**XXXX - Communication and Escalation Plan**

**Objective**

To establish clear and effective communication channels and escalation procedures in the event of a security incident.

Version: 1.0

Last Updated: October 13, 2023

**Communication Channels**

**Internal Communication:**

Primary Contact: **Telvina Cole, IT Security Manager**

Secondary Contact: **John Doe, System Administrator**

Email:[Telvina.cole@gentel.com](mailto:Telvina.cole@gentel.com)

Phone: (123) 345-7890

**Communication Platform: Internal Messaging System (Slack)**

**External Communication:**

Affected Parties: **Customers, Regulatory Bodies**

Spokesperson: **Michael Redd, CEO**

Contact Information:[michael.red@gentel.com](mailto:michael.red@gentel.com), (301) 444-2525

Communication Platform: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Third-Party Experts:**

Contact Information: **Dr. Chandler Brown Cyberforensics, CyberSolutions Inc**.

Email: [**Chandler.Brown@cybersolutions.com**](mailto:Chandler.Brown@cybersolutions.com)

Phone: **(555) 111-2222**

Expertise: **Forensic Analysis, Attribution**

**Communication Protocol: Secure File Transfer**

Escalation Procedures

Incident Severity Levels:

Level 1: Suspicious Activity

Level 2: Data Breach

Level 3: System Compromise

**Escalation Contacts:**

Level 1 Escalation: **Mark Jones, IT Director,** [**mark.jones@gentel.com**](mailto:mark.jones@gentel.com)

Level 2 Escalation: **Lisa Roberts, Chief Information Officer,** [**lisa.roberts@gentel.com**](mailto:lisa.roberts@gentel.com)

Level 3 Escalation: **Michael Redd, CEO,** [**michael.reed@gentel.com**](mailto:michael.reed@gentel.com)

**Escalation Timeline:**

Level 1 to Level 2 within 1 hour.

Level 2 to Level 3 within 30 minutes.

**Escalation Criteria:**

Level 1 to Level 2: Confirmation of data breach.

Level 2 to Level 3: Evidence of system compromise or legal implications.

**Communication Plan**

**Initial Notification:**

In the event of an incident, the Primary Contact (Emily Anderson) will be notified immediately through the internal messaging system (Slack).

**Internal Communication:**

The Incident Response Team (IRT) and key stakeholders will be notified within 30 minutes of incident detection, including IT staff and legal representatives.

**External Communication:**

If the incident is confirmed as a data breach (Level 2), Michael Redd will initiate external communication through the company website, social media, and press releases.

**Third-Party Expert Engagement:**

In case of Level 2 or Level 3 incidents, contact Dr. Chandler Brown, Cyberforensics for forensic analysis and attribution using the secure file transfer protocol.

**Testing and Training**

Regularly test the communication and escalation plan through tabletop exercises and incident simulations quarterly.

Ensure that all relevant personnel are trained on their roles and responsibilities within this plan during onboarding and annually as part of cybersecurity training.

Periodically review and update the plan to reflect any organizational or cybersecurity changes.