THIRUMALAI CHEMICALS LIMITED

CYBER SECURITY POLICY

[Information and cyber security policies ensure that IT resources efficiently serve the primary business functions, provide security for members' electronic data, and comply with federal and other regulations. Security policies are an integral and critical component of daily business.]

Antivirus Policy

All computer devices connected to the THIRUMALAI CHEMICALS network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.
The virus protection software must not be disabled or bypassed without IT approval. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Each file server, attached to the THIRUMALAI CHEMICALS network, must utilize THIRUMALAI CHEMICALS IT approved virus protection software and setup to detect and clean viruses that may infect THIRUMALAI CHEMICALS resources.

Each e-mail gateway must utilize THIRUMALAI CHEMICALS IT approved e-mail virus protection software. All files on computer devices will be scanned periodically for malware. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Service Desk.

If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the THIRUMALAI CHEMICALS network until the infection has been removed.

Email Security

Corporate e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on THIRUMALAI CHEMICALS's computer systems. THIRUMALAI CHEMICALS can, but is not obliged to, monitor emails without prior notification. All e-mails, files, and documents – including personal e-mails, files, and documents – are owned by THIRUMALAI CHEMICALS, may be subject to open records requests, and may be accessed in accordance with this policy.

Incoming email must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will

be quarantined for the user to review for relevancy. Introducing a virus or malicious code to THIRUMALAI CHEMICALS systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, IT must be immediately notified.

Anti-spoofing practices have been initiated for detecting spoofed emails. Employees should be diligent in identifying a spoofed email. If email spoofing has occurred, IT must be immediately notified.

Incoming emails are scanned for malicious file attachments. If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed from the email prior to delivery.

Email rejection is achieved through listing domains and IP addresses associated with malicious actors. Any incoming email originating from a known malicious actor will not be delivered.

Any email account misbehaving by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.

E-mail is to be used for business purposes and in a manner that is consistent with other forms of professional business communication. All outgoing attachments are automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm THIRUMALAI CHEMICALS's reputation.

The following activities are prohibited by policy:

- Sending e-mail that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability.
- Using e-mail for conducting personal business.
- Using e-mail for the purposes of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.
- Sending e-mail using another person's e-mail account, except when authorized to send messages for another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- Forging or attempting to forge e-mail messages.
- Using unauthorized e-mail software.
- Knowingly disabling the automatic scanning of attachments on any THIRUMALAI CHEMICALS personal computer.
- Knowingly circumventing e-mail security measures.
- Sending or forwarding joke e-mails, chain letters, or hoax letters.
- Sending unsolicited messages to large groups, except as required to conduct THIRUMALAI CHEMICALS business.
  Sending excessively large messages or attachments (More than 10 MB).
- Knowingly sending or forwarding email with computer viruses.

- Setting up or responding on behalf of THIRUMALAI CHEMICALS without management approval.

All confidential or sensitive THIRUMALAI CHEMICALS material transmitted via e-mail, outside THIRUMALAI CHEMICALS's network, must be encrypted. Passwords to decrypt the data should not be sent via email.

E-mail is not secure. Users must not e-mail passwords, social security numbers, account numbers, pin numbers, dates of birth, mother's maiden name, etc. to parties outside the THIRUMALAI CHEMICALS network without encrypting the data.

All user activity on THIRUMALAI CHEMICALS information system assets is subject to logging and review. THIRUMALAI CHEMICALS has software and systems in place to monitor email usage.

Firewall Policy

All network firewalls, installed and implemented, must conform to the current standards as determined by THIRUMALAI CHEMICALS's IT Department. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

The approach adopted to define firewall rulesets is that all services will be denied by the firewall unless expressly permitted in this policy.

Outbound – allows all Internet traffic to authorized groups
All traffic is authorized by Internet Protocol (IP) address and port

The firewalls will provide

Packet filtering – selective passing or blocking of data packets as they pass through a network interface. The most often used criteria are source and destination address, source and destination port, and protocol.

