INCIDENT RESPONSE AUTHORIZATION AGREEMENT

Client: _____

Company/Entity: _____

Address: _____

Contact (Name/Phone/Email): _____

Provider (Responder): _____

Contact: _____

Authorization Date: _____

---

1. Purpose

Client authorizes Provider to respond to and remediate cybersecurity incidents on the client's systems, networks, and applications, including but not limited to: malware infections, unauthorized access, ransomware attacks, or other security breaches.

---

2. Scope of Activities

- Investigate and analyze incidents
- Contain and mitigate threats
- Restore affected systems and data where possible
- Communicate findings to client in a timely manner
- Coordinate with third-party vendors if required

All actions will be limited to agreed systems and in accordance with applicable law.

---

3. Emergency Authorization & Safe Harbor

- Provider is authorized to act **immediately** upon discovery or notification of an incident.
- Provider and its agents acting under this agreement will **not be liable** for incidental damage to systems caused **during authorized incident response**, provided actions follow industry-standard practices.

---

4. Confidentiality

All findings, data, and communications will remain confidential and shared only with client personnel or as required by law.

---

5. Reporting

Provider will provide a written report summarizing the incident, actions taken, and recommendations for future mitigation **within ___ hours/days** of containment.

---

6. Acceptance

By signing below, Client confirms authorization for Provider to perform incident response as outlined above.

Client Authorized Signatory

Name: _____ Title: _____ Date: _____

Signature: _____

Provider Authorized Signatory

Name: _____ Title: _____ Date: _____

Signature: _____