1. Vorbereitung und Grundlagen

- ☐ Verantwortliche Person(en) für den Notfallplan sind benannt.
- ☐ Projektstart ist kommuniziert und Management eingebunden.
- ☐ Rechtliche und normative Anforderungen sind identifiziert (z.B. ISO 27001, BSI, ...).

2. Risikoanalyse

- ☐ Kritische Prozesse und Ressourcen sind ermittelt (z.B. IT, Produktion, Logistik).
- ☐ Relevante Risiken sind identifiziert (z.B. Feuer, Cyberangriff, Stromausfall, Pandemien).
- ☐ Risikoauswirkungen sind bewertet (Wahrscheinlichkeit und Schaden).
- ☐ Schutzbedarfe und Prioritäten sind identifiziert.

3. Notfallszenarien und Maßnahmen

- ☐ Sofortmaßnahmen pro Szenario sind beschrieben (technisch, organisatorisch, personell).
- ☐ Wiederanlaufstrategien sind definiert (Recovery-Zeiten: RTO, RPO, Prioritäten).
- ☐ Alternativen für Lieferanten, Personal, IT und/oder Standorte sind dokumentiert.

4. Dokumentation

- ☐ Notfallplan ist schriftlich erstellt und versioniert.
- ☐ Kontaktlisten (intern/extern) sind aktuell gepflegt.
- ☐ Standort- und Technikpläne sind integriert (z.B. Gebäudepläne, IT-Systemübersicht).
- ☐ Checklisten und Ablaufpläne pro Szenario sind enthalten.

5. Kommunikation

- ☐ Alle Stakeholder sind über identifizierte Risiken und geplante Maßnahmen informiert.
- ☐ Kommunikation ist nachweisbar klar und verständlich.
- ☐ Regelmäßige Berichterstattung und Meetings zur Risikoüberwachung sind implementiert.

6. Tests, Schulung & Pflege

- ☐ Schulung des Notfallteams ist durchgeführt.
- ☐ Sensibilisierung der Mitarbeitenden ist erfolgt.
- ☐ Notfallübungen sind regelmäßig geplant und werden durchgeführt.
- ☐ Plan wird mindestens 1x jährlich aktualisiert (auch nach Vorfällen und Umstrukturierungen.

7. Optionale Erweiterungen (je nach Branche)

- ☐ Backup- & Wiederherstellungsstrategie ist dokumentiert (IT).
- ☐ Evakuierungspläne & Brandschutz sind integriert.
- ☐ Zugriffskontrolle & Zutritt im Notfall sind geregelt.
- ☐ Zusammenarbeit mit Behörden oder Dienstleistern ist abgestimmt.