Factory address: survey No 347, Village: Lunej,
Khambhat- Golana road,
Tal.Khambhat, Dist: Anand, Gujarat-388 620
(M) +91 94278 42983 / 94282 14487

INFORMATION SECURITY POLICY

We use information technology to advance the business interests of the company and our customers.

We recognize that the use of information technology and associated systems such as email, software, networks, applications, internet and social media might all be subject to cyberattacks and other similar internal and external threats.

We use our information technology responsibly, only for legitimate business purposes, consistent with the company's interests and rights, and in accordance with the company's rules, regarding our information technology systems.

We take great pride in our spirit of innovation. The company has created an immensely valuable brand and continuously adds to its portfolio of intellectual property that is incorporated into patents, copyrights, trademarks, service marks, trade secrets, design rights, and other proprietary rights.

We also possess vast amounts of expertise and other confidential information that give us a competitive edge in the marketplace.

We vigorously protect our intellectual property and confidential information, and follow our internal policies on the proper use, safekeeping, marking and handling of such property and information.

We respect the intellectual property and confidential information of others and expect the same from others in return.

We acknowledge the importance of personal data protection and believe that the principles behind data protection strengthen individual rights. We collect, use, store, handle, transfer and disclose personal data in accordance with applicable laws and expect our suppliers and business partners to do the same. Company's global standards for safeguarding personal data ensures that company provides a high level of protection regardless of where the data is collected and processed.

Records being generated as part of this policy shall be retained for a period of three years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

A. Information Handling:

A.1 Classification of information

An inventory will be maintained of all the Technichem Organics Pvt. Ltd. major IT assets and the ownership of each asset will be clearly stated. Within the inventory, the information processed by each IT asset will be classified according to sensitivity.

A.2 Precautions against hardware, software or data loss

All IT equipment must be safeguarded appropriately, especially when left unattended. Files downloaded from the internet carry a risk and should only be downloaded from trusted sites and scanned with an anti-virus product. Email poses a significant threat and files attached to and links within email must be treated with caution to safeguard against Phishing type attacks which seek to harvest personal information and deliver malicious code including ransomware that can lead to the encryption of important business data. IT users have a duty to check the address of the recipient each time an email is sent to reduce the chance of accidental data loss through email.

Individuals must avoid the automatic forwarding of email from their company account to personal email accounts where there is the possibility for confidential or sensitive information being delivered to their company mailbox. The use of USB storage devices is a common cause of compromise through infections from computer viruses, malware and spyware and should be avoided. USB storage devices which are not from a trusted source must not be attached to a company computer. Files on trusted USB storage devices must be scanned with an anti-virus product before use or transfer to Technichem Organics Pvt. Ltd. systems and network drives.

A.3 Disposal of equipment

When permanently disposing of equipment containing all types of storage media, including but not limited to hard disk drives, backup tapes and USB removable media all sensitive or confidential data and licensed software should be irretrievably deleted during the disposal process. Damaged storage devices containing sensitive or confidential data will undergo an assessment to determine if the device should be destroyed, repaired, or discarded. Such devices will remain the property of Technichem Organics Pvt. Ltd. and only be removed from site with the permission of the information asset owner. Secure disposal verification certificates should be sought for media that has contained sensitive and confidential data

A.4 working practices

The organization advocates a clear screen policy particularly when employees are absent from their normal desk and outside normal working hours. Employees must log out or lock their workstations when not in use. Screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorized persons. This applies to both fixed desktops, laptops and mobile devices. Additionally, screens should be positioned so that they are not easily visible through external windows.

Whilst sharing screens on video conferencing and collaboration platforms additional care should be taken to ensure sensitive information cannot be viewed by unauthorized persons. Wherever possible computer applications should be closed before permitting remote access to IT support colleagues undertaking support and maintenance. Individuals must ensure that any screenshots provided to initiate a support ticket or aid with troubleshooting a problem do not contain sensitive and confidential data.

A.5 Backup and recovery

Backups of the Technichem Organics Pvt. Ltd. information assets and the ability to recover them are important priorities. Information owners must ensure that system backup and recovery procedures are in place and that these are routinely tested. Backup copies of data must be protected throughout their lifecycle from accidental or malicious alteration and destruction, particularly against the threat of ransomware for which offline; air-gapped; immutable backup technologies provide the strongest safeguards.

Access to data backups and supporting infrastructure must be restricted to those persons who are authorised to perform systems administration or management functions. All system managers must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace files that are more recent.

A.6 Additional data protection declaration requirement

Where a role requires access to specific business systems that contain sensitive personal or financial information, individuals may be required to sign a data protection declaration before they are sanctioned to carry out these duties

A.7 Computer Network Use Limitations Prohibited Activities:

The computer network may not be used to disseminate, view, or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.), or any other unauthorized materials. Occasional limited appropriate personal use of the computer is permitted if such use does not - a) interfere with the user's or any other employee's job performance; b) have an undue effect on the computer or company network's performance; c) or violate any other policies, provisions, guidelines or standards of this agreement or any other of Technichem Organics Pvt. Ltd. Furthermore, users are responsible for the professional, ethical and lawful use of the computer system & internet. Personal use such as Net banking/access to personal emails is a privilege that may be revoked at any time.

A.8 Virus detection:

Files obtained from sources outside the Company, including media brought from home (External hard disk/memory card/pen drives, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to the e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the Company's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first scanning the material with Technichem Organics Pvt. Ltd. -approved virus- checking Seqrite EPS software. If you suspect that a virus has been introduced into the Technichem Organics Pvt. Ltd. network, notify the System Administrator immediately.

A.9 Outsourcing and Third-Party Access

External suppliers

All external suppliers who have access to Technichem Organics Pvt. Ltd. IT Systems or data must work under the supervision of Technichem Organics Pvt. Ltd. staff and in accordance with this Policy. A copy of the Policy will be provided by the system owner to each third-party supplier at the commencement of any new contract or as this policy changes.

Wherever possible supplier remote access accounts should remain disabled by default and enabled temporarily, as required to undertake a specific task, at the request of the system owner or administrator limiting access to agreed timeframes to reduce the opportunity for unauthorized activities that may lead to data loss or unintended disruption. Accounts must be immediately deleted when no longer required.

All activities undertaken by third party suppliers must be agreed to in advance.

A.10 Risk assessment

The security risks to the information assets of all system development projects will be assessed by system owners and access to those assets will be controlled.

A.11 IT Security concern / complaint

Employees of Technichem Organics Pvt. Ltd. can report any misconduct, maloperation or breach of rules laid down in this policy to the below persons.

Or if any stakeholder is found to be guilty regarding IT security concerns, the incidence shall be reported to the below persons.

Name: Mr. Piyush Nathwani

Mobile: 79845 35603

Email: piyush.technichem@gmail.com

Approved By,

Director

Rev.01 Effective From: 01.04.2024