For Assignment 1 you will need to analyze an application scenario and develop a security plan. You must work in a group of 2 - 3 members.

This document includes the instructions and background information:

* Page 2 describes the application scenario, ref. ‘Scenario: Student Grading System Security’.
* Page 3-4 is the template for the Security Plan you need to develop, ref. ‘IT Security Plan Template’. **You must use this template for your submission.**
* Pages 5-6 provide some ideas to guide you in developing your Security Plan, ref. ‘Security Plan Ideas’.

**Submission Instructions**:

Please read the following instructions carefully:

**EACH** student (even though you worked in a group) needs to submit a copy of the report in PebblePad. Please follow the instructions on the Assignment page to submit your report. For us to conduct a peer review, please make sure your submission is ANONYMOUS (i.e., the names of the group members are not mentioned).

**ONE** student per group must also submit the report with the Revision History appended to the end of report on Learning@Griffith. This is for you to receive official marks and feedback. It does not matter which student of the group uploads the submission.

# IT Security Plan Revision History

*Outline the development history of the plan, including the dates, authors, and a summary of changes.*

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
|  |  |  |

**For 7623ICT Students**: You will need to develop an IT Security Plan Review Report after the peer review process in Week 8. This is an individual task and worth 5%. Please submit your Review Report on Learning@Griffith using the *Review Report* submission point. You will receive further instructions in the Week 8 lab instructions.

**Scenario: Student Grading System Security**

Remarkable University is implementing a new student grading system. The system needs to be developed and implemented to ensure that it is both fit for purpose and secure from identified threats.

The student grading system’s core components include:

* a front-end web/application server which is used by students, academics and administrative staff
* a database which holds students’ grades

The system will need to be built and managed to ensure that the servers are deployed securely and remain secured against common automated and simple manual attacks. Dedicated, targeted attacks are difficult to protect against, however simple measure can be taken to protect against most automated attacks. Identified threats against the system include:

* Grade hacking/modification, e.g. students who may wish to modify their own results or view or modify the results of others
* Privacy concerns, e.g.:
  + internal users such as staff or students who may wish to view or modify results; and
  + external users who may wish to gain access to or modify results or other personal information
* Malicious code such as worms
* Automated scanning and exploit tools
* Targeted exploit attempts
* Phishing attempts

The grading system application needs to remain secured, use appropriate access controls, enforce least privilege, and ensure that information flowing to and from the system is protected. The application needs to be developed in a secure manner and be protected against common attacks, and the database needs to be protected against common automated attacks and use appropriate access controls.

All components of the systems, and in particular the application and database, need to have appropriate access controls in place to ensure that only authorized users can access and update the system, and that access is tied to the role of each user. All access to the system should be logged, regardless of whether the access is by a user or administrators, and regardless of which component of the system is being accessed.

**IT Security Plan Template**

# Introduction

*Outline the* ***importance*** *of the plan and its relationship with the organisation’s Security Policy.*

# Scope

*This section should establish the organisational context and relevant IT assets (****organisational risk profile*** *and key* ***IT assets****, as per the case scenario).*

# Risk Assessment

*This provides a summary and analysis of the risk assessment. Identify* ***risks*** *to key assets (threats, threat sources, vulnerabilities), by thinking about the different security areas (User Authentication and Access Control, Server Security, Software Security…) and how breaches in those can affect the confidentiality, integrity, and availability of the key assets. Analyse those risks (likelihood, consequence, resultant risk), and summarise your findings in a* ***Risk Register****.*

The following structure and headings are recommended

List all the security areas and for each area, choose some asset(s) to which the area may be applicable and identify the risks to confidentiality and/or integrity and/or availability of that asset. It is not required that you go through all assets for each area, but each asset should appear under at least one area.

# User Authentication and Access Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Risks** | Confidentiality | Integrity | Availability |
| IT Asset 1 |  |  |  |
| IT Asset 2 |  |  |  |
| … |  |  |  |

# Server Security

…

# Software Security

…

# Network Security

…

# Other Risks

…

Risk Register (or Implementation Plan)

# Security Strategies and Actions

*This section should outline security strategies and recommended* ***controls****, based on estimated cost/benefit analysis. Develop a security* ***Implementation Plan****. Classify the selected treatments as management, operational, and/or technical controls.*

The same structure and headings as Section 3 are recommended

# Residual Risks

*By definition, the residual risks are those that remain after all possible (cost-effective) mitigation or treatment of risks. Estimate, describe, and rate these residual risks to guide the priorities for ongoing monitoring of risks.*

# Resources

*This section should detail the resources (e.g., hardware, software, and human resources) for implementing the recommendations outlined in the earlier section on Strategies and Actions*.

# Maintenance and Training

*Outline the recommended maintenance of the security mechanism and training for the relevant personnel*.

**Security Plan Ideas**

**User Authentication and Access Controls**

Describe mechanisms to be used for IT system user authentication by the organization. Given the outcomes of the risk assessment, you should identify whether these mechanisms would be an appropriate control to improve its security posture.

Also you should describe the categorization of users into groups that may then be used for access control decisions to IT resources. Describe the access control mechanism in detail. This can be described on the level of application or database access control, i.e., restriction of certain aspects of the application (e.g., admin functionality) or of certain piece of data (e.g., sensitive and confidential data).

**Server Security**

Describe the management and security configuration of key servers for the organization. Detail the server’s security requirements, identifying:

* what information it contains, and how sensitive that information is
* what applications it runs, how they manipulate the information stored, and how critical their availability is
* who has access to the system, and what type of access they have
* who has administrative access to the system, and how this is controlled
* what change management procedures are used to manage its configuration

You can also detail its basic operating system and patching process to provide a suitable level of security on this server. You can research ways of hardening the O/S, as well as key applications used, to suit the server’s security requirements.

**Software Security**

Describe whether the organization uses critical software which is exposed to possible external attacks, such as software running on an externally visible web server to handle responses to forms or other dynamic data handling.

**Network Perimeter Security**

Describe the organization’s network perimeter security arrangements, that is, their use of firewalls, intrusion detection/prevention systems etc. You can describe what access policy is being used for network traffic, detailing the network services allowed to or across the network perimeter.

You should then suggest an appropriate firewall settings (e.g., inbound and outbound), with details justifying its selection.

**End User PC Security**

Given the known problems with import of malware onto client PC’s or workstations, you can desribe mechanisms to be used to configure and update such systems in the organization, and identify any anti-virus, anti-spyware, and personal firewall products to be used. Suggest whether you believe the current mechanisms should be improved, stating your reasons.

**Security Policy (Optional)**

You can review the current organizational security policy. Indicate whether there are any areas not covered in the existing policy that you believe ought to be.

**Reference**

[1] Griffith Information Security Policy: [http://policies.griffith.edu.au/pdf/Information Security Policy.pdf](http://policies.griffith.edu.au/pdf/Information%20Security%20Policy.pdf)

[2] Griffith Information Security Policy Schedule: <http://policies.griffith.edu.au/pdf/Information-Security-Policy-Schedule-A-Roles-Standards-Operational-Procedures.pdf>

[3] Information Security Policy Templates: <https://www.sans.org/security-resources/policies/>