RANSOMWARE RESPONSE CHECKLIST

INFOTECH

DETECTION & ANALYSIS

- [ ] Immediately isolate impacted systems.
- [ ] Prioritize critical systems for containment.
- [ ] Consider taking the network offline if necessary.
- [ ] Preserve evidence for forensic investigation.

TRIAGE IMPACTED SYSTEMS

- [ ] Identify critical systems for restoration.
- [ ] Prioritize restoration based on predefined critical asset list.
- [ ] Keep track of unaffected systems for efficient recovery.

INITIATE THREAT HUNTING ACTIVITIES

- [ ] Conduct thorough analysis for signs of compromise.
- [ ] Look for evidence of unauthorized access or data exfiltration.
- [ ] Utilize threat intelligence sources for insights.

CONTAINMENT & ERADICATION

- [ ] Take decisive action to contain the spread of ransomware.
- [ ] Implement network segmentation and access controls.
- [ ] Deploy endpoint detection and response solutions.

RECOVERY & POST-INCIDENT ACTIVITY

- [ ] Restore systems from backups prioritizing critical services.
- [ ] Document lessons learned and update security protocols.
- [ ] Engage in post-incident reviews and information sharing.

Tel: 323-638-1870 Email: hello@stginfotech.com Website: www.stginfotech.com