CORPORATE TECHNOLOGIES LLC
gocorptech.com

IT MONITORING FOR MANUFACTURERS CHECKLIST

Executive Tool for Operational Visibility & Uptime

Built for manufacturing leaders and IT decision-makers. Use this checklist to assess your IT monitoring maturity and reduce unplanned downtime.

How to Use

1. Takes 20–30 minutes
2. Check each box that applies
3. Count the total number of checked items
4. Identify monitoring gaps and risk exposure

1

Monitoring Strategy & Coverage

- ☐ Document monitoring goals for systems
- ☐ List critical systems to monitor
- ☐ Define key performance indicators (KPIs) to track
- ☐ Document alert thresholds and response times
- ☐ Assign monitoring ownership internally
- ☐ Include a roadmap for expanding coverage

2

Data Collection & Visibility

- ☐ Enable real-time logging of critical devices
- ☐ Monitor network traffic for anomalies
- ☐ Track server and endpoint performance
- ☐ Track bandwidth usage trends
- ☐ Collect logs from firewalls and routers
- ☐ Ensure logs are stored securely for review

3

Alerts & Notification Setup

- ☐ Configure automated alerts for failures
- ☐ Define alert levels (critical vs warning)
- ☐ Set alert channels (email, SMS, dashboard)
- ☐ Test alert delivery and escalation paths
- ☐ Document alert response procedures
- ☐ Review alert noise and refine thresholds

4

Security & Anomaly Detection

- ☐ Monitor for unauthorized access attempts
- ☐ Track unusual login patterns
- ☐ Detect unexpected changes in device behavior
- ☐ Log potential security events for audit
- ☐ Validate intrusion alerts with manual review
- ☐ Integrate alerts with response procedures

5

Reporting & Analysis

- [ ] Generate uptime reports
- [ ] Review historical trends for recurring issues
- [ ] Document root-cause findings
- [ ] Share reports with leadership monthly
- [ ] Update KPIs based on performance alerts
- [ ] Adjust monitoring settings based on findings

6

Support & Response Readiness

- [ ] Document incident response procedures
- [ ] Assign incident responder roles and contacts
- [ ] Test response processes regularly
- [ ] Define escalation paths for unresolved alerts
- [ ] Record third-party support contacts
- [ ] Review support performance quarterly

Scoring Model

- Count the total number of checked items
- Total Possible Score: 36
- 0–12 → High Risk
- 13–29 → Moderate Risk
- 30–36 → Controlled / Visible & Ready

Immediate Red Flags

- No documented monitoring goals
- No automated alerts configured
- No security anomaly detection in place
- No performance reporting available
- No escalation procedures defined
- Logs not stored for review

Next Step

If your score indicates exposure, schedule an IT Monitoring Readiness Assessment.

IT Monitoring Readiness Assessment