Question 3

29 marks

A public university's online portal, which hosts student grades, enrolment details, and personal contact information, is experiencing various cyberattacks and system disruptions.

a) Malicious Threats and Impacts: (10 marks) Explain two distinct malicious data security threats could compromise the university portal. For each threat, describe its specific impact on the confidentiality, integrity, or availability of student data, drawing on the CIA Triad principles.

b) Network Protection Measures: (9 marks) Recommend two specific networking measures (e.g., cloud-based DDoS protection, network segmentation, firewalls) that the university could implement to mitigate the threats identified in part (a). Justify your recommendations by explaining how they address the specific risks posed to the university portal.

c) Data Minimization and Ethical Practices: (10 marks) Discuss the ethical principle of data minimization and how it relates to the university's responsibility to collect and retain only necessary student data. Align your discussion with principles of transparency and informed consent in data handling, referring to how these concepts safeguard individual privacy.

Marking Guide – Question 3

Part A

Marks	Criteria	Evidence of achievement
1	Identifies first threat	Names a malicious threat (e.g. SQL Injection).
1	Defines how threat works	Explains the method, e.g. injecting malicious SQL into queries.
1	Links threat to confidentiality	Explains how attacker could access private student records.
1	Links threat to integrity	Explains how attacker could modify or delete grades or enrolment data.
1	Links threat to availability	Explains how attack may disrupt portal function or deny access.
1	Identifies second threat	Names another distinct threat (e.g. DDoS attack).
1	Defines how second threat works	Explains the method, e.g. overwhelming server with traffic.
1	Links second threat to confidentiality	Notes risk of exposure if error handling leaks information.
1	Links second threat to integrity	Notes risk of corrupted transactions under load.
1	Links second threat to availability	Explains denial of service preventing student access to grades and enrolment.

Sample Response

One threat is SQL Injection, where attackers insert malicious SQL code into input fields to manipulate the database. This compromises confidentiality by exposing sensitive records such as student grades and contact details. It affects integrity by allowing attackers to alter or delete data, for example, changing grades. It impacts availability because a manipulated query can crash the database or make the portal unusable.

A second threat is a Distributed Denial of Service (DDoS) attack, which floods the portal’s servers with massive traffic from multiple sources. This primarily impacts availability, as legitimate users cannot access enrolment or grade services during the attack. It can also risk integrity if transactions fail or are corrupted under heavy load, and indirectly threaten confidentiality if error messages reveal system details.

Part B

Marks	Criteria	Evidence of achievement
1	Identifies first measure	States a networking measure (e.g. firewall, WAF).
1	Explains first measure function	Describes how it blocks or filters malicious traffic.
1	Links to SQL Injection threat	Explains how measure protects data integrity (e.g. WAF blocks malicious queries).
1	Provides justification	Explains why measure is suitable for university portal.
1	Identifies second measure	States a different networking measure (e.g. cloud-based DDoS protection).
1	Explains second measure function	Describes how it absorbs or mitigates excessive traffic.
1	Links to DDoS threat	Explains how measure ensures availability during attack.
1	Provides justification	Explains why measure is appropriate in context of protecting student services.
1	Integrates both measures	Explains how measures together provide layered defence for the portal.

Sample Response

A suitable measure is a Web Application Firewall (WAF). A WAF filters and blocks malicious SQL queries before they reach the database, protecting against SQL Injection. By sanitising input and detecting unusual query patterns, it safeguards the integrity of grades and enrolment data. This is appropriate for a university portal because it directly addresses the most common web-based threats.

A second measure is cloud-based DDoS protection, which reroutes and absorbs excess traffic through distributed servers. This ensures the portal remains available even during large-scale attacks. It is effective for global universities because it scales automatically to handle high traffic peaks, such as enrolment deadlines. Together, WAF and DDoS protection provide layered security by protecting against both injection and traffic-based attacks.

Part C

Marks	Criteria	Evidence of achievement
1	Defines data minimization	States principle is collecting and retaining only necessary data.
1	Explains relevance to universities	Links principle to reducing risk of exposure of unnecessary student data.
1	Links to transparency	States students should know what data is collected and why.
1	Explains transparency in context	Example: privacy notices when collecting enrolment information.
1	Links to informed consent	States students must agree to collection and use of their data.
1	Explains informed consent in context	Example: opt-in consent for secondary data uses such as research.
1	Links to confidentiality	States collecting less data reduces risk of breach impact.
1	Links to integrity	Notes maintaining accurate, minimal records prevents misuse or errors.
1	Links to availability	Notes storing only essential data simplifies secure system management.
1	Ethical justification	Argues minimization, transparency, and consent safeguard privacy and meet obligations.

Sample Response

The principle of data minimization requires collecting and retaining only the student data necessary for university functions, such as enrolment and grading. This reduces risk by limiting the amount of information exposed if a breach occurs.

Aligned with transparency, the university must clearly inform students of what data is collected and why, for example, through a privacy notice at enrolment. Aligned with informed consent, students should agree to the collection and use of their data, and be able to opt-in to any secondary uses such as research participation.

Data minimization also supports the confidentiality principle by reducing the amount of personal information held. It strengthens integrity by focusing on maintaining accurate and essential records only. It improves availability by reducing the complexity of secure data management. Ethically, applying minimization, transparency, and consent demonstrates the university's responsibility to safeguard student privacy and trust.