Student Grading System Security Plan

1. Introduction

A student grading system defines a major role in the administrative system of any university. But such systems do not often relate expectations, outcomes and performance. As each student desires to achieve a good score for each assignment, exam, project the whole process adds heavy workload for lecturers in order to make their evaluation fair, compressive and accurate. From the university perspective these are necessary to avoid disagreement from students as well as from lecturers. A computerized grading system is a highly desirable addition to the education in particularly when it can provide less effort and a more effective and timelier outcome.

Security Plan is to protect the information and critical resources from vast range of different kind of threats and vulnerabilities in order to ensure the privacy, integrity, confidentially and the availability of the Student Grading system without any harmful interferences from any particular attacks. A suitable security plan can be implemented using suitable set of controls, including policies, processes, procedures, protocols, organizational structures and software and hardware functions. These functions need to be launched, implemented, monitored, controlled, reviewed and improved where necessary to ensure that the specific security and university organizational system objectives are met. This also make sure about the each and every department and individual responsibilities are met and controlled from any harmful sources which arises internally or externally to the organization. IT security measures should intend to protect information assets and preserve the privacy of teachers, lecturers, students, administrative board and other associated levels. Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations. When consistently applied throughout the University, these policies and procedures assure that information technology resources are protected from a range of threats in order to ensure and maximize the confidentiality, integrity and the availability of information.

2. Scope

This security plan applies to all the tech community, lecturers, students and the rest of the administrative level workers who have a direct or indirect interference with the university server and tech systems, specially the grading level evaluation and submitting level authorized parties.

The IT assets regarding to this Student Grading system would include student id and information details, student authentication numbers, student results and gradings, resurrected

answer and corrected result sheets, confirmation letters and the finally submitted data, backup storage medias, university access codes and modifying authentication codes and data sheets.

3. Risk Assessment

A risk assessment is a process where we can determine what require the protection and to understand and document potential risks from security failures that may cause harmful actions towards the information and data which needed to have security regarding the integrity, confidentiality and the availability. The purpose of a risk assessment is to help to make appropriate strategies, security system techniques and control access measures regarding the grading system. It is because regulations, working conditions will change rapidly but mechanisms are needed to identify and deal with the special risk associated with change.

Risk assessment is very much needed in today's world due to vast number of latest vulnerabilities and threats, where the administrates may need to deal with proactively. According to information received regarding the year 2018, Ransomware, Major Data leaks, Malware and malicious mobile apps and computer hijacking are the highly rated threats.

As for a university, student information, access and authentication codes, student results, corrected and resurrected answer sheets, assignment quiz results, GPA gradings and other special remark documents such as medicals and other achievements of each and every student should be highly preserved when managing an online student grading system. Security actions should be taken to protect those assets.

User Authentication and Access Control

Risks	Confidentiality	Integrity	Availability
Student Information, medicals, results & gradings, letters etc. – *human interference data leaks*	Exposure of information that should be only available to the administration or to the student	Modification of data	unavailability
Access & authentication codes – *denial of service*	Exposure to all the parties	Code & data modification	Access denials
Question & Answer sheets – *human interference*	Public exposure which should only be exposed to the lecturers	Swiping answer sheets or modifications	Unavailability of data

Server Security

Risks	Confidentiality	Integrity	Availability
Backup storage media – *human interference or denial of service*	Disclosure to the non-authorized parties	Modification or removal of data	Unavailability of certain data
Access & authentication codes – *server hijacking*	Exposure to all the parties	Code & data modification	Server Access denials

Software Security

Risks	Confidentiality	Integrity	Availability
Information updating & calculation - *3rd party software*	Unnecessary access to the server and data theft	-	Service unavailability

Network Security

Risks	Confidentiality	Integrity	Availability
Computer Virus	Mutating and exposure of data	Modification or removal of data	Network breakdown
Rogue security software	-	-	Access denials or Network breakdown
Data & information - *Phishing Attack*	Blackmailing and exposure of data	Modification or removal of data	-

Other Risks

Risks	Confidentiality	Integrity	Availability
System failure	Exposure of data	-	Unavailability of all the data, information, serer backups
Natural Disaster	-	-	Unavailability of all the data, information, serer backups

Risk Register

Id	Description of Risk	Assessment of **Likelihood**	Assessment of **Consequences**	Assessment of **Resultant Risk**
1	System failure – overheating / loss of power	HIGH	LOW	MEDIUM
2	Malicious human Interference – Distributed Denial of Service	HIGH	HIGH	MEDIUM
3	Natural Disaster – Earthquake / flooding	LOW	HIGH	HIGH
4	Accidental human interference	HIGH	LOW	MEDIUM
5	Usage of rouge security software & 3rd party software	HIGH	MEDIUM	MEDIUM
6	Phishing Attack	MEDIUM	HIGH	MEDIUM
7	Server Hijacking	MEDIUM	HIGH	HIGH
8	Computer Virus, Trojan Horses & Worms	HIGH	MEDIUM	MEDIUM

4. Security Strategies and Actions

To overcome the impact causing by the harmful attacks or threats there should be some strategies and actions which can be used to take part in action when there is a security breach. Having this kind of analysis will help so much during the execution running period of this system and enables the safety in a high manner which emphasis the safety of the system by having control of the confidentiality, integrity and availability of data and information and other key assets.

