POLICY ON

Cyber Security Policy

Table of Contents

1. Preamble

This Cyber Security Policy outlines the measures and protocols implemented by Antony Waste Handling Cell Limited (referred to as "AWHCL" or the "Company") to protect its technology and information assets. The policy aims to identify potential threats to these assets and establish guidelines for their protection.

2. Scope and Objectives

This Policy is applicable to the Company and its subsidiary or associated companies under same management for protecting and safeguarding the Information Technology assets owned by them. This aims to implement into company users, employees, contractors, service providers, and other authorized users of the Company and the user's responsibilities and privileges.

This policy also contains procedures for responding to incidents that threaten the security of the Company Information Technology Assets.

3. Definitions

a. **"Act"** means the Companies Act, 2013 as may be amended from time to time.
b. **"Board of Directors"** or **"Board"** means the Board of Directors of Antony Waste Handling Cell Limited, as constituted from time to time.
c. **"Policy"** shall mean the Cyber Security Policy, as amended from time to time.
d. **"The Company"** means Antony Waste Handling Cell Limited and its subsidiary companies, and associates which are under same management, from time to time.
e. "**Cyber Security**" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;
f. **"Information Technology Assets"** shall include Computer systems, servers, networks, firewall, software, applications including cloud applications, peripherals, communication devices, database programme etc.;
g. **"Security Administrator"** shall mean a Head of Informational Technology Department from time to time;

h. Any other term not defined herein shall have the same meaning as defined in the Act, Listing Regulations, Insider Trading Regulations or any other applicable law or regulation, amended from time to time.

4. Classification of Information

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The company shall classify the information controlled by them. The Security Administrator is required to review and approve the classification of the information and determine the appropriate level of security to best protect it. Furthermore, the Security Administrator shall classify information controlled by units not administered by Security Administrator.

5. Risk Assessment of Information Technology Assets

The Company has assessed the following risk associated with Information Technology Assets:

- Information systems vulnerability
- Physical Security for IT
- Critical Process vulnerabilities
- Data Security breach
- Malware Protection
- Social engineering attacks e.g. Hackers.
- Software supply chain attacks
- Phishing emails

6. Mitigation process

To reduces the overall cyber risk or impact administrator implement application whitelisting, VAPT, patching applications, patching operating systems and using the latest version, firmware updates, minimising administrative privileges, antivirus installations, limited access to websites, blocking USB, creating data backups, conducting regular employee cybersecurity training, using strong and complex passwords, Installing firewalls and blocking ports, VPN access for secure connections.

7. User Responsibilities

The Company users, employees, contractors, service providers, and other authorized users of shall have following responsibilities once they have been granted access to any of the Information Technology Assets by the System Administrator:

7.1. Acceptable Use

(i) All the user account on the Information Technology Assets shall exclusively for the business purpose and any unauthorized use of the same for illicit, or illegitimate purpose shall constitute illegal activity under applicable legal statues and can be punishable by law.

Therefore, unauthorized use of the same shall constitute grounds for either civil or criminal prosecution.

(ii) Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the company.

(iii) Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.

(iv) Users shall not attach unauthorized devices on their computer systems or workstations unless they have received specific authorization from their superiors and/or the system, administrator.

(v) Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate superiors.

7.2. Use of Internet

The company will provide Internet access to employees who are connected to the internal network and who have a business need for this access. Employees and must obtain permission from their supervisor and file a request with the Security Administrator.

The Internet is a business tool for the Company. It is to be used for business-related purposes such as communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving, or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threating in nature for "chain letters" or any other purpose which is illegal or for personal gain.

7.3. Monitoring Use of Computer Systems

AWHCL has the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is not the company policy or intent to continuously monitor all computer usage by employees or other users of the company computer systems and network. However, users of the systems should be aware that the company may monitor usage, including, but not limited to, partners of usage of the Internet (e.g., site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with company policy.

7.4. Access Control

A fundamental component of our Cyber Security Policy is controlling access to critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources.

Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users

based on their job requirements.

7.5. User System and Network Access - Normal Use identification

All users shall be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever.

Employees shall be responsible for all transactions occurring during Logan sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

7.6. Connecting Devices to the Network

Only authorized devices shall be connected to the company network(s). Authorized devices include PCs and workstations owned by a company that comply with the configuration guideline of the company. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-company that are not authorized, owned and/or controlled by company. Users are specifically prohibited from attaching USB drives and Mobiles to the company network.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g., USB drives and writable CD's.

7.7. Remote Access

Only authorized persons may remotely access the company network. Remote access is provided to those employees and service providers of the company that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to company network connection. The only acceptable method of remotely connecting into

the internal network is using a secure ID.

7.8. Unauthorized Remote Access

The attachment of (e.g., hubs / switches /CCTV) user's PC or workstation that connected to the company LAN is not allowed without the written permission of the company. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

8. Security Awareness and Training

AWHCL recognizes that employees play a vital role in maintaining a secure environment. The Company will provide regular security awareness and training programs to educate employees about best practices, security policies, and their responsibilities in safeguarding technology and information assets.

9. Security Incident Handling Procedures

The terms "Security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network.

Some examples of security incidents are:

a. Illegal access of a company computer system. For example, a hacker logs onto a production server and copies the password file.
b. Damage to a company computer system or network caused by illegal access. Releasing a virus or worm would be an example.
c. Denial of service attack against a company web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
d. Malicious use of system resources to launch an attack against other computer outside of the company network. For example, the system administrator notices a connection to an

unknown network and a strange process accumulating a lot of server time.

User who believe their information technology assets have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their HOD and System Administrator immediately.

User shall not turn off the computer delete suspicious files. Leaving the computer in the condition it was in when the Security incident was discovered will assist in Identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

Procedure of handling pre and post security incidents

Pre Incident	Post Incident
Preparation Identification	Identification
	Containment
	Eradication
	Investigation and analysis
	Conclusion
	Fast, Effective Recovery
	Conducting post-incident reviews to identify areas for improvement

10. Policy Review

The policy shall be periodically reviewed and brought in conformity with statutory and regulatory requirements, as and when required, by the Risk Management Committee of the Company.

11. Interpretation

In any circumstance where the provisions of this Policy differ from any existing or newly enacted law, rule, regulation or standard governing the Company, the relevant law, rule,

regulation or standard will take precedence over this Policy until such time as this Policy is changed to conform to the said law, rule, regulation or standard.

12. Disclosure

The Policy is disclosed on Company's website i.e. www.antony-waste.com.