BROTHERLY
TECHNOLOGY

MANUFACTURING CONTINUITY CHECKLIST

The Manufacturing IT Continuity Checklist

Keeping production systems running, and keeping the office network from becoming the way an attacker reaches the floor.

01	**Separating production systems from the office network**
02	**Continuity planning for line-critical software**
03	**Backup requirements for machine and ERP data**

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology
Owner-led IT, security, and compliance support.

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

[ ] IT, OT, machines, controllers, HMIs, engineering stations, servers, and remote access are inventoried.	[ ] Yes [ ] Partial [ ] No
[ ] Network zones separate office, production, safety, vendor, guest, and management traffic.	[ ] Yes [ ] Partial [ ] No
[ ] Traffic between zones is explicitly allowed, logged, reviewed, and minimized.	[ ] Yes [ ] Partial [ ] No
[ ] Remote vendor access is approved, MFA-protected, time-limited, and monitored.	[ ] Yes [ ] Partial [ ] No
[ ] Unsupported systems have documented compensating controls and replacement plans.	[ ] Yes [ ] Partial [ ] No
[ ] Line-critical applications have owners, dependencies, RTO, RPO, and manual workarounds.	[ ] Yes [ ] Partial [ ] No
[ ] Machine recipes, configurations, programs, keys, and licensing details are backed up.	[ ] Yes [ ] Partial [ ] No
[ ] ERP/MES/database backups are application-consistent, isolated, monitored, and tested.	[ ] Yes [ ] Partial [ ] No
[ ] Critical network and compute components have configuration backups and a spare strategy.	[ ] Yes [ ] Partial [ ] No
[ ] Patch and change processes include vendor compatibility and controlled testing.	[ ] Yes [ ] Partial [ ] No
[ ] Alternate communications and authority are defined for production outages.	[ ] Yes [ ] Partial [ ] No
[ ] Exercises test office compromise, line outage, vendor failure, and recovery priorities.	[ ] Yes [ ] Partial [ ] No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

SEGMENTATION

Keep an office compromise from reaching production

Segmentation is an enforced trust boundary, not simply a different IP range. Document required flows and deny unnecessary paths.

Zone / path	Default position	Required evidence
Office to production	Denied except approved services and jump paths	Flow list, firewall rule, owner, review
Vendor remote access	Off by default; approved, MFA, timed, recorded	Request, session log, disable confirmation
Engineering station	Managed bridge with restricted tools and transfers	Build standard, allowlist, scan process
Production to internet	Minimized to required destinations	Destination list, logging, exception approval
Management interfaces	Dedicated restricted path	Admin identities, MFA, logs, backup
Guest / personal devices	No path to office or production assets	Wireless design and validation test

Validate segmentation from both sides. A diagram is not proof that firewall rules, routes, wireless bridges, and vendor tunnels enforce it.

LINE CONTINUITY

Plan around the software and data the line cannot run without

Recovery must include licenses, drivers, interfaces, recipes, configurations, vendor knowledge, and compatible hardware - not just a server image.

1	Rank production services by safety, quality, throughput, revenue, and restart complexity; approve RTO and RPO.
2	Map power, network, identity, time, database, ERP/MES, machine, vendor, and facility dependencies.
3	Back up machine programs, recipes, PLC/HMI configurations, historian, quality data, ERP/MES, licenses, and network configurations.
4	Maintain tested spares or replacement paths for long-lead components and unsupported hardware.
5	Exercise a representative recovery in a safe test window and validate output with production and quality owners.

What to watch for

WATCH: Office and production are on separate VLANs but routing allows broad access.

WATCH: A vendor tunnel is permanently enabled with a shared account.

WATCH: Machine configuration exists only on the controller.

WATCH: The recovery plan depends on obsolete hardware available from one supplier.

WATCH: IT can restore the server, but production has never validated the line workflow.

MAKE IT ACTIONABLE

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	____________________
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	____________________
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	____________________
NEXT QUARTER	Test the process, document results, and assign improvements.	____________________

Notes / decisions / questions for your provider

____

____

____

____

____

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.

Reference points: CISA Industrial Control Systems: cisa.gov/topics/industrial-control-systems | NIST SP 800-82 Rev. 3: csrc.nist.gov/pubs/sp/800/82/r3/final