Gotham Ltd. Information Security Policy

---

1. Introduction

This Information Security Policy is designed to protect Gotham Ltd.'s information assets, ensuring confidentiality, integrity, and availability of data. It aligns with best practices such as NIST and ISO 27001 standards and adheres to local regulations, including Indonesia's Personal Data Protection Act (PDPA).

2. Scope

This policy applies to all employees, contractors, third parties, and all physical and digital assets under Gotham Ltd.'s jurisdiction.

3. Information Security Objectives

- **Confidentiality** : Restrict access to authorized individuals.
- **Integrity** : Maintain data accuracy and completeness.
- **Availability** : Ensure data is accessible when needed.

4. Risk Management

- Identify potential threats (cyberattacks, natural disasters).
- Assess likelihood and impact of identified risks.
- Implement controls to mitigate risks.

5. Access Control

- **Authentication** : Enforce multi-factor authentication (MFA).
- **Authorization** : Implement role-based access control (RBAC).
- **Privilege Management** : Regularly review and update access privileges.

6. Data Protection

- **Encryption** : Protect data at rest and in transit.
- **Backup Strategies** : Regular, secure backups with off-site storage.
- **Disaster Recovery Plan** : Plan for quick recovery from disruptions.

7. Network Security

- **Firewalls** : Establish perimeter security with updated rules.
- **Intrusion Detection Systems (IDS)** : Monitor network traffic for suspicious activities.
- **VPN Configuration** : Secure remote access using encrypted tunnels.
- **Wireless Network Security** : Use strong encryption and authentication protocols.

8. Physical Security

- **Access Controls** : Implement security patrols, biometric access cards, and surveillance cameras.
- **Security Drills** : Conduct regular drills to test physical security measures.

9. Compliance and Legal Considerations

- Adhere to PDPA and other relevant laws.
- Maintain records of audits and incident reports.

10. Incident Response Plan

- **Detection** : Use logs and monitoring tools for threat detection.
- **Containment** : Isolate affected systems to prevent spread.
- **Eradication** : Remove malicious software.
- **Recovery** : Restore from backups; ensure data integrity post-recovery.
- **Post-Incident Analysis** : Review incidents to improve future responses.

11. Training and Awareness

- Conduct annual workshops and phishing simulations.
- Educate employees on security best practices and threat recognition.

12. Monitoring and Auditing

- Use SIEM tools for real-time threat detection.
- Perform regular audits to ensure policy compliance and identify improvements.

13. Third-party Management

- Assess risks posed by suppliers.
- Include security clauses in contracts; conduct third-party security audits.

14. Acceptable Use Policy

- Define employee guidelines on resource usage, including restrictions on personal devices accessing sensitive data.

15. Asset Classification and Handling

- Categorize assets as critical, important, or general; apply varying security measures.
- Implement procedures for proper storage, handling, and disposal of assets.

16. Contingency Planning

- Develop disaster recovery plans (DRP) and business continuity management (BCM) to ensure quick resumption of operations post-disruption.

17. Policy Implementation and Enforcement

- Ensure the policy is actively implemented and enforced.
- Regularly review and update the policy to adapt to new threats and business changes.

Appendices

- Include detailed technical information, forms for incident reporting, and other supportive documents.

This structured approach ensures that Gotham Ltd.'s information security is comprehensive, adaptable, and aligned with best practices, providing a robust defense against potential threats.