Application proxy – every packet is stopped at the proxy firewall and examined and compared to the rules configured into the firewall.

Stateful Inspection – a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

The firewalls will protect against:

IP spoofing attacks – the creation of IP packets with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.

Denial-of-Service (DoS) attacks - the goal is to flood the victim with overwhelming amounts of traffic and the attacker does not care about receiving responses to the attack packets.

Any network information utility that would reveal information about the THIRUMALAI CHEMICALS domain.

A change control process is required before any firewall rules are modified. Prior to implementation, the Third-party Vendor and THIRUMALAI CHEMICALS network administrators are required to have the modifications approved by the VP Finance.

All firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic.

Firewall rulesets and configurations require periodic review to ensure they afford the required levels of protection:

THIRUMALAI CHEMICALS must review all network firewall rulesets and configurations during the initial implementation process and periodically thereafter.

Firewall rulesets and configurations must be backed up frequently to alternate storage
(Not on the same device). Multiple generations must be captured and retained, to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.

Network Security and VPN Acceptable Use

Users are permitted to use only those network addresses assigned to them by *THIRUMALAI CHEMICALS 's IT Department.*

All remote access to THIRUMALAI CHEMICALS will either be through a secure VPN connection on a THIRUMALAI CHEMICALS owned device that has up-to-date anti-virus software, or on approved mobile devices (see the THIRUMALAI CHEMICALS Owned Mobile Device Acceptable Use and Security Policy and the Personal Device Acceptable Use and Security Policy).

Remote users may connect to THIRUMALAI CHEMICALS Information Systems using only protocols approved by IT.

Users inside the THIRUMALAI CHEMICALS firewall may not be connected to the THIRUMALAI CHEMICALS
network at the same time a remote connection is used to an external network.

Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point to the THIRUMALAI CHEMICALS network without THIRUMALAI CHEMICALS IT approval.

Users must not install network hardware or software that provides network services without THIRUMALAI CHEMICALS IT approval.

Non-THIRUMALAI CHEMICALS computer systems that require network connectivity must be approved by THIRUMALAI CHEMICALS IT.

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, THIRUMALAI CHEMICALS users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the THIRUMALAI CHEMICALS network infrastructure. Only the IT Department is permitted to perform these actions.

Users are not permitted to alter network hardware in any way.

Remote Access

It is the responsibility of THIRUMALAI CHEMICALS employees, volunteers/directors, contractors, vendors, and agents, with remote access privileges to THIRUMALAI CHEMICALS's corporate network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to THIRUMALAI CHEMICALS.

General access to the Internet, through the THIRUMALAI CHEMICALS network is permitted for employees who have flat-rate services and only for business purposes. THIRUMALAI CHEMICALS employees are responsible to ensure that they:

- Do not violate any THIRUMALAI CHEMICALS policies
- Do not perform illegal activities
- Do not use the access for outside business interests

THIRUMALAI CHEMICALS employees bear responsibility for the consequences should access be misused.

Employees are responsible for reviewing the following topics (listed elsewhere in this policy) for details of protecting information when accessing the corporate network via remote access methods and acceptable use of THIRUMALAI CHEMICALS's network:

- Virtual Private Network (VPN)
- Wireless Communications

Must ensure that their computer, which is remotely connected to THIRUMALAI CHEMICALS's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

Must not use non-THIRUMALAI CHEMICALS email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct THIRUMALAI CHEMICALS business, thereby ensuring that official business is never confused with personal business.

For remote access to THIRUMALAI CHEMICALS hardware, all hardware configurations must be approved by IT.

All hosts that are connected to THIRUMALAI CHEMICALS internal networks, via remote access technologies, must use up-to-date, anti-virus software applicable to that device or platform.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the THIRUMALAI CHEMICALS production network must obtain prior approval from IT.

