Security Policy Document for Gotham Ltd.

---

1. Introduction

This Security Policy outlines the guidelines and procedures for safeguarding Gotham Ltd.'s information assets and ensuring business continuity in the face of cybersecurity threats. It applies to all employees, contractors, and third parties accessing Gotham Ltd.'s IT resources.

---

2. Purpose

The primary objectives of this policy are:

- To protect sensitive information from unauthorized access, breaches, or leaks.
- To ensure business continuity by mitigating risks that could disrupt operations.
- To comply with local and international data protection laws, including Indonesia's Personal Data Protection Act (PDPA) and the General Data Protection Regulation (GDPR).

---

3. Scope

This policy applies to:

- All employees of Gotham Ltd.
- Contractors and third-party vendors.
- All IT assets, including headquarters in Jakarta, branches in Bandung and Surabaya, warehouse, and factory in Bogor.
- Communication through company emails and the web-based application used for interactions with suppliers and partners.

---

4. Definitions

- **Data Center:** A dedicated server facility housing critical data and applications.
- **WAN/VPN:** Wide Area Network and Virtual Private Network connections linking all assets.
- **RBAC (Role-Based Access Control):** System controlling access based on user roles.
- **MFA (Multi-Factor Authentication):** Security measure requiring multiple forms of verification for access.

---

5. Access Control

- **Remote Access:** Implement MFA for secure remote access via WAN and VPNs.
- **RBAC:** Enforce based on job roles to ensure minimal privilege levels.
- **Visitor Management:** Restrict physical access to facilities with security badges or escorted visits.

---

6. Data Protection

- **Physical Security:** Restrict access to the data center with biometric scanners and security cameras.
- **Encryption:** Apply encryption for data at rest and in transit, with HTTPS for web communications.
- **Backups:** Regular backups stored securely on-site and off-site, tested periodically.

---

7. Monitoring and Logging

- **Network Monitoring:** Continuously monitor IT assets for suspicious activities.
- **Log Management:** Maintain logs of all security events for a specified retention period.
- **Incident Detection:** Use tools to detect and alert potential security breaches.

---

8. Incident Response

- **Response Team:** Establish a team with clear roles for handling incidents.
- **Steps:** Identify, contain, eradicate, recover from, and report incidents.
- **Communication Protocol:** Define who is informed first in case of a breach (management, legal teams, customers).

---

9. Legal Compliance

- **PDPA/GDPR:** Ensure compliance with Indonesia's PDPA and international GDPR standards for data handling.

---

10. Web-Based Application Security

- **Security Audits:** Conduct regular audits to identify and fix vulnerabilities.
- **Updates:** Keep software updated and implement strong authentication methods.

---

11. Network Segmentation

- **Isolation:** Segment the network to isolate sensitive areas from less critical ones, reducing attack surfaces.

---

12. Training and Awareness

- **Frequency:** Conduct quarterly or bi-annual training sessions on cybersecurity.
- **Content:** Cover latest threats, security practices, and incident response procedures.

---

13. Physical Security Measures

- **Location-Specific:** Tailor physical security measures to each location's conditions (e.g., Jakarta vs. Bandung).

---

14. Enforcement and Accountability

- **Policy Review:** Regularly review and update the policy as needed.
- **Compliance Audits:** Conduct audits to ensure adherence across all departments.

---

15. Conclusion

This Security Policy is a collaborative effort involving IT, HR, legal, and management teams. It ensures that Gotham Ltd. operates with robust cybersecurity measures, protecting its assets and maintaining compliance with relevant laws.

Approved by:

[Name]
[Title]
Gotham Ltd.