εξοπλισμός
        - Λειτουργικά συστήματα, ενδιάμεσο λογισμικό, βάσεις δεδομένων
        - Εφαρμογές λογισμικού και πληροφοριακά συστήματα
        - Εγκαταστάσεις (γραφεία, Data Room, κ.λπ..)
        - Φυσικά αρχεία (εκτυπώσεις, πρωτότυπα έγγραφα)
    - **Ασφάλεια καταγεγραμμένων πόρων:** Για κάθε καταγεγραμμένο πόρο του φυσικού πληροφοριακού αγαθού, ο υπεύθυνος ιδιοκτήτης σε συνεργασία με τον υπεύθυνο ασφάλειας καθορίζουν τα μέτρα που κρίνονται απαραίτητα για την προστασία του πόρου.
- Καταστροφή / Παραβίαση Δεδομένων
    - **Πολιτική καταστροφής δεδομένων:** Πριν από την καταστροφή εντύπων ή ηλεκτρονικών αρχείων που περιέχουν προσωπικά δεδομένα θα πρέπει να λαμβάνονται τα κατάλληλα μέτρα ώστε να διασφαλίζεται η πλήρης και μόνιμη διαγραφή των δεδομένων αυτών.
    - **Αναφορά συμβάντων παραβίασης δεδομένων:** Όλα τα μέλη του προσωπικού είναι υποχρεωμένα να αναφέρουν οποιαδήποτε συμβάν και ευπάθεια αναγνωρίσουν ή αναφερθεί σε σχέση με την ασφάλεια πληροφοριών. Η αναφορά θα γίνεται στον υπεύθυνο ασφάλειας για την αξιολόγηση του συμβάντος και την πιθανή ενεργοποίηση των κατάλληλων μέτρων ασφάλειας.
    - **Διαχείριση περιστατικών παραβίασης δεδομένων:** Ο υπεύθυνος ασφάλειας πρέπει να εφαρμόζει τη διαδικασία διαχείρισης περιστατικών ασφάλειας σε περίπτωση που αξιολογηθεί θετικά η αναφορά συμβάντος.
- Έλεγχος Ασφάλειας
    - **Διαδικασία τακτικών ελέγχων ασφάλειας:** Προβλέπεται πως πρέπει να γίνονται τακτικοί έλεγχοι ασφάλειας σε όλους τους πόρους (φυσικούς ή μη) του πανεπιστημίου, τουλάχιστον μια φορά το εξάμηνο. Τα αποτελέσματα των ελέγχων διαβιβάζονται στα αρμόδια διοικητικά όργανα και ο υπεύθυνος ασφάλειας τα αξιοποιεί προβαίνοντας στον προγραμματισμό των αναγκαίων τροποποιήσεων και προσθηκών στα μέτρα ασφάλειας καθώς και στο σχέδιο ασφάλειας.

2.2.2. Τεχνικά Μέτρα Ασφάλειας

- Έλεγχος Πρόσβασης
    - **Λογαριασμοί χρηστών:** Το πληροφοριακό σύστημα πρέπει να διαθέτει διαδικασίες για τη διαχείριση των λογαριασμών των χρηστών, όπως για παράδειγμα τη μεταβολή ιδιοτήτων του χρήστη.
    - **Κωδικοί Πρόσβασης:** Το πληροφοριακό σύστημα πρέπει να διαθέτει κατάλληλα μέτρα δημιουργίας και κανόνες προστασίας των κωδικών πρόσβασης των χρηστών.
    - **Μέθοδοι ελέγχου πρόσβασης:** Το πληροφοριακό σύστημα πρέπει να διαθέτει κατάλληλα μέτρα που να εξασφαλίζουν την εγγυημένα ορθή ταυτοποίηση και αυθεντικοποίηση των

χρηστών, ενώ ταυτοχρόνως πρέπει να γίνεται σε τεχνικό επίπεδο συγκεκριμένη εκχώρηση δικαιωμάτων/εξουσιοδοτήσεων σε κάθε χρήστη.

