ChecklistGuro

# MRP System Security Checklist

## User Access Controls

Ensures appropriate user permissions and role-based access to MRP system data and functionalities.

### Default User Role Assignment Policy

- [ ] Automatic based on department
- [ ] Manual assignment by administrator
- [ ] Hybrid approach

### Sensitive Data Access Restrictions

- [ ] Cost data
- [ ] Supplier contracts
- [ ] Production schedules
- [ ] Inventory levels

### New User Approval Process

- [ ] Immediate
- [ ] Manager Approval
- [ ] Security Team Approval

### Maximum Concurrent User Sessions Allowed

Enter a number...

**Last User Access Review Date**

Enter date...

**Details of User Access Review Process**

Write something...

# Password Management

Verifies password complexity, rotation policies, and secure storage of user credentials.

**Minimum Password Length**

Enter a number...

**Password Complexity Requirements**

- [ ] Uppercase Letters
- [ ] Lowercase Letters
- [ ] Numbers
- [ ] Special Characters

**Password Expiration Time (Days)**

Enter a number...

**Last Password Policy Review Date**

Enter date...

**Password Policy Documentation Link/Location**

Write something...

**Password Reset Method**

- [ ] Self-Service
- [ ] Administrator Assisted

**Number of Password Reuse Prevention**

Enter a number...

# Data Encryption

Confirms encryption of sensitive data at rest and in transit within the MRP system.

**Encryption Method Used:**

- [ ] AES-256
- [ ] RSA
- [ ] Triple DES
- [ ] Other (Specify)

**Specify Other Encryption Method (if applicable):**

Write something...

**Data Encrypted at Rest?**

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

**Data Encrypted in Transit?**

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

**Encryption Key Rotation Period (Days):**

Enter a number...

**Description of Key Management Process:**

Write something...

**Encryption Policy Document (Optional):**

Upload File

# Audit Trails & Logging

Validates comprehensive logging of user actions, system events, and data modifications for auditability.

### Describe Audit Trail Configuration

Write something...

### Maximum Audit Log File Size (MB)

Enter a number...

### Audit Log Storage Location

- [ ] Local Server
- [ ] Cloud Storage
- [ ] Dedicated Logging Server

### Last Audit Log Review Date

Enter date...

### Frequency of Automated Audit Log Summaries

### Key Events Being Logged (e.g., User Login, Data Changes)

Write something...

**Audit Log Retention Policy**

- [ ] 3 Months
- [ ] 6 Months
- [ ] 12 Months
- [ ] Custom

# Network Security

Assesses network access controls, firewalls, and intrusion detection systems protecting the MRP environment.

**Firewall Rule Count**

Enter a number...

**Firewall Vendor**

- [ ] Cisco
- [ ] Fortinet
- [ ] Palo Alto
- [ ] Other

**Network Segmentation Strategy**

Write something...

**VPN Usage**

- [ ] Enabled
- [ ] Disabled

**Last Firewall Rule Review Date**

Enter date...

**Intrusion Detection/Prevention Systems (IDS/IPS)**

- [ ] Enabled
- [ ] Disabled

**Description of Network Access Control (NAC) Implementation**

Write something...

## Backup and Recovery

Confirms regular data backups and a tested recovery plan in case of system failures or security breaches.

**Backup Frequency (Daily/Weekly/Monthly)**

Enter a number...

**Last Successful Full Backup Date**

Enter date...

**Last Successful Incremental Backup Date**

Enter date...

**Backup Storage Location (e.g., cloud, on-site server)**

Write something...

**Backup Retention Period (in days)**

Enter a number...

**Offsite Backup Enabled**

☐ [object Object]

**Disaster Recovery Plan Documentation Location (Link/File)**

Write something...

# System Patching & Updates

Verifies timely application of security patches and system updates to address known vulnerabilities.

**Last Patch Applied Date**

Enter date...

**MRP System Version**

Enter a number...

**Patch Notes/Description (including version number)**

Write something...

**Next Scheduled Patch Review Date**

Enter date...

**Patch Source (e.g., Vendor, Internal)**

- [ ] Vendor
- [ ] Internal IT

**Number of Critical Patches Pending**

Enter a number...

# Integration Security

Evaluates security measures for data integration with other systems, preventing unauthorized access and data leakage.

**Describe Integration Points**

Write something...

**Integration Method (API, File Transfer, Database Link)**

- [ ] API
- [ ] File Transfer (SFTP, FTP)
- [ ] Database Link

**Encryption Strength (e.g., TLS version)**

Enter a number...

**Data Validation Checks Performed**

- [ ] Data Type Validation
- [ ] Format Validation
- [ ] Range Validation
- [ ] Mandatory Field Check

**Last Integration Security Review Date**

Enter date...

# Vendor Access & Management

Controls and monitors vendor access to the MRP system, ensuring compliance with security policies.

**Vendor Access Method**

- [ ] VPN
- [ ] Direct Access (Controlled)
- [ ] Web Portal

**Number of Active Vendor Users**

Enter a number...

**Last Vendor Access Review Date**

Enter date...

**Justification for Vendor Access Level**

Write something...

**Data Access Permissions Granted**

- [ ] Read Only
- [ ] Limited Edit
- [ ] Full Access

**Vendor Access Agreement (Signed)**

Upload File

**Specific Security Protocols Shared with Vendor**

Write something...

# Security Awareness Training

Confirms users receive regular security awareness training to recognize and avoid potential threats.

**Describe phishing recognition techniques taught.**

Write something...

**Which topics were covered in the training?**

- [ ] Password Security
- [ ] Phishing Awareness
- [ ] Data Privacy
- [ ] Malware Prevention
- [ ] Social Engineering
- [ ] Physical Security

**Date of training completion.**

Enter date...

**Score on post-training quiz (if applicable).**

Enter a number...

**Briefly summarize key takeaways from the training.**

Write something...

**Training delivery method (e.g., online, instructor-led).**

- [ ] Online
- [ ] Instructor-led
- [ ] Hybrid