IT Security Policy for 1st Waste Management Consultants Limited

1. Purpose

The purpose of this IT Security Policy is to ensure that the information technology (IT) systems of 1st Waste Management Consultants Limited (1st Waste) are protected from unauthorized access, disclosure, alteration, and destruction. This policy outlines the responsibilities, standards, and protocols required to safeguard sensitive information, ensure compliance with relevant regulations, and protect the company's business processes.

---

2. Scope

This policy applies to all employees, contractors, vendors, and any other individuals who have access to the IT systems, networks, or data owned or managed by 1st Waste. It covers all hardware, software, networks, cloud systems, data, and services used within the organization.

---

3. Roles and Responsibilities

- **IT Security Officer (ITSO):** The IT Security Officer is responsible for overseeing the implementation, maintenance, and enforcement of this policy.
- **All Employees:** All staff members are responsible for understanding and complying with this policy and reporting any suspicious activities or security breaches.
- **System Administrator (GetOn I.T. Consultants Ltd):** Responsible for managing user access, performing regular system checks, monitoring for security vulnerabilities, applying security updates, and reporting non-adherence to the policy.
- **Third-Party Vendors:** Must comply with this policy and any relevant security procedures during the provision of services to 1st Waste.

---

4. Information Classification and Handling

All company data shall be classified into three categories:

1. **Public:** Information that can be freely shared outside the organization.
2. **Internal:** Non-sensitive information intended for internal use only.
3. **Confidential:** Sensitive information requiring the highest level of protection, such as financial records, customer information, business plans and staff personnel records.

- **Confidential Data Handling:**
    - Encryption should be used for confidential data in transit and at rest.
    - Only authorized personnel should have access to confidential data.
    - Confidential information should not be shared via unsecured channels, including email unless encrypted.

---

5. Access Control

- **User Access Management:**
    - User accounts must be created, managed, and disabled by authorized personnel only.
    - Access to systems must be based on job roles and responsibilities, adhering to the principle of least privilege.
    - Multi-factor authentication (MFA) must be enforced where possible.
- **Password Management:**
    - Passwords must meet complexity requirements (minimum of 8 characters, including uppercase, lowercase, numbers, and symbols).
    - Passwords must not be shared or written down.

---

6. Network Security

- **Firewalls and Intrusion Detection Systems (IDS):** Firewalls and IDS must be deployed to protect internal systems from external threats. Regular audits and updates must be conducted jointly between the ITSO and System Administrators.
- **Wireless Networks:**
    - Wireless networks should be protected with strong encryption (e.g., WPA3).
    - Guest access to Wi-Fi should be separated from the main network.
- **Remote Access:**
    - Virtual Private Networks (VPNs) must be used for remote access to the company's network.
    - Remote access should be monitored and restricted to authorized users only.

---

7. Data Protection and Backup

- **Data Backup:** Regular backups of critical data must be conducted and stored in a secure, encrypted environment.

- **Data Retention:** Data must be retained as per legal and business requirements. Sensitive data must be securely deleted when no longer needed.

---

8. Software and Patch Management

- All software used within 1st Waste must be authorized, licensed, and regularly updated.
- Security patches must be applied promptly to address any known vulnerabilities.
- Unapproved or pirated software is strictly prohibited.
- No software is to be downloaded without written authorisation from the system administrator.

---

9. Incident Management

- **Reporting Incidents:** All security incidents, including suspicious activities, system malfunctions, or breaches, must be reported immediately to your senior management team.
- **Incident and Data Breach Response Plan:**
    - In case of becoming aware of a possible data breach, the user should report this to your senior management team and if possible, the ITSO.
    - The System Administration team will assess the situation and mitigate the damage, if any. The ITSO should be notified as soon as any threat has been removed.

---

10. Training and Awareness

- All employees must receive training on IT security best practices, phishing, and social engineering threats.
- Employees should be educated on recognizing security threats and following company protocols to mitigate risks.

---

11. Compliance and Auditing

- **Legal Compliance:** 1st Waste will comply with all relevant legal and regulatory requirements, including data protection laws like GDPR.
- **Internal Audits:** Regular IT security audits should be conducted to assess the effectiveness of the company's security measures and identify potential areas for improvement.

12. Personal Devices (BYOD) Policy

1st Waste does not permit the use of personal devices, including smartphones, tablets, and laptops, for work-related purposes. All employees must use company-issued devices for any work-related activities. This ensures that company data remains secure and under the control of the 1st Waste.

- **Prohibited Actions:**
    - No personal devices are allowed to connect to the company network or access company resources (e.g., email, cloud storage, etc.).
    - Employees are not allowed to use personal devices to store, process, or transfer any company data.
- **Monitoring and Enforcement:**
    - Any unauthorized use of personal devices for work-related purposes will be considered a violation of this policy and may result in disciplinary action.

13. Unauthorized USB Devices and Cables

To protect the integrity of the company's IT infrastructure and prevent data leakage, the following policies apply to the use of USB devices and cables:

- **USB Device Restrictions:**
    - Only company-issued or authorized USB devices (including external hard drives, flash drives, etc.) may be used on company systems.
    - Personal USB devices are prohibited from being connected to company computers, servers, or other IT assets unless explicit approval has been granted by the IT department or a 1st Waste Director.
- **USB Port Control:**
    - Any authorized use of USB devices must comply with encryption standards to ensure data security.
- **Unauthorized USB Cables:**
    - Employees are not permitted to use non-authorized **USB charging cables** or data transfer cables on company systems, as these can introduce potential malware or security vulnerabilities.
- **Reporting Unauthorized Devices:**
    - Any suspicious or unauthorized use of USB devices or cables should be reported to your senior management team or system administrator immediately.
- **Data Transfer Restrictions:**

- Transferring sensitive or confidential data to external storage devices, including USB drives, is strictly prohibited unless encryption is used and approval is granted by management.

14. Policy Review

This IT Security Policy shall be reviewed as needed to address evolving security threats, business needs, or regulatory requirements.

Approved by:
Mr R. Groome
Managing Director
1st Waste Management Consultants Limited

Date: 21/10/2026 Signature: 