



Business Continuity & Disaster Recovery Guide

A practical planning guide for keeping operations moving during outages, data loss, or cyber incidents.

Your IT Department. Your Cybersecurity Team. Your Technology Partner.

Network Solutionist, LLC

Serving Wilmington, Newark, Middletown, Dover, Rehoboth Beach, and businesses across Delaware.



The Goal

Business continuity focuses on keeping essential operations running. Disaster recovery focuses on restoring systems and data. Together, they help a business reduce downtime and recover with confidence.

Planning Checklist

Done	Security Item	Why It Matters
☐	Identify critical systems and applications.	Know which systems must come back first.
☐	Define recovery priorities by department.	Not every system has the same business urgency.
☐	Document recovery time and recovery point expectations.	Leadership should understand downtime and data-loss tolerance.
☐	Maintain protected backups for servers, cloud data, and key workstations.	Critical data may live in more than one place.
☐	Test restores on a regular schedule.	Testing proves recovery is possible before an emergency.
☐	Document emergency vendor contacts.	Support numbers and account IDs should be easy to find.
☐	Create communication templates for staff and clients.	Clear communication reduces confusion during outages.
☐	Inventory hardware, software, licenses, and warranties.	Accurate inventory speeds replacement and recovery.
☐	Review power, internet, and physical access risks.	Outages can be technical, environmental, or facility-related.
☐	Run tabletop exercises with leadership.	Practice exposes gaps before a real incident.

Recovery Strategy Questions

- What must be restored first for the business to function?
- Who can approve emergency spending?
- Where are backup credentials and encryption keys stored?
- How will employees communicate if email is unavailable?
- How will the business operate if the primary office is inaccessible?



Helpful Reference Points

- CISA guidance recommends reviewing and approving an incident response plan and treating security as an everyday activity.
- FTC guidance recommends backing up important files regularly and protecting sensitive data.

Disclaimer

This guide is for general educational purposes and does not replace a formal cybersecurity assessment, compliance review, or incident response engagement.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, monitor, and support your business technology environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com

