CYBER SECURITY POLICY

Archean Chemical Industries Limited

1. Introduction

1.1.1. Archean Chemical Industries Limited provide IT resources to its employees to enhance their efficiency and productivity. These resources are meant as tools to access and process information related to their areas of work. These resources help officials to remain well informed and carry out their functions in an efficient and effective manner.

1.1.2. For this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

1.1.3. Misuse of these resources can result in unwanted risk and liabilities for the Archean Chemical Industries Limited. It is, therefore, expected that these resources are used primarily for Archean Chemical Industries Limited related purposes and in a lawful and ethical way.

2. Scope

2.1.1. This policy governs the usage of IT Resources from an end user's perspective

2.1.2. This policy is applicable to all employees of Archean Chemical Industries Limited.

3. Objective

3.1.1. The objective of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users. Use of resources provided by Archean Chemical Industries Limited imply the user's agreement to be governed by this policy.

4. Roles

4.1. The official identified for the task should be responsible for the management of the IT resources deployed for the use of entire user base under their respective domain

4.1.1. Implementing Authority – IT -Head Archean Chemical Industries Limited.

4.1.2. Implementing Department – IT department

5. Access to the Network

5.1. All devices on the network of Archean Chemical Industries Limited should not be accessible without proper Authentication (Preferably Biometric Authentication for Physical access to Computer / Data Centre at Office Premises).

6. Access to Internet and Intranet

6.1. A user should register the client system and obtain one time approval /permission from the Implementing authority before connecting the client system to the Archean network.

6.2. Users should not undertake any activity through any website or applications to bypass filtering / Policy / Firewall / UTM of the network or perform any other unlawful acts which may affect the network's performance or security

6.3. Users are not allowed to change the NIC configuration, IP address or any other parameters set for accessing company's LAN & WAN without permission of implementing authority

6.4. Users shall not connect any other devices to access Internet / any other network in the same client system configured for connecting to LAN/WAN of the company without permission.

6.5. It is the responsibility of the user to ensure that the client system is free from any Virus/Malware/Potential threat software/pirated copy of software before connecting to company's network.

7. Access to Archean Chemical Industries Limited Wireless Networks

For connecting to a Archean Chemical Industries Limited wireless network, user should ensure the following:

7.1. A user should register the access device and obtain one time approval / permission from the Implementing authority before connecting the access device to the Archean Chemical Industries Limited wireless network

7.2. Wireless client systems and wireless devices should not be allowed to connect to the Archean Chemical Industries Limited wireless access points without due authentication

7.3. To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks. It is the responsibility of the user to ensure that the device is free from any Virus/Malware/Potential threat software/pirated copy of software before connecting to company's Wi-Fi network.

8. Filtering and blocking of sites:

8.1. Implementing Department may block content over the Internet which is in contravention of the relevant provisions of the Government Laws and other applicable laws or which may pose a security threat to the network.

8.2. Implementing Department may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the network security and productivity of the users/organization.