- Αντίγραφα Ασφαλείας
    - **Δημιουργία και τήρηση αντιγράφων ασφαλείας:** Πρέπει να εφαρμόζεται πολιτική για τη δημιουργία και διαχείριση των αντιγράφων ασφάλειας σε όλους τους κεντρικά κρίσιμα συστήματα.
- Κακόβουλο Λογισμικό
    - **Προστασία από κακόβουλο λογισμικό:** Προβλέπεται πολιτική προστασίας από κακόβουλο λογισμικό για όλα τα συστήματα. Σε κάθε προσωπικό υπολογιστή υποχρεωτικά εγκαθίσταται και λειτουργεί antivirus και firewall, τα οποία πρέπει να διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις. Επιπλέον, στο λειτουργικό σύστημα των υπολογιστών πρέπει να εγκαθίστανται σε τακτά χρονικά διαστήματα οι ενημερώσεις ασφάλειας.
- Δικτυακή Ασφάλεια
    - **Απομακρυσμένη πρόσβαση:** Η απομακρυσμένη πρόσβαση σε κρίσιμα συστήματα και εφαρμογές επιτρέπεται μόνο μέσω ασφαλών καναλιών με ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση (όπως VPN).
- Ασφάλεια Λογισμικού και Εφαρμογών
    - **Σχεδιασμός εφαρμογών:** Ο σχεδιασμός των εφαρμογών και του λογισμικού πρέπει να γίνεται πάντα με βάση τις βασικές αρχές προστασίας προσωπικών δεδομένων και της ιδιωτικότητας τους.
    - **Αναβάθμιση / Συντήρηση λογισμικού:** Το λογισμικό όλων των υπολογιστών του προσωπικού πρέπει να ενημερώνεται συχνά με τις νέες εκδόσεις ασφάλειας μέσω των προβλεπόμενων
      διαδικασιών αναβάθμισης.
- Τροποποιήσεις και Αλλαγές
    - **Δοκιμή αλλαγών:** Οι των αλλαγών διεξάγονται αποκλειστικά σε δοκιμαστικό περιβάλλον και συμπεριλαμβάνουν μεθοδολογία επαλήθευσης της ασφάλειας των εφαρμογών.
    - **Διαχείριση αλλαγών:** Ο υπεύθυνος κάθε πληροφοριακού συστήματος έχει την ευθύνη της διαχείρισης των αλλαγών. Καθήκοντά του είναι:
        - Να καταγράφει όλα τα αιτήματα αλλαγής
        - Να καθορίζει τους ρόλους που έχουν δικαιώματα έγκρισης αλλαγών
        - Να καθορίζει τα κριτήρια αποδοχής μιας αλλαγής
        - Να καθορίζει το χρονοδιάγραμμα υλοποίησης

2.2.3. Μέτρα Φυσικής Ασφάλειας

- Φυσική Προστασία
    - **Φυσική πρόσβαση σε εγκαταστάσεις:** Στους χώρους που βρίσκεται κεντρικός υπολογιστικός και δικτυακός εξοπλισμός πρέπει να εφαρμόζονται κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης, έτσι ώστε να επιτρέπεται η πρόσβαση μόνο σ εξουσιοδοτημένο προσωπικό.
    - **Προστασία φορητών μέσων αποθήκευσης:** Προβλέπεται πως τα φορητά μέσα αποθήκευσης πρέπει να φυλάσσονται σε ασφαλή σημεία όταν δεν χρησιμοποιούνται και

να επιβλέπονται κατά τη διάρκεια της χρήσης τους.
    - **Προστασία έντυπων εγγράφων:** Τα έντυπα έγγραφα που περιέχουν προσωπικά δεδομένα πρέπει να είναι τοποθετημένα σε ασφαλή σημεία, ώστε να μην εκτίθενται σε κοινή θέα και πρέπει να καταγράφεται πάντα η φυσική μεταφορά τους.
- Περιβαλλοντικές Καταστροφές
    - **Προστασία από φυσικές καταστροφές**: Προβλέπεται η λήψη και τήρηση κατάλληλων μέτρων για την προστασία του εξοπλισμού των συστημάτων από ζημιές που μπορούν να προκληθούν από φυσικές καταστροφές ή κακόβουλες ενέργειες.

2.2.4. Μέτρα Ανάκαμψης από Φυσικές Καταστροφές

- Φυσική Ανάκαμψη
    - **Προστασία σε περίπτωση φυσικής καταστροφής:** Για την προστασία των προσωπικών δεδομένων σε περίπτωση κάποιου έκτακτου περιστατικού, όπως φυσικές καταστροφές ή μεγάλης εμβέλειας περιστατικά ασφάλειας απαραίτητη η λειτουργία κατάλληλα διαμορφωμένου κεντρικού υπολογιστικού και δικτυακού εξοπλισμού σε εναλλακτική εγκατάσταση, η οποία θα βρίσκεται σε μεγάλη χιλιομετρική απόσταση από τις κεντρικές εγκαταστάσεις.