Backup & Disaster Recovery Checklist

Stay one step ahead of potential disasters

- Identify all potential risks
  Include hardware failures, theft, damage, natural disasters and any other contingency that would impact business operations.

- Define goals for contingency plan
  Do you want to maintain full operations or partial? Different adverse events might have different answers.

- Identify mitigation strategies to reduce impact loss
  A secure backup environment with integrated recovery are essential – surge protectors and backup generators are also important to reducing impact and loss.

- Create procedures for power outages or limited office access
  Look to bring systems back online remotely through cloud services and remote locations.

- Appoint a disaster recovery team
  The team should be responsible for planning, testing and managing implementation.

- Procure services, equipment and resources needed for continuity
  This may include Disaster Recovery as a Service (DRaaS), virtual networks, VOIP, surge protectors, etc.

- Train personnel
  Ensure that all parties who are impacted during an adverse event know their role and the correct procedures to follow.

- Implement backup systems and recovery procedures
  Ensure a full backup is made daily (at night is best) and consider creating copies more frequently.

- Conduct testing exercises – disaster recovery
  Testing should happen quarterly and as close to “real-world” as possible without disrupting operations.

Is your company prepared for a disaster?

We can help!

☎️ 800.875.5042
📧 info@milner.com