User Authentication and Access Control

Risks	Strategies and Actions	Category
Student Information, medicals, results & gradings, letters etc. – *human interference data leaks*	Access should be done only at a specific location which has high security for the server system and not allow any other party to access the system and should have a secondary server access for the administrative data and information.	Technical Management Operational
Access & authentication codes – *denial of service*	Double authentication with two-way security factor which asks for the pin code which has sent to the user's mobile phone or his/her email	Operational

Question & Answer sheets – *human interference*	Only allow lecturers to access and provide only a copy when someone requests to retrieve the data and doesn't allow any modification without the senior lecturer authentication	Management

Server Security

Risks	Strategies and Actions	Category
Backup storage media – *human interference or denial of service*	It should be on a separate server which doesn't have any access to anyone except the IT tech & the senior head lecturer combined access. Only a copy of the media should be on the publicly available server.	Technical Operational
Access & authentication codes – *server hijacking*	Access and authentication should be categorized into levels and each and every level should have restrictions when accessing the server and it should have several layers where the attacker has to breach through every wall to gain the access and have control of it.	Management Technical

Software Security

Risks	Strategies and Actions	Category
Information updating & calculation - *3rd party software*	Have integrity and behavioral checkers and use only shrink-wrapped software and changes can only be done by the administrative level access	Technical

Network Security

Risks	Strategies and Actions	Category
Computer Virus	Use antivirus software and only give permission to access the trustworthy channels and the rest of the access parties should go through a certain inbound firewall to access data	Technical
Rogue security software	Only give permission to access the trustworthy channels and the rest of the access parties should go through a certain firewall to access data and only the main server	Technical
Data & information - *Phishing Attack*	Use Two-way factor authentication and a security message which only the user knows and firewall protection	Technical Operational

Other Risks

Risks	Strategies and Actions	Category
System failure	Have an additional power system to upload the server system files into a backup base when the power goes off.	Technical Operational
Natural Disaster	Keep an updated daily backup system at a safe remote location	Technical

Adding security features to computer hardware will be an effective and necessary step to mitigate security threats. For the most of the time IT security has been relying on access control using the password and other authentication systems, software-based antivirus and malware systems. However, those have changed and no longer provide the best safety which it supplied before due to the changes of the user expectations. Hardware based security is the one to boot up first and operates independently. Software protected by hardware-based security is shielded from potential malware and other threats that may have infected the main operating system. The dedicated security hardware also operates without burdening the main host server processor, avoiding server slowdowns or lost availability and productivity.

The goal is to deliver the best security measures which have the minimum attack level and designed to maximize the security and privacy of the end user activity as well as to maximize the back-end server security by invisibly protecting against viruses, breaches, hijackings, phishing and persistent threats.

5. Residual Risks

From Risk mitigation it is not possible to completely wipe out all the attacks, threats & vulnerabilities. It is because by mitigation it works as avoidance, acceptence, transference and limitation of threats. Therefore, it still there will be security breaches which the system limits the cause or accept the cause and those will be somehow very harmful before the administrate realizes it.

Risks	Description	Rating
System failure	To some extent there will be some failures which can't be identified but it can be minimize to our best.	LOW
Phishing Attack	Newly invented adware or login procedures could be entered into the server through the firewall because of the unawareness	HIGH
Denial of Service	Whatever the action we take DOS could be happen due to some circumstances which couldn't be identified on our survey	MEDIUM
Modified Access Codes & false entry	There could be minor server braking due to the misrepresentation and modification of access codes and ability to gain the access to data which are not allowed.	HIGH
Server Hijacking	Access codes & authentication data should be changed once in a while otherwise it would be great chance to hijack the server with the same list of access codes used within in the server	LOW
3rd party Web application adware and spams	There are some applications which is not cost effective to buy but it allows to use freely through the web manager and allows all the functions but it cause some security threats because with the free entry it comes up with several vulnerabilities to the system	MEDIUM

6. Resources

7. Maintenance and Training

Before and after the deployment of the system, a security training should be done specially to who control the security system and who has the high access authorizations as well as to all the university lecturers, workers and the students Keeping the people who need to know informed in the operation of the new system is important to ensure the smooth implementation of your security and safety protocols.

Once or twice a week university IT tech should follow some maintenance follow-up and Every six months they should follow a full maintenance program to catch up with the security measures they currently use and add safety criteria to the newly introduced threats and vulnerabilities and make sure everything functions optimally.