Gotham Ltd. Incident Response Policy

1. Introduction: The purpose of this policy is to provide a structured approach for detecting, responding to, and recovering from incidents that may compromise the confidentiality, integrity, or availability of data or systems within Gotham Ltd. This policy aligns with industry standards such as NIST and ISO 27001, ensuring preparedness, effective response, and continuous improvement.

2. Scope: This policy applies to all employees, contractors, and third parties who have access to Gotham Ltd.'s information systems and data. It covers incidents related to cyberattacks, disasters, system failures, and other security breaches.

3. Definitions:

- **Incident:** Any event that compromises the confidentiality, integrity, or availability of data or systems.
- **Incident Response Team (IRT):** A team responsible for managing and resolving incidents, including members from IT, security, legal, and communications departments.

4. Roles and Responsibilities:

- **IRT:** Coordinates incident response activities, including detection, containment, investigation, communication, and recovery.
- **IT Department:** Provides technical support and expertise during incident response and recovery.
- **Legal Department:** Ensures compliance with legal obligations and internal policies.
- **Communications Department:** Manages external and internal communications related to the incident.

5. Incident Detection:

- Implement monitoring tools and systems to detect unusual activities or potential threats.
- Establish a Security Operations Center (SOC) for real-time monitoring and threat analysis.

6. Incident Response:

- **Containment:** Immediately take steps to contain the incident to prevent further damage, such as isolating affected systems.
- **Investigation:** Conduct a thorough investigation to determine the cause, extent, and potential impact of the incident.
- **Communication:** Notify relevant stakeholders, including employees, customers, and regulators, in accordance with legal and compliance obligations.

7. Recovery:

- Develop and maintain a disaster recovery plan (DRP) and business continuity management (BCM) to ensure quick resumption of operations post-disruption.
- Restore systems from backups, ensuring data integrity and system availability.

8. Post-Incident Review:

- Document the incident details, including cause, impact, response actions, and outcomes.

- Conduct a root cause analysis to identify systemic issues and improve future security measures.
- Update policies, procedures, and training programs based on lessons learned from the incident.

9. Continuous Improvement:

- Regularly review and update the incident response policy to adapt to new threats and technologies.
- Conduct simulations and drills to test the effectiveness of the incident response plan and ensure preparedness for real-life scenarios.

10. Training and Awareness:

- Provide regular training sessions for employees on incident response procedures, threat recognition, and security best practices.
- Ensure all employees are aware of their roles and responsibilities during an incident.

11. Tools and Technologies:

- Utilize SIEM (Security Information and Event Management) tools for real-time monitoring and threat detection.
- Implement network forensics tools to support investigation efforts.

12. Escalation Protocols:

- Define clear escalation procedures for incidents that require external assistance or involve significant regulatory implications.

13. Legal Compliance:

- Ensure all incident response activities comply with relevant laws, including PDPA and GDPR, especially when handling personal data.
- Cooperate with legal authorities and provide required information during investigations.

14. Communication Protocols:

- Establish communication channels and protocols for internal and external stakeholders during an incident.
- Develop a crisis communication plan to manage media relations and public announcements.

15. Documentation and Reporting:

- Maintain detailed records of all incidents, including detection, response, containment, recovery, and post-incident analysis.
- Submit required reports to regulatory bodies as per legal obligations.

Conclusion: The Incident Response Policy is a critical component of Gotham Ltd.'s overall risk management strategy. By adhering to this policy, the organization ensures preparedness for potential incidents, minimizes their impact, and maintains compliance with legal and regulatory requirements. Continuous improvement through regular testing, training, and updates will enhance the effectiveness of incident response efforts.