**StudioPlus Crisis Management Plan**

*The purpose of this crisis management plan is to guide our response during unexpected emergencies. We hope to provide clarity so decisive action may be taken in the face of a time-sensitive disaster. It outlines roles, communication strategies, and actions to minimize harm and restore normal operations.*

**Crisis Leadership Team**
- **CEO**: Josiah - Overall decision-maker.
- **Lead Developer**: Matt H - Technical response lead.
- **Sales Manager**: Melinda - Handles external messaging.
- **Legal Counsel**: Advises on legal matters.
- **Tech Support Manager**: Matt R - Coordinates technical actions.
- **HR Manager**: Lori - Addresses employee concerns.

**Risk Analysis**

Potential crises:
- **Cybersecurity Breach**: Data breaches, ransomware attacks. Potential Severity: 10/10
- **Software Failure**: Critical system downtime. Potential Severity: 8/10
- **Natural Disasters**: Earthquakes, floods. Potential Severity: 2/10
- **Reputation Crisis**: Negative media coverage. Potential Severity: 7/10
- **Legal Action against the Company**: A disgruntled employee or customer sues company. Potential Severity: 9/10

**Response Procedures**

**Cybersecurity Breach**
1.) **Isolate Affected Systems**:
   a. Lead Developer or Tech Support Manager disconnects compromised servers.
2.) **Notify IT Security Provider**:
   a. Engage external experts.
3.) **Communicate Internally**:
   a. Notify employees about the breach.
4.) **Legal and PR Response**:
   a. Legal counsel advises on legal obligations.
   b. PR team drafts external statements.

**Software Failure**
1.) **Assess Impact**:
   a. Determine affected services.
2.) **Activate Backup Systems**:
   a. Lead Developer or Tech Support Manager switches to backup servers.
3.) **Communicate with Clients**:
   a. Inform clients about the issue and expected resolution time.
4.) **Post-Incident Review**:
   a. Conduct a thorough analysis to prevent recurrence.

**Natural Disasters**
1.) **Employee Safety First**:
   a. Evacuate if necessary.

b. Account for all employees.
2.) **Backup Data and Systems**:
   a. Ensure data backups are secure.
3.) **External Communication**:
   a. Notify clients about potential delays.
4.) **Recovery Plan**:
   a. Restore systems once safe.

**Reputation Crisis**
1.) **Media Monitoring**:
   a. Monitor news and social media.
2.) **Designate Spokesperson**:
   a. Sales Manager or CEO handles external messaging.
3.) **Craft Statements**:
   a. Sales Manager or CEO drafts official statements.
4.) **Address Employee Concerns**:
   a. HR communicates internally.

## Communication Protocols
- **Internal Communication**:
  - Use Teams channels for real-time updates.
  - Regular team briefings during crises.
- **External Communication**:
  - Official statements via website and social media.
  - Media inquiries directed to Sales Manager or CEO.

## Testing and Training
- Verbally Conduct quarterly exercises.
- Train employees on their roles.
- Review and update the plan annually.

## Contact Information
- Emergency Services: 911
- CEO - Josiah: 763-607-3384
- Lead Developer – Matt H: 612-889-6307
- IT Support - Julie: 406-890-5636
- Legal Counsel: