Assignment: Network Security Controls

Assignment Requirements
Securing Windows networks requires recognizing potential vulnerabilities and selecting the best control to address that vulnerability. You as a network administrator working for Ken 7 Windows Limited have been given the task of reviewing the current network security policy and recommending the best network security control to satisfy the policy. You can select from a short list of network security controls.

For each policy statement, select the best control to ensure Ken 7 Windows Limited fulfills the stated requirements and provide a rationale.

Required Resources
- Case Scenario for Rationale: Importance of Windows Access Control and Authentication (see below)
- Worksheet: Network Security Requirements Policy (see below)

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

Self-Assessment Checklist
- ✓ I have selected appropriate network security controls for each domain of the Ken 7 IT environment.
- ✓ I have provided rationale for my choices by explaining how each control makes the environment more secure.
- ✓ I have followed the submission requirements.
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: Network Security Requirements Policy

Securing Windows networks requires recognizing potential vulnerabilities and selecting the best control to address that vulnerability. You as a network administrator working for Ken 7 Windows Limited have been given the task of reviewing the current network security policy and recommending the best network security control to satisfy the policy. You can select from a short list of network security controls.

For each policy statement, select the best control to ensure Ken 7 Windows Limited fulfills the stated requirements and also provide a rationale at the end of the table.

Select from these security controls:

- Place a firewall between the Internet and your Web server.
- Place a firewall between your Web server and your internal network.
- Enforce password complexity.
- Implement Kerberos authentication for all internal servers.
- Require encryption for all traffic flowing into and out from the Ken 7 Windows environment.
- Separate wired and wireless network entry points into separate logical networks.
- Require all personnel attend a lunch and learn session on updated network security policies.

Security policy statements:

1. More and more users are using the Ken 7 Windows network to access social media sites during business hours, causing the network to slow down. Users should not use Ken 7 network resources for social media access.

2. Most Ken 7 personnel own mobile phones and PDAs that can connect to the Internet. Ken 7 network administrators are concerned that personal device access may pose a security threat to Ken 7 network resources. Personal devices must not be allowed to connect to the Ken 7 Windows network.

3. Anonymous users of Ken 7 Web application should only be able to access servers located in the demilitarized zone (DMZ). No anonymous Web application users should be able to access any protected resources in the Ken 7 infrastructure.

4. Users who print confidential reports must not be allowed to send reports to unsecured printers.

5. Passwords should not be words found in the dictionary.