ChecklistGuro

ERP Remote Access Security Checklist

User Authentication & Authorization

Verifies the security of user logins and access controls.

Multi-Factor Authentication (MFA) Enabled?

- [ ] Yes
- [ ] No
- [ ] Partial

Password Complexity Requirements Enforced?

- [ ] Yes
- [ ] No
- [ ] Review Needed

Maximum Number of Failed Login Attempts Allowed

Enter a number...

Last Password Policy Review Date

Enter date...

Account Lockout Duration

- [ ] 15 Minutes
- [ ] 30 Minutes
- [ ] 1 Hour
- [ ] Custom

Detailed Explanation of Password Reset Process

Write something...

Device Security & Management

Assesses the security posture of devices accessing the ERP system remotely.

Device Operating System

- [ ] Windows
- [ ] macOS
- [ ] iOS
- [ ] Android
- [ ] Linux

Device Encryption Status (0 = Not Encrypted, 1 = Encrypted)

Enter a number...

Security Software Installed (Select all that apply)

- [ ] Antivirus
- [ ] Firewall
- [ ] Endpoint Detection and Response (EDR)
- [ ] Mobile Device Management (MDM)

Last Security Scan Date

Enter date...

Device Management Status

- [ ] Managed
- [ ] Unmanaged

Device Security Configuration Notes

Write something...

Network Security & Encryption

Evaluates the network connections used for remote access and the encryption protocols in place.

VPN Protocol in Use:

- [ ] IPsec
- [ ] SSL/TLS
- [ ] OpenVPN
- [ ] Other

Encryption Protocol for Data Transmission:

- [ ] TLS 1.2
- [ ] TLS 1.3
- [ ] SSL 3.0 (Not Recommended)
- [ ] Other

Encryption Key Length (bits):

Enter a number...

Network Segmentation Implemented?

- [ ] Yes - ERP isolated
- [ ] Yes - Limited access zones
- [ ] No
- [ ] Partial

Firewall Rules for ERP Access:

- [ ] Strict inbound/outbound rules
- [ ] Moderate rules
- [ ] Limited rules
- [ ] No specific rules

Details of any network monitoring tools or systems used:

Write something...

Data Loss Prevention (DLP)

Confirms measures to prevent sensitive data from leaving the organization through remote access.

DLP Software in Use?

- [ ] Yes
- [ ] No
- [ ] N/A

Data Types Protected by DLP (Select all that apply)

- [ ] PII (Personally Identifiable Information)
- [ ] Financial Data
- [ ] Proprietary Business Information
- [ ] Legal Documents
- [ ] Healthcare Records (PHI)
- [ ] Other

Number of DLP Rules Configured

Enter a number...

Description of DLP Policy Enforcement Methods

Write something...

Are Data Leakage Alerts Monitored?

- [ ] Yes
- [ ] No

Last DLP Policy Review Date

Enter date...

Session Management & Monitoring

Checks controls for managing remote sessions and for monitoring user activity.

Maximum Concurrent Remote Sessions per User

Enter a number...

Session Timeout (Idle)

Enter time...

Session Recording Enabled?

- [ ] Yes
- [ ] No

Session Recording Storage Location & Retention Policy

Write something...

Alerting/Notification System for Suspicious Activity?

- [ ] Yes
- [ ] No

Description of Audit Logging Details

Write something...

Multi-Factor Authentication (MFA)

Ensures MFA is enabled and properly configured for all remote ERP access.

MFA Enrollment Status

- [ ] Fully Enrolled
- [ ] Partially Enrolled
- [ ] Not Enrolled

Primary MFA Method

- [ ] SMS
- [ ] Authenticator App
- [ ] Hardware Token
- [ ] Biometrics

Number of Active MFA Devices Per User (Max)

Enter a number...

Bypass MFA Procedure

- [ ] Defined & Documented
- [ ] Not Defined
- [ ] Ad Hoc

Last MFA Policy Review Date

Enter date...

User Groups Requiring MFA

- [ ] Executive Team
- [ ] Finance Department
- [ ] HR Department
- [ ] All Users

Least Privilege Access

Verifies users have only the minimum necessary access permissions for remote ERP use.

ERP Module Access Review Frequency

- [ ] Monthly
- [ ] Quarterly
- [ ] Annually
- [ ] Ad-hoc

Common ERP Modules Requiring Review

- [ ] Finance/Accounting
- [ ] Human Resources
- [ ] Inventory Management
- [ ] Sales & CRM
- [ ] Manufacturing
- [ ] Procurement

Number of Users with 'Administrator' Access

Enter a number...

Method for Justifying Elevated ERP Access

- [ ] Formal Request Form
- [ ] Manager Approval
- [ ] Periodic Review
- [ ] Automated Workflow

Documentation of Access Justification Rationale

Write something...

Software Updates & Patch Management

Confirms timely updates and security patches are applied to remote access software.

Last Patch Applied (Version Number)

Enter a number...

Date of Last Patch Application

Enter date...

Patch Delivery Method

- [ ] Automated
- [ ] Manual
- [ ] Third-Party Vendor

Notes Regarding Patching Process (e.g., downtime, testing)

Write something...

Patch Testing Environment

- [ ] Separate Test Environment
- [ ] Staging Environment
- [ ] Production Environment (with caution)

Next Scheduled Patch Update Date

Enter date...

Endpoint Security Software

Checks for the presence and proper configuration of antivirus and other endpoint security tools.

Antivirus Software Installed?

- [ ] Yes
- [ ] No
- [ ] Not Applicable

Firewall Enabled?

- [ ] Yes
- [ ] No
- [ ] Not Applicable

Last Antivirus Scan Date (DD/MM/YYYY)

Enter a number...

Endpoint Detection and Response (EDR) Solution?

- [ ] Yes
- [ ] No
- [ ] Not Applicable

Intrusion Prevention System (IPS) Active?

- [ ] Yes
- [ ] No
- [ ] Not Applicable

Description of Endpoint Security Software

Write something...

VPN Security Configuration

Evaluates the security settings of the VPN used for remote access (if applicable).

VPN Tunnel Encryption Strength (bits)

Enter a number...

VPN Protocol in Use

- [ ] IPsec
- [ ] SSL/TLS
- [ ] WireGuard

VPN Server Authentication Method

- [ ] Certificate-Based
- [ ] Pre-shared Key

Last VPN Server Security Audit Date

Enter date...

Description of VPN Segmentation/Access Controls

Write something...

Split Tunneling Enabled?

- [ ] Yes
- [ ] No