SECURITY POLICY

Tube/Corp. Pol.04, Rev.01/15.06.2024

Our Mission
Security is a vital element of Tubestar and key to the success of the company is the protection of the company's employees, subcontractors, assets, information, integrity, and reputation from potential threats.

Our Approach
Tubestar's code of conduct guides our operational and service delivery approach. It includes professionalism, respect for employees, subcontractors, stakeholders, and a commitment to continual improvement. This enables Tubestar to provide the most reliable service without unnecessarily exposing clients or us to security risk. Key is the need to create secure environments and processes that can be trusted by clients, stakeholders, and national and international regulatory bodies.

Scope
This policy applies to all our employees, contractors, volunteers, and anyone who has permanent or temporary access to our systems and hardware and applicable to all Tubestar locations irrespective of any geographical locations. In case the local/regional legal/customer has any additional requirements known, the same must be followed over and above the requirements of this policy.

A) Physical Security:
The company physical security policy aims at protecting its physical assets, such as buildings, equipment, vehicles, inventory including computers and other IT equipment. Information security policy aims to protect intellectual property from costly events, like data breaches and data leaks.

Protecting IT physical assets is particularly important because the physical devices contain company data. If a physical IT asset is compromised, the information it contains, and handles is at risk. In this way, information security policies are dependent on physical security policies to keep company data safe.

Although the company does not have any sensitive building/rooms, it is practiced having controlled access to company premises including controls on handling and movement of physical assets.

B) Information Security:
Tubestar Information security policy outlines guidelines and provisions for preserving the security of company related data technology infrastructure.

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

As we rely on technology to collect, store, and manage information, there are high chances of severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

To reduce the Information Security risks, necessary measures have been applied and this policy is in force to strengthen these efforts.

Policy Elements

1. **Confidential data**
   Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas, or new technologies
- Customer lists (existing and prospective)
- Personal data of Employees, contractors

All personnel working on behalf of Tubestar are obliged to protect this data.

2. **Protect personal and company devices**
   When employees/service partners use their digital devices to access company emails or accounts, they introduce security risk to company data. We advise keeping both their personal and company-issued computer, tablet, and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees/service partners to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive company-issued equipment they will receive instructions for:

- Password management for their system
- Installation of antivirus/ anti-malware software

They must follow instructions to protect their devices and refer to a company authorized IT Service provider through the Administration Dept. and location head.

3. **Keep emails safe**
   Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, employees/service partners shall:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

   If the user is not sure that an email, they received is safe, they can refer to the company's Administration Dept. and location head.

4. **Manage passwords securely**
   Password leaks are dangerous since they can compromise a company's entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, it is advised to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary, with written permission from superiors. When exchanging them is not possible in-person, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords regularly.

5. **Transfer data securely**
   Transferring data introduces security risk. employees/service partners must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask the company Administration Dept. and location head for help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

6. **Information Security Incident Reporting**
   The company Administration Dept. and location head need to know about scams, breaches, and malware so they can better protect the company infrastructure. For this reason, employees/service partners are advised to report perceived attacks, suspicious emails, or phishing attempts as soon as possible to Administration Dept. and location head; which in turn, will communicate to company top management for any specialist support required externally. The company Administration Dept. and location head and subject specialist, as required, shall investigate promptly, communicate with company top management, resolve the issue, and send a companywide alert if deemed necessary.

The company Administration Dept. and location head are responsible for advising employees on how to detect scam emails. It is encouraged that employees/service partners reach out to them with any questions or concerns.

Additional measures

The employees/service partners, on joining Tubestar are made aware of the company's Information Security policy, through Administration Dept. and location head on:

-confidentiality requirements for any data related to policies, procedures, standards, operating practices of current or potential company operations/locations, its customers, colleagues, contractors/subcontractors, licensors, business partners, in any form and nature which may or may not have any effect on current or future business and activities. This includes all data as a minimum, related Tubestar globally along with its current and future subsidiaries, and Saudi Aramco, KOC, QE, ADNOC and any such entities company may have businesses with currently or in future

-They must sign and abide F HR 18 - Confidentiality Agreement and requirements stated therein

To reduce the likelihood of security breaches, it is advised to all employees/service partners to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR and Administration Dept. and location head.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on their company equipment.
- Avoid accessing suspicious websites.

It is expected that employees/service partners shall restrict use of company provided devices and resources for personal use, social media as well as anything related to pornography.

The company Administration Dept. and location head shall:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange security training for all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Remote employees

The remote employees/service partners must follow this policy. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. In case of any information security related issues, remote employees/service partners shall seek advice from the company Administration Dept. and location head.

Disciplinary Action

The company expects that all employees/service partners shall always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: the company will issue a verbal warning through the Administration Dept. and location head and train the employee on security.
- Intentional, repeated, or large-scale breaches (which may causé severe financial or other damage): the company will invoke more severe disciplinary action up to and including termination.
  The information security related incidents shall be examined and investigated on a case-by-case basis.

Additionally, employees/service partners who are observed to disregard the information security related instructions, shall will face progressive disciplinary actions, even if their behavior hasn't resulted in a security breach.

Hardik Mehta
Director

Date: 15.06.2024