VU LEARNING HUB

CS507 Assignment 1 Solution

Fall 2026

📢 Join our official WhatsApp Channel for instant VU updates, past papers & assignment solutions!

➡ **https://whatsapp.com/channel/0029VbDOzXMC6ZvZBUbW8k2n**

💬 Questions? Chat with us on WhatsApp for quick help & guidance!

➡ **https://wa.me/923135320064**

🌐 Visit our website for more past papers, notes & assignment solutions!

➡ **https://vulearninghub.xyz**

CS507 — Information Systems

Assignment No. 1 — Fall 2026 | Maximum Marks: 15

1. Two major information-system security risks in the scenario

First, unauthorized access through a compromised account. The system does not ask for a second verification step during remote logins, so when an unauthorized user got hold of a supplier account, he could enter the system easily and change delivery quantities. This damaged the accuracy of the stock data and caused delayed orders and confusion between the warehouse and hospital teams.

Second, excessive access rights and no individual accountability. All employees share one common account for updating stock records, so it is impossible to know who made a particular change. At the same time, supplier accounts are able to view customer contact details which they do not need for their work. This breaks the privacy of customer data and increases the chance that sensitive information is misused.

2. Two recommended access-control / authentication mechanisms

(a) Multi-Factor Authentication (MFA) for all remote logins.

(b) Role-Based Access Control (RBAC) combined with the Principle of Least Privilege and unique user accounts for every employee.

3. How each mechanism reduces the identified risks

Multi-Factor Authentication: Even if an attacker steals a supplier’s password, he still cannot log in remotely without the second factor, such as a one-time code on the user’s phone. This would have stopped the unauthorized user from entering the supplier account and changing delivery quantities.

Role-Based Access Control with Least Privilege: Every user would receive only the permissions needed for his own role. Suppliers would no longer see customer contact details, and warehouse staff would only update the stock records related to their own work. If any one account is misused, the damage stays limited, and every action can be traced back to a single person.

4. One benefit of separate user accounts instead of a shared account

The main benefit is accountability. When every employee has his own account, each change in the system carries that person’s name, so management can quickly find out who updated a record, who made a mistake, or who misused the system, instead of blaming the whole team.