Assignment: Policy for Securing the Windows Environment

Assignment Requirements
Securing Windows applications requires hardening each application to prevent vulnerabilities from being exploited. Your job is to select an appropriate control to address each anticipated vulnerability. You have been given the task of reviewing security policies and recommending appropriate security controls to respond to vulnerabilities identified by the security team in the new ERP software.

You will be provided a list of security controls to detect or prevent each stated threat. For each vulnerability, select the best control to ensure Ken 7 Windows Limited fulfills the stated requirements to secure its application software.

Submission Requirements
- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: APA Style
- Length: 1–2 pages

Self-Assessment Checklist
- I have properly selected the best security control that best satisfies each ERP vulnerability.
- I have provided a proper justification of choosing each security controls.

Required Resources
- Text Sheet: Case Scenario for Rationale: Importance of Windows Access Control and Authentication (see below)
- Worksheet: Security Controls and Vulnerabilities (see below)
Case Scenario for Rationale: Importance of Windows Access Control and Authentication

Ken 7 Windows Limited is a manufacturer of Windows for residential and commercial builders. Ken 7 Windows Limited carries a variety of Windows and related products. It supplies builders with all of the tools and supplies to install finished Windows in any type of building.

Ken 7 Windows Limited has just purchased a new enterprise resource planning (ERP) software package to help control costs and increase both quality and customer responsiveness. The ERP software collects and stores information including:

- Raw material costs
- Labor costs
- Materials and labor requirements for products
- Purchasing requirements

Ken 7 Windows Limited has identified six basic roles for users in the new ERP software:

- Administrators—maintain ERP data and system operation.
- Planners—run planning software and generate requirements reports.
- Shop Floor users—enter operational data (receiving, shipping, and product progress during manufacturing).
- Managers—manage department personnel.
- Purchasing users—generate purchasing documents based on planning requirements.
- Accounting users—maintain cost and accounting data.

Access controls limit what users or roles can do with different types of data. For example, consider the following types of data:

- Cost information—raw materials and labor costs, including the cost of finished goods.
- Manufacturing details—cost, amount of labor, and time required to produce finished goods.
- Purchasing requirements—rules for determining when raw materials, components, or supplies should be purchased.

Through access control:

- Cost information can be viewed only by Accounting users.
- Manufacturing details can be viewed only by Shop Floor users.
- Purchasing requirement can be viewed only by Purchasing users.

During the analysis phase of the ERP implementation, Ken 7 Windows Limited raised concerns about users being able to access restricted data.

- Accounting users are able to login to shop floor computers.
- Purchasing users are able to access human resource (HR) applications and data.

The ERP implementation team suggested the following access control measures to protect restricted data.

- Create an organizational unit (OU) in Active Directory for shop floor computers.
- Deploy Group Policy Objects (GPOs) to restrict shop floor users to the shop floor OU.
- Define data access controls in the ERP software to deny access for all non-HR users to restricted data.

Implementation of several access control measures helped Ken 7 Windows Limited to restrict the data access. Hence access control and authentication is important, as it helped Ken 7 Windows Limited in reducing costs and increasing profits.
Worksheet: Security Controls and Vulnerabilities

You can select from a short list of security controls to detect or prevent each stated threat. For each vulnerability, select the best control to ensure Ken 7 Windows Limited fulfills the stated requirements to secure its application software.

Select from these security controls:
- a. Place a firewall between the Internet and your Web server.
- b. Place a firewall between your Web server and your internal network.
- c. Remove the mail server service.
- d. Require encrypted connections for all remote ERP clients.
- e. Apply the latest security patches.
- f. Use a packet sniffer to view the contents of network packets.
- g. Require all personnel attend a lunch and learn session on updated security policies.

Identified ERP software vulnerabilities:

1. The ERP software vendor reports that some customers have experienced denial-of-service (DoS) attacks from computers sending large volumes of packets to mail servers on the Web server computers.

2. Users that leave their workstations logged in during long durations of inactivity could allow attackers to hijack their session and impersonate them in the application.

3. Attackers with packet sniffers and proxy software could potentially intercept exchanges of private data.

4. Four software vulnerabilities in previous ERP software versions could allow attackers to escalate their permissions and assume administrator privileges.

5. Incorrect Web server configuration may allow unencrypted connections to exchange encrypted information.