ARMOUR CYBERSECURITY
Protecting What Matters.

Proactive Readiness

Sample Incident Response Plan

□ **Isolate the System:** Disconnect the infected device from all networks to prevent spread.

□ **Avoid Shutting Down:** Power down only if network disconnection isn't possible; be cautious of data loss.

□ **Document the Ransom Note:** Save screenshots or photos of the ransom message for evidence.

□ **Notify IT & Cyber Response Teams:** Alert your IT and incident response team to begin containment.

□ **Assess Impact:** identify affected systems and prioritize recovery efforts.

□ **Preserve Evidence:** Do not modify or delete files; they are critical for forensic analysis.

□ **Report to Law Enforcement:** Notify authorities to leverage their resources and expertise.

□ **Consult Experts:** Involve cybersecurity specialists or insurance providers for effective recovery.

□ **Communicate Transparently:** Keep stakeholders informed while avoiding unnecessary panic.

□ **Evaluate Ransom Risks:** Carefully weigh the risks of paying, consulting legal counsel first.

We all have a role to play in staying safe!