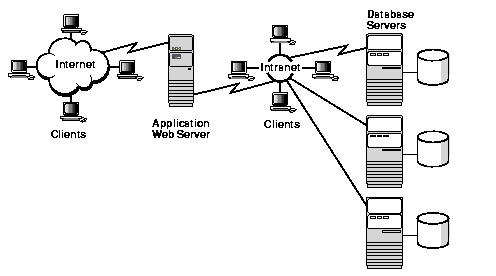
**IS6574 Assignment 2**

You are the leader of a small online business that provides government information to many universities in the USA.

Since you have CUI (Controlled Unclassified Information) in your system that you are responsible for, your company needs to follow the NIST 800-171 guidelines.

Your company has a simple website that the clients (university professors) can login to and download CUI from.

Here is a picture of the small business architecture your company uses:



The Internet Clients are the professors who connect to the Web Server. The IntRAnet Clients are employees of the company who work on computers.

The Application Web Server connects to the IntRAnet and can extract information from the many Database Servers (which contain the CUI).

Download the CUI-SSP-Template document from Canvas for Assignment 2. This document is a real SSP for the NIST 800-171 program.

Use the SSP to answer the following questions. Keep your answers to just a few sentences that focus on answering the question succinctly. This is what an auditor would expect to read.

1. **For control 3.1.1 what might you implement at your company to satisfy the control?**

To satisfy this control, implement strong access control measures such as unique user IDs and passwords for each professor and employee, multi-factor authentication (MFA), and strict role-based access controls (RBAC) to ensure only authorized users can access the system.

1. **For control 3.1.2 what might you implement at your company to satisfy the control?**

Implement role-based access controls (RBAC) that restrict users to only the necessary functions and transactions required for their role. For example, professors should only have access to download CUI, whereas employees should have access to database servers for maintenance and updates.

1. **For control 3.1.4 what might you implement at your company to satisfy the control?**

Establish clear separation of duties by assigning different roles to different individuals and ensuring no single individual has control over all aspects of critical functions. For example, one group manages access permissions while another handles data management.

1. **For control 3.1.5 what might you implement at your company to satisfy the control?**

Ensure all users, including administrators, have the minimum level of access necessary to perform their job functions. Regularly review and update access rights to align with the principle of least privilege.

1. **For control 3.1.9 what might you implement at your company to satisfy the control?**

Display clear privacy and security notices on the login page and throughout the website to inform users about their responsibilities regarding CUI. Ensure these notices comply with CUI handling and dissemination guidelines.

1. **For control 3.2.2 what might you implement at your company to satisfy the control?**

Implement a comprehensive training program for all employees and users that covers security policies, procedures, and best practices for handling CUI. Regularly update the training materials and require periodic retraining sessions.

1. **For control 3.3.3 what might you implement at your company to satisfy the control?**

Use encryption to protect CUI stored on system media, including hard drives and removable media. Implement strict controls over the use of mobile devices, ensuring they comply with security policies and are managed through a mobile device management (MDM) solution.

1. **For control 3.5.3 what might you implement at your company to satisfy the control?**

Implement multi-factor authentication (MFA) for all user accounts accessing the system, both locally and remotely. This should include privileged and non-privileged accounts to add an extra layer of security against unauthorized access.

When you are finished upload this document into Canvas for your submission.