CORPORATE TECHNOLOGIES LLC
gocorptech.com

SCHOOL NETWORK TESTING-DAY PROTECTION CHECKLIST

Executive Control Framework to Prevent Testing-Day Outages

Built for school IT leaders responsible for standardized testing reliability. Use this checklist to prevent downtime, security incidents, and testing disruption.

How to Use

1. Takes 20–30 minutes
2. Completed by IT Director, Network Admin, or CIO
3. Check each box that applies.
4. Count the total number of checked items.
5. Identify outage and security exposure

1 Web Filtering & CIPA Compliance

- [ ] Deploy CIPA-compliant web content filter
- [ ] Blacklist high-risk content categories
- [ ] Whitelist approved academic domains
- [ ] Enable automatic filter updates
- [ ] Configure DNS-based cloud filtering
- [ ] Enable alerts for repeated malicious requests

2 Firewall & Network Segmentation

- [ ] Block all unsolicited inbound traffic
- [ ] Restrict outbound traffic by required ports only
- [ ] Segment testing network from admin devices
- [ ] Isolate guest Wi-Fi from internal network
- [ ] Apply access control lists by user role
- [ ] Monitor outbound traffic anomalies

3 Encryption & Secure Traffic

- [ ] Enforce SSL/TLS for all web applications
- [ ] Require encrypted connections for testing platforms
- [ ] Disable legacy insecure protocols
- [ ] Monitor for suspicious packet inspection activity
- [ ] Restrict unauthorized network monitoring tools
- [ ] Validate certificates before testing window

4 Monitoring & Intrusion Prevention

- [ ] Deploy 24/7 network monitoring solution
- [ ] Enable intrusion detection and prevention (IDS/IPS)
- [ ] Configure real-time threat notifications
- [ ] Monitor bandwidth during testing hours
- [ ] Log all security events for audit review
- [ ] Test alert escalation process

5

Testing-Day Readiness Controls

- ☐ Conduct pre-test network stress test
- ☐ Confirm testing platform uptime status
- ☐ Verify bandwidth capacity for peak load
- ☐ Assign live monitoring during testing window
- ☐ Establish incident response contact chain
- ☐ Define acceptable downtime limit

6

Support & Escalation

- ☐ Confirm MSP 24/7 support availability
- ☐ Document emergency escalation contacts
- ☐ Test after-hours response procedures
- ☐ Review cloud monitoring configurations
- ☐ Assign internal testing-day command lead
- ☐ Conduct post-event review after testing

Scoring Model

- Count the total number of checked items
- Total Possible Score: 36
- 0–12 → High Risk
- 13–24 → Moderate Risk
- 25–36 → Controlled / Testing-Day Ready

Immediate Red Flags

- Testing network not segmented
- No live monitoring during testing
- No outbound traffic restrictions
- SSL/TLS not enforced across systems
- No stress test conducted before exams
- No defined escalation contacts

Next Step

If your score indicates exposure, schedule a School Network Readiness Assessment.

School Network Readiness Assessment