Virtual Private Network (VPN)

The purpose of this section is to provide guidelines for Remote Access IPsec or L2TP Virtual Private Network (VPN) connections to the THIRUMALAI CHEMICALS corporate network. This applies to implementations of VPN that are directed through an IPsec Concentrator.

This applies to all THIRUMALAI CHEMICALS employees, volunteers/directors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the THIRUMALAI CHEMICALS network.

Approved THIRUMALAI CHEMICALS employees, volunteers/directors, and authorized third parties (customers, vendors, etc.) may utilize the benefit of a VPN on a THIRUMALAI CHEMICALS device, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying associated fees. Further details may be found in the Remote Access section.

Wireless Communications

Access to THIRUMALAI CHEMICALS networks is permitted on wireless systems that have been granted an exclusive waiver by IT for connectivity to THIRUMALAI CHEMICALS's networks.

This section covers any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to THIRUMALAI CHEMICALS's networks do not fall under the review of this policy.

Password Policy

Passwords for THIRUMALAI CHEMICALS network access must be implemented according to the following guidelines:

Email Passwords must be changed every 90 days
Passwords must adhere to a minimum length of 8 characters
Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=?/~';',<>|\).
passwords must not be easily tied back to the account owner such as:
username, social security number, nickname, relative's names, birth date, etc.

Passwords must not be dictionary words or acronyms
Passwords cannot be reused for 3 times

THIRUMALAI CHEMICALS passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.

Passwords must not be written down and stored anywhere in any office.
Passwords must not be stored in a file on a computer system or mobile device
(Phone, tablet) without encryption.

If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:

Take control of the passwords and protect them Report the discovery to IT

Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.

PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.

Vulnerability Assessment

The operating system or environment for all information system resources must undergo a regular vulnerability assessment. This standard will empower the IT Department to perform periodic security risk assessments for determining the area of vulnerabilities and to initiate appropriate remediation. All employees are expected to cooperate fully with
any risk assessment.

Vulnerabilities to the operating system or environment for information system resources must be identified and corrected to minimize the risks associated with them.

Audits may be conducted to:

Ensure integrity, confidentiality, and availability of information and resources

Investigate possible security incidents and to ensure conformance to THIRUMALAI CHEMICALS's security policies

Monitor user or system activity where appropriate

To ensure these vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo an authenticated vulnerability assessment.

The frequency of these vulnerability assessments will be dependent on the operating system or environment, the information system resource classification, and the data classification of the data associated with the information system resource.

Retesting will be performed to ensure the vulnerabilities have been corrected. An authenticated scan will be performed by either a Third-Party vendor or using an in-house product.

All data collected and/or used as part of the Vulnerability Assessment Process and related procedures will be formally documented and securely maintained.

IT leadership will make vulnerability scan reports and on-going correction or mitigation progress to senior management for consideration and reporting to the Board of Directors.

E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of THIRUMALAI CHEMICALS, unless appropriately authorized (explicitly or implicitly) to do so.

Users must not send, forward, or receive confidential or sensitive THIRUMALAI CHEMICALS information through non-THIRUMALAI CHEMICALS email accounts. Examples of non-THIRUMALAI CHEMICALS e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and e- mail provided by other Internet Service Providers (ISP).

Users with non-THIRUMALAI CHEMICALS issued mobile devices must adhere to the Personal Device Acceptable Use and Security Policy for sending, forwarding, receiving, or storing confidential or sensitive THIRUMALAI CHEMICALS information.

Patch Management

Many computers operating systems, such as Microsoft Windows, Linux, and others, include software application programs which may contain security flaws.

Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the THIRUMALAI CHEMICALS network, and all computers connected to it. Almost all operating systems and many software applications have periodic security patches, released by the vendor, that need to be applied.

Patches, which are security related or critical in nature, should be installed as soon as possible.

In the event that a critical or security related patch cannot be centrally deployed by IT, it must be installed in a timely manner using the best resources available.

Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a violation of policy