The manufacturing disaster recovery checklist.

A step-by-step checklist for building, testing, and documenting a disaster recovery plan that covers production systems, not just office servers. Use it to build a plan from scratch, or hold your existing plan up against it and see what falls out.

01 Know your numbers first

- [ ] **Downtime cost per hour is calculated and written down**, per line or per site.
  Every recovery decision (and budget conversation) hangs on this number.
- [ ] **Every critical system has a defined RTO** (how long you can afford it down): ERP, MES/SCADA, quality systems, shipping, email, phones.
- [ ] **Every critical system has a defined RPO** (how much data you can afford to lose): an hour of ERP transactions is very different from a day.
- [ ] **The list is ranked.** When everything is down, the plan says what comes back first and why.
- [ ] **Dependencies are mapped**: the ERP that needs the database that needs the domain controller that needs DNS. Recovery order follows the map, not guesswork.

02 Backup architecture

- [ ] **The 3-2-1 rule holds**: three copies of critical data, on two different media, one offsite.
- [ ] **At least one backup copy is immutable or offline**, unreachable with the same credentials ransomware would steal.
- [ ] **Backups cover more than servers**: PLC programs, HMI projects, robot programs, equipment configurations, network device configs, license keys.
- [ ] **SaaS data is backed up too.**
  Microsoft 365 and your cloud ERP have retention policies, not backups. Deleted is deleted.
- [ ] **Backup jobs are monitored and failures are chased the same day**, not discovered during a restore.
- [ ] **Backup coverage is reviewed when equipment changes**: new line, new server, new SaaS tool, new backup scope.

03 Documentation (assume the network is down when you need it)

- [ ] **The DR plan exists on paper and offline**, not only on the file server it's meant to recover.
- [ ] **Network diagrams, IP schemes, and credentials are documented** and stored where an incident can't take them out (sealed offline copy or vaulted password manager with break-glass access).
- [ ] **Vendor contacts and contract numbers are listed**: ISP, ERP vendor, machine builders, insurer, IT provider, with support entitlements noted.
- [ ] **Recovery runbooks exist for the top systems**: the actual steps, in order, that a competent person could follow under stress.
- [ ] **Insurance requirements are reflected in the plan.**
  Cyber policies increasingly dictate response steps and notification windows; violating them can void coverage.

04 People and communication

- [ ] **Roles are named, with backups**: who declares the disaster, who leads recovery, who talks to staff, customers, and the insurer.
- [ ] **The call tree works without company systems**: personal phone numbers, printed, current.
- [ ] **Operations leadership has agreed, in advance, on shutdown and restart authority** for production equipment during an IT incident.
- [ ] **Manual operating procedures are documented** for what production, shipping, and receiving do while systems are down: paper travelers, offline scales, manual BOLs.
- [ ] **Customer communication templates are drafted** for the first 4 hours, before anyone knows everything.

05 Testing (a plan that hasn't been tested is a theory)

- [ ] **File and database restores are tested quarterly**, from the actual backup media, timed.
- [ ] **A full recovery of the top-priority system (usually ERP) is tested at least annually**, and the measured time is compared against the RTO you promised yourself.
- [ ] **A PLC or equipment config restore has been tested** at least once: right file, right version, machine runs.
- [ ] **A tabletop exercise runs at least annually** with operations, finance, and leadership in the room, walking a realistic scenario (ransomware on a Sunday night is the classic).

- [ ] **Test results generate fixes.** Every test ends with a written list of what didn't work and who owns each fix by when.
- [ ] **The plan has a review date.**
  Plants change. A DR plan more than a year old describes a facility that no longer exists.

Scoring

All five sections solid

You're ahead of most manufacturers. The remaining risk is drift: calendar the tests and reviews.

Sections 1–2 solid, 3–5 thin

Common and dangerous: good backups nobody can execute under pressure. Documentation and testing turn backups into recovery.

Section 1 unchecked

Start there. Without RTOs, RPOs, and a ranked list, every other investment is unaimed.

The one-question self-test: if ransomware hit at 11 p.m. tonight, does everyone know the first three phone calls, and could you run production tomorrow morning without a single server? If either answer is no, that's your starting point.

Not sure where to start?

Network Builders IT designs and tests recovery plans for manufacturers with production-critical ERP and OT systems. Book a discovery call and we'll walk this checklist against your actual environment, honestly, whether or not we ever work together.

nbit.com/book-a-call
Book a 30-minute discovery call

(888) 816-6248
Talk to an engineer

info@nbit.com
Email us your questions