CORPORATE TECHNOLOGIES LLC
gocorptech.com

REMOTE-READY IT ENVIRONMENT CHECKLIST

Executive Tool for Secure & Scalable Remote Work

Built for business leaders planning or evaluating remote IT capabilities. Use this checklist to assess readiness, security, and reliability of remote work systems.

How to Use

1. Takes 20–30 minutes
2. Check each box that applies
3. Count the total number of checked items
4. Identify gaps in remote readiness

1

Infrastructure & Connectivity

- ☐ Ensure reliable broadband for remote users
- ☐ Document VPN or secure access solution
- ☐ Define remote access policy and requirements
- ☐ Confirm internet redundancy where practical
- ☐ List required remote productivity tools
- ☐ Document network segmentation strategy

2

Device & Endpoint Management

- ☐ Inventory employee remote devices
- ☐ Ensure endpoint protection on all devices
- ☐ Enforce device encryption standards
- ☐ Implement standardized configuration templates
- ☐ Track patch and update schedules
- ☐ Record devices missing key security controls

3

Identity & Access Controls

- ☐ Require multi-factor authentication for all users
- ☐ Use a centralized identity provider (SSO)
- ☐ Assign role-based access permissions
- ☐ Audit inactive or orphaned accounts
- ☐ Implement secure password policies
- ☐ Record access control reviews regularly

4

Remote Security Controls

- ☐ Configure the firewall for remote connections
- ☐ Enable encrypted communication channels
- ☐ Monitor for unusual login activity
- ☐ Log security events for review
- ☐ Limit administrative privileges remotely
- ☐ Validate remote security configurations

5

Collaboration & Performance

- ☐ Ensure remote collaboration tools are operational
- ☐ Monitor remote user connectivity health
- ☐ Track remote app performance trends
- ☐ Configure alerts for dropped sessions
- ☐ Review usage logs for bottlenecks
- ☐ Document performance issues and fixes

6

Support & Continuity Planning

- ☐ Establish remote helpdesk procedures
- ☐ Document escalation contacts and hours
- ☐ Test remote support workflows
- ☐ Implement a knowledge base for users
- ☐ Plan an emergency communication strategy
- ☐ Review support satisfaction periodically

Scoring Model

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

Immediate Red Flags

- No secure remote access documented
- MFA not required for remote users
- No endpoint security on remote devices
- No monitoring for remote connectivity health
- No policy for remote access or device use
- No support path for remote issues

Next Step

If your score indicates exposure, schedule a Remote IT Readiness Assessment.

Remote IT Readiness